PROTEÇÃO DE DADOS OBTIDOS POR RECONHECIMENTO FACIAL: UMA ANÁLISE JURÍDICA COMPARATIVA ENTRE O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (GDPR) EUROPEU E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) BRASILEIRA

PROTECTION OF DATA OBTAINED BY FACIAL RECOGNITION: A COMPARATIVE LEGAL ANALYSIS BETWEEN THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR) AND THE BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD)

Artigo recebido em 14/09/2024
Artigo aceito em 05/10/2024
Artigo publicado em 09/02/2025

Marco Aurélio Marrafon
Professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro – UERJ. Doutor e Mestre em Direito do Estado pela Universidade Federal do Paraná – UFPR com estudos doutorais na *Università degli Studi di Roma Tre* – Italia. Presidente (2012-2018) e Membro da Academia Brasileira de Direito Constitucional. Coordenador do LabDIa – Laboratório de Direito e Inteligência Artificial do PPGD/UERJ. Advogado; e-mail: marco_marrafon@yahoo.com.br; *Lattes:* http://lattes.cnpq.br/1641645608013458**;** Orcid: https://orcid.org/0000-0002-6891-6221.

Ani Karini Muniz Schiebert
Doutoranda pela Universidade do Estado do Rio de Janeiro (PPGD/UERJ). Mestre em Direito Alemão e Europeu pela Humbodt Universität zu Berlin (Alemanha). Pós-graduada em Direito Público pela Universidade Candido Mendes (UCAM), Graduada em Letras (Língua e Literatura Alemã) pela Universidade Federal Fluminense (UFF) e em Direito pela Universidade Candido Mendes (UCAM). Advogada; e-mail: anikarinims@gmail.com ; *Lattes:* http://lattes.cnpq.br/4115567618335416 ; Orcid: https://orcid.org/0000-0001-7581-9166.

RESUMO: O problemático uso de sistemas de reconhecimento facial que tratam e armazenam dados pessoais sensíveis sem o consentimento do titular de dados tem se tornado um importante dilema da Era Digital. Baseado no Regulamento Geral de Proteção de Dados (GDPR) e na Lei Geral de Proteção de Dados brasileira (LGPD), o presente trabalho analisa de maneira comparada os respectivos diplomas legais e propõe medidas de salvaguarda dos dados obtidos com o uso dessa tecnologia para o legislador brasileiro. Verificou-se que as disposições gerais da Lei de Proteção de Dados devem ser aplicadas, pois ainda não há regulamentação específica no Brasil, com a necessidade de expandir a proteção legislativa ao nível semelhante ao regulamento europeu. Essas medidas visam a assegurar a efetividade dos direitos fundamentais à intimidade, vida privada, liberdade, não-discriminação e autonomia da vontade, conforme determinado pela Constituição de 1988.

PALAVRAS-CHAVE: reconhecimento facial; proteção de dados; LGPD; GDPR; biometria; direitos fundamentais; privacidade.

ABSTRACT: The problematic use of facial recognition systems that process and store sensitive personal data without the consent of the data subject has become an important dilemma of the Digital Age. Based on the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD), this paper analyzes the respective legal diplomas in a comparative manner and proposes measures to safeguard data obtained through the use of this technology for the Brazilian legislator. It was found that the general provisions of the Data Protection Law should be applied, as there is still no specific regulation in Brazil, with the need to expand legislative protection to a level similar to the European regulation. These measures aim to ensure the effectiveness of the fundamental rights to privacy, private life, freedom, non-discrimination and autonomy of will, as determined by the 1988 Constitution.

KEYWORDS: facial recognition; data protection; LGPD; GDPR; biometrics; fundamental rights; privacy.

1 INTRODUÇÃO

O acelerado desenvolvimento tecnológico do mundo contemporâneo prenuncia o advento de uma verdadeira Era Digital, com predomínio de uma sociedade da informação baseada em dados. Nesse contexto, sobressai a importância da tecnologia de reconhecimento facial, em especial para ações de identificação e controle dos cidadãos e usuários desse dispositivo.

Essa inovação tem sido utilizada com diversas finalidades, desde sistemas de segurança pública, controle de fronteiras e vigilância, entretenimento e emissão de documentos até propaganda, educação e saúde, uma vez que, nas versões mais aprimoradas, ela tem permitido realizar análises do comportamento do consumidor (p. ex. sua satisfação, fidelidade, etc), promover acessibilidade e o reconhecimento de emoções e aferir condições médicas por intermédio das características biométricas da face humana.

Como PINs, senhas e, inclusive, sistemas de segurança por uso de impressão digital podem ser falsificados, há um grande interesse pela obtenção de informações biométricas dos indivíduos que estejam disponíveis e possam ser obtidas em tempo real, em um formato passível de leitura por computadores. (HIRSCHBERG, 2017, p. 01).

A discussão sobre esse tema controverso vem se intensificando, sobretudo após a publicação do projeto de lei da Comissão da União Europeia, em abril de 2021, tratando

da regulamentação do uso de inteligência artificial (COMISSÃO EUROPEIA, 2021), que também engloba o emprego da biometria facial.

Devido à capacidade de análise de sentimentos, emoções e condições psíquicas, surge o questionamento acerca dos riscos do uso dessa ferramenta, em especial no que se refere à necessária proteção de dados obtidos por seu intermédio.

Nesse contexto, visando a assegurar a proteção de dados e as garantias de intimidade, privacidade e liberdade previstas na Constituição de 1988, o presente artigo se propõe a analisar o uso de tecnologias de reconhecimento facial no Brasil e a legislação protetiva dos dados cidadãos, notadamente por meio de um estudo comparado do Regulamento Geral sobre o Regulamento Geral de Proteção de Dados da União Europeia 2016/679 (sigla em inglês: GDPR) e da Lei Geral de Proteção de Dados brasileira, Lei 13.709/2018 (LGPD).

Nessa perspectiva, o estudo visa a esclarecer as seguintes indagações de pesquisa: 1. Que garantias legislativas são aplicáveis atualmente em relação ao processamento e armazenamento dos dados pessoais de forma não consentida, mediante o uso de tecnologia de reconhecimento facial? 2. Considerando-se a situação do Brasil, essas medidas são suficientes para a garantia dos direitos fundamentais de intimidade, privacidade e liberdade dos cidadãos ou devem ainda ser ampliadas, e de que forma?

Como método de pesquisa foi realizada uma análise qualitativa com base em fundamentos teóricos doutrinários e na legislação aplicável. A escolha da metodologia se deve ao fato de ser um estudo comparativo entre dois sistemas normativos: o Regulamento Geral sobre a Proteção de Dados (GDPR) europeu e a Lei Geral de Proteção de Dados (LGPD) brasileira. Uma abordagem quantitativa não será objeto desta investigação, vez que a utilização dessas tecnologias é muito recente e ainda há incipiente apreciação jurisprudencial, além de parca quantificação estatística.

Para alcançar seus objetivos, o trabalho apresenta inicialmente uma visão geral do funcionamento e do estado atual da tecnologia de reconhecimento facial, contendo uma breve exposição do desenvolvimento histórico e algumas formas de aplicações no Brasil. Na sequência, são abordados os aspectos legais sobre o uso do sistema de monitoramento por vídeo com tecnologia de reconhecimento facial com fulcro no GDPR e na, na etapa seguinte, é realizada uma análise comparada com a LGPD e examinado o uso dessa tecnologia tendo em conta a legislação brasileira.

Por último, são desenvolvidas algumas reflexões e propostas medidas protetivas com vistas a contribuir para o aperfeiçoamento da regulamentação do tema no Brasil, em

especial, contra o uso não autorizado de dados obtidos com a tecnologia de reconhecimento facial, em uma interpretação à luz do viés constitucionalista do direito fundamental à intimidade e à privacidade.

2. CONTEXTUALIZAÇÃO HISTÓRICA E VISÃO GERAL SOBRE A TECNOLOGIA DE RECONHECIMENTO FACIAL

Inicialmente, o presente trabalho objetiva descrever a funcionalidade da tecnologia de reconhecimento facial e, para isso, apresenta em linhas gerais seu desenvolvimento histórico, algumas aplicações gerais por parte de instituições públicas e privadas ou pessoas físicas, bem como sua introdução no Brasil.

Em uma primeira acepção, o objetivo do reconhecimento biométrico é constatar a identidade de uma pessoa (identificação), confirmar ou refutar a identidade reivindicada (verificação) (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), por meio das medidas da face. Sua etimologia indica a proveniência do grego antigo *bios* - vida – e *métron* - medida (DUDEN, 2016, p. 163). Assim, o termo diz respeito à mensuração e à descrição de características biológicas individuais e diferenciadas do ser humano, tais como: formatos de rosto, impressões digitais, voz, retina e íris, com o propósito específico de reconhecimento (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), b).

Em relação ao funcionamento do sistema de reconhecimento facial, primeiramente, a imagem de uma pessoa é capturada digitalmente por intermédio de uma câmera ou digitalização. Em seguida, ocorre a etapa de detecção do rosto: ele é analisado e identificado como tal (ZHAO; CHELLAPPA; PHILLIPS, 2003, p. 401).

As características biométricas de um rosto, como olhos, boca, sobrancelhas, nariz, seus contornos e diversos outros pontos nodais podem ser encontradas e extraídas. Os atributos característicos serão agrupados e registrados no conjunto dos dados referenciais (“modelo”) (DIE LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ NIEDERSACHSEN, 2018).

Caso a verificação seja feita, o software de reconhecimento compara a imagem capturada da pessoa no momento com o modelo armazenado e/ou com as demais fotos do rosto armazenadas no banco de dados (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), a). Quando o modelo e as características referentes à pessoa

a ser verificada são idênticos entre si, com uma certa margem de tolerância, indica-se que houve correspondência, o que demonstra que o procedimento de reconhecimento foi bem-sucedido.

Os estudos sobre reconhecimento facial automatizado foram iniciados no final da década de 1960 (COX; GHOSN; YIANILOS, 1996, p. 209). Entre o final da década de 1980 e o início da década de 1990, os sistemas de reconhecimento facial foram usados no reconhecimento de imagens estáticas e, mais tarde, tiveram sua utilização ampliada (CHELLAPPA; SINHA; PHILLIPS, 2010, p. 46).

Em 1990, o uso de um sistema de coordenadas faciais com alta probabilidade de recorrência permitiu um método matemático mais preciso para avaliar as formas faciais humanas (KIRBY; SIROVICH, 1990, p. 103). Em 1991, foi desenvolvido um sistema computacional "em tempo quase real" (TURK; PENTLAND, 1991, p. 71). Tornou-se possível com isso, identificar um rosto a partir de um contexto espacial com variações de iluminação, escala e orientação (TURK; PENTLAND, 1991, p. 71 e 81).

Entre 1993 e 1996, foi desenvolvido nos EUA o programa de Tecnologia de Reconhecimento Facial (FERET) (PHILLIPS; RAUSS; DER, 1996, p. 7). Suas principais metas eram o desenvolvimento de algoritmos de reconhecimento facial, a avaliação contínua desses algoritmos e a criação de um banco de dados de referência para dar suporte ao pessoal de vigilância, aos serviços de inteligência e às autoridades policiais (PHILLIPS; RAUSS; DER, 1996, p. 7).

Com os ataques terroristas nos EUA em 2001, a tecnologia de reconhecimento facial foi impulsionada no mundo todo e atraiu a atenção de governos e das principais organizações internacionais como ferramenta essencial no combate ao terrorismo (GATES, 2006, p. 417) . Com a realização de mais estudos que aprimoraram as técnicas, em 2006, o FRVT foi o primeiro programa a fazer uma comparação direta do desempenho desses sistemas entre humanos e máquinas (PHILLIPS *et al.*, 2007, p. 3).

Desde então, o progressivo desenvolvimento dessa tecnologia faz com que hoje seja bastante comum a sua utilização não apenas para medir dados biométricos da face e compará-los com os modelos para fins de identificação, mas também para realizar leituras mais complexas de sentimentos, emoções, reações psicológicas positivas ou negativas e aferição de níveis de satisfação psíquica ante a um evento/ fato presenciado.

No Brasil, a tecnologia de reconhecimento facial foi introduzida por autoridades públicas e empresas privadas em 2011, tornando-se popular em 2019, conforme pesquisa do Instituto Igarapé (INSTITUTO IGARAPÉ, 2017).

O Instituto aponta que essa tecnologia começou a ser utilizada com mais frequência no transporte público para tomar medidas contra pessoas que obtinham o direito de viajar gratuitamente por meio de falsificação e fraude. As demais aplicações se deram em contextos de segurança pública, instituições de ensino e controles de fronteira, sempre com viés de identificação, vigilância e controle. Em 2019, p. ex., a tecnologia de reconhecimento facial foi usada pela polícia brasileira durante o Carnaval e várias pessoas procuradas pelo judiciário brasileiro foram presas graças a esse sistema (LISBOA, 2019).

Por ter sediado e frequentemente sediar eventos importantes e de grande atratividade internacional, tais como a Conferência das Nações Unidas sobre Desenvolvimento Sustentável de 2012 (Rio+20), a Copa do Mundo de 2014, os Jogos Olímpicos e Paraolímpicos de 2016 e a Copa América de Futebol Masculino de 2019 e os carnavais anuais, o Brasil acabou se tornando predestinado para a implementação de tecnologias de vigilância estrangeiras (CANTO, 2019, p.1), muitas vezes em caráter experimental com vistas a fornecer elementos para seu desenvolvimento mais eficiente.

Em 21 de agosto de 2019, foi apresentado um interessante projeto de lei - PL 4612/2019 – na Câmara dos Deputados, dispondo sobre a regulamentação para o desenvolvimento, implementação e uso de tecnologias de reconhecimento facial e emocional e outras tecnologias digitais para a identificação de indivíduos e previsão ou análise de comportamento (BIBO NUNES, 2019).

Esse projeto previu a observância de pressupostos para o uso da tecnológica (como a transparência, direito à informação do uso da ferramenta, proibição de discriminação), buscou regulamentar os critérios de uso dos dados, estabelecendo a competência da Autoridade Nacional de Proteção de Dados para cuidar da temática, fiscalizando e monitorando as práticas das empresas e instituições, bem como dispôs sobre direitos dos cidadãos afetados e deveres e critérios na utilização e compartilhamento do uso de dados, a fim de assegurar o mínimo de segurança jurídica.

Todavia, as regras nele previstas se revelaram demasiadamente imprecisas e abertas, de modo que, possivelmente, a Lei dele advinda não traria grandes benefícios, uma vez que a redação legal permitia inúmeras brechas. De qualquer modo, ele foi apensado a outro projeto anterior que tratava da temática (PL 12/2015) e, no momento em que este artigo está sendo escrito, os referidos PLs aguardam pauta na Comissão de Comunicação da Câmara dos Deputados.

Esse vazio legislativo tem promovido diversos riscos, uma vez que a tecnologia encontra-se em constante aprimoramento técnico e vem sendo usada com cada vez mais com frequência por instituições públicas e privadas, bem como por pessoas físicas. Não havendo uma legislação específica em *terrae brasilis*, as diretrizes normativas devem advir da LGPD.

Tampouco há, no Regulamento Geral de Proteção de Dados da União Europeia, normativa específica para o tema, ao menos até a data de redação deste estudo. Portanto, é necessário indagar até que ponto as disposições gerais das leis gerais de proteção de dados podem ser aplicadas. Primeiramente será analisado o emprego da videovigilância com a tecnologia de reconhecimento facial em relação ao GDPR e, em seguida, em relação à LGPD.

Com a promulgação do Regulamento de Inteligência Artificial da União Europeia (AI Act), o uso dessa tecnologia foi legalizado, ainda que submetido a diversas condições, devido aos altos graus de risco que a envolvem[1]

De qualquer modo, ainda que haja pontos de sobreposição acerca do tema da proteção de dados e certa repetição de principiologia, suas disposições não afetam a aplicação das regras de proteção de dados obtidos e originados pelo uso de reconhecimento facial, questão que encontra maior guarida nas normas gerais de proteção de dados da GDPR, que seguem vigentes e aplicáveis a esses casos. Desta feita, faz todo sentido que a investigação acerca da proteção de dados siga em torno da GPDR e sua análise comparativa com a LGPD, o que será realizado nos tópicos seguintes.

3. PROTEÇÃO DE DADOS ORIUNDOS DO USO DO RECONHECIMENTO FACIAL SOB A PERSPECTIVA DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (GDPR) EUROPEU

Os dados biométricos obtidos por “métodos técnicos específicos” para a identificação de uma pessoa estão regulamentados no artigo 4, n.º 14, do GDPR. Como exemplo, as imagens faciais são expressamente mencionadas. Esses dados pertencem à categoria de dados pessoais especiais (também chamados de “dados sensíveis”, segundo o considerando 10, sentença 5 do

[1] Para aprofundamento, conferir o texto do Regulamento de Inteligência Artificial da União Europeia, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689#page=44.71 Acesso: 02/09/2024.

GDPR) e fazem jus à proteção especial, devido aos riscos significativos aos direitos e liberdades fundamentais dos titulares dos dados (considerando 51, sentença 1 do GDPR).

No entanto, não são aplicados os dispositivos normativos sobre o processamento de dados sensíveis para o tratamento das fotografias sem o uso de procedimentos técnicos especiais. Conforme o considerando 51, terceira frase, o tratamento de dados só se enquadra nas categorias especiais de dados pessoais sensíveis se for empregado "por meios técnicos específicos" para identificação ou autenticação inequívoca de uma pessoa física. Além dos dados biométricos, que podem ser coletados e processados por sistemas de reconhecimento facial, os dados pessoais sensíveis incluem a idade do indivíduo, o gênero, a afiliação étnica, política e religiosa etc.

Em princípio, o tratamento de categorias especiais de dados pessoais é proibido. O artigo 9 (1) do GDPR proíbe o processamento de dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, bem como dados genéticos, dados biométricos para fins de identificação inequívoca de uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física. O processamento desses dados somente é permitido nas situações elencadas no artigo 9 (2) do GDPR.

A tecnologia de reconhecimento facial permite que os dados biométricos pessoais sejam tratados mediante processo decisório, o qual pode ser totalmente automatizado e baseado em algoritmos (SCHULZ, 2018). Já o artigo 22 do GDPR, que dispõe que "o titular dos dados tem o direito de não ficar sujeito a uma decisão baseada unicamente no tratamento automatizado", determina, em princípio, a proibição do processamento de dados com base em decisões geradas exclusivamente por meios automatizados. Essa proibição se aplica tanto a instituições públicas, quanto a instituições privadas (MARTINI, 2018).

Nesses termos, o mencionado artigo 22 incide sobre decisões que se baseiam exclusivamente no processamento automatizado de máquinas ("*Automated Decision Making*"), ou seja, sem a participação de uma pessoa física (SCHULZ, 2018). Esse seria o caso, por exemplo, de um "processo de recrutamento on-line" (o chamado "recrutamento eletrônico"), quando não há nenhuma intervenção humana, conforme o considerando 71, primeira frase, do GDPR. (SCHULZ, 2018, Rn. 7).

Além disso, a decisão automatizada deve afetar de forma duradoura os direitos e as liberdades dos titulares dos dados. (MARTINI, 2018, Rn. 7). Daí porque ele somente é aplicado se o uso dessa tecnologia produzir efeitos legais em relação ao titular dos dados ou afetá-lo significativamente.

O objetivo dessa norma é evitar o dano substancial causado a um indivíduo por meio de avaliação exclusivamente automatizada de seus aspectos pessoais e que ensejam consequências legais. É indiferente o fato de a consequência legal gerar vantagens ou desvantagens econômicas. (MARTINI, 2018, Rn.12)

A criação de *profiling*, mediante qualquer forma de tratamento automatizado de dados pessoais e que produza efeitos jurídicos ou afete significativamente uma determinada pessoa para avaliar aspectos pessoais é, a princípio, proibida pelo artigo 22 (1) c/c sentenças 1 e 2 do considerando 71 do GDPR. Esses perfis são utilizados geralmente em análises e previsões de aspectos relacionados ao desempenho profissional, situação econômica, saúde, preferências, interesses pessoais, comportamento, localização, etc., desde que produzam efeitos jurídicos ou afetem significativamente o indivíduo.

No entanto, essa proibição não se aplica irrestritamente, mas alcanças apenas os elaborados de forma exclusivamente automatizada, nos termos do artigo 22 (1) do GDPR (MARTINI, 2018, Rn. 21), ou seja, sem nenhuma intervenção humana.

Os casos excepcionais são expressamente regulados no artigo 22 (2) c/c frase 3 do considerando 71 do GDPR. Como, por exemplo, para a execução ou celebração de um contrato (artigo 22 (2) (a) c/c considerando 71, terceira frase do GDPR). Ou quando há autorização na legislação da União Europeia (UE) ou dos próprios Países-Membros (por meio de "cláusulas abertas"), desde que existam medidas para salvaguardar os direitos, liberdades e os interesses legítimos do titular dos dados - artigo 22 (2) (b) do GDPR.

Também faz parte da exceção quando usado para monitorar e cumprir normas e recomendações de instituições da UE ou órgãos de supervisão nacionais com fins de controle e prevenção de fraudes e evasão fiscal. Ou ainda, para garantir a segurança e confiabilidade de um serviço fornecido pelo controlador (conforme o considerando 71, terceira frase do GDPR) (MARTINI, 2018, Rn. 3).

Outra exceção bastante relevante é o consentimento expresso do titular dos dados (artigo 22 (2) (c) c/c considerando 71, terceira frase do GDPR). A anuência deve ser dada por livre escolha, devidamente informada por meio de uma linguagem clara e simples (MARTINI, 2018, Rn. 28) e para uma finalidade específica e explícita. Ela deve ser dada na forma de uma declaração ou outro ato afirmativo claro, consoante o artigo 4 n.º 11 c/c considerando 43 do GDPR.

Conforme já explicitado, a tomada de decisão automatizada e a criação de perfis (*profiling*) com base em dados pessoais sensíveis são, em princípio, proibidas. No entanto,

podem ser permitidas, desde que preenchidos determinados requisitos – cf. artigo 22 (4) c/c o considerando 71, sentença 7 do GDPR, p. ex., quando houver o consentimento explícito do titular dos dados.

Essas permissões legais não se aplicam a categoria especiais de dados sensíveis, exceto se existirem restrições a elas por meio de regulamentação específica, nos termos da legislação da UE ou do Estado Membro, consoante o artigo 22 (4) c/c artigo 9 (2)(a) do GDPR. Ou ainda caso haja um interesse público significativo, respeitando-se a essência da legislação de proteção de dados e os direitos e interesses fundamentais do titular dos dados, nos termos do artigo 9 (2) (g) do GDPR. Desde que seja necessário e proporcional, como para a investigação ou prevenção de crimes graves (MARTINI, 2018, Rn. 41). Além disso, devem ser implementadas garantias adequadas para proteger os direitos e liberdades bem como os interesses legítimos do titular dos dados (artigo 22, 4, do GDPR).

Por sua vez, o considerando 71, frase 5 do GDPR, estabelece que as crianças não devem ser afetadas por decisões automatizadas. Em relação às crianças, aplica-se uma "proibição relativa" (MARTINI, 2018, Rn. 30). Se a pessoa responsável implementar medidas protetivas adequadas para salvaguardar os direitos pessoais da criança, então o processo de decisão automatizado poderá ser permitido excepcionalmente (MARTINI, 2018, Rn. 30).

Além disso, os artigos 13 (2) (f) e 14 (2) (g) do GDPR impõem obrigações específicas de informação ao titular dos dados, quanto ao uso de processos decisórios automatizados, incluindo a criação de perfis (*profiling*), p. ex., por meio de inteligência artificial. O controlador deve informar ao titular dos dados sobre a existência de tal tecnologia, sobre a lógica envolvida e o escopo e os possíveis impactos do tratamento de dados. As informações devem ser fornecidas "de forma precisa, transparente, compreensível e de fácil acesso, ter linguagem clara e simples (artigo 12 (1), primeira frase, GDPR). Adicionalmente, elas devem ser fornecidas gratuitamente (artigo 12 (5), primeira frase, GDPR).

O titular dos dados tem o direito de ser informado pelo controlador sobre a existência de um procedimento de tomada de decisão exclusivamente automatizada. Além disso, devem ser fornecidos a lógica envolvida e o escopo dos efeitos do processamento, segundo o artigo 15 (1) (h) c/c considerando 63, terceira frase, do GDPR. Ademais, o titular dos dados tem o direito de se opor à criação de perfis, conforme o artigo 21 (1), primeira frase, segunda metade do GDPR.

O uso de novas tecnologias, como reconhecimento facial, pode gerar sérias violações aos direitos e liberdades das pessoas envolvidas. Com isso, faz-se necessária a realização de uma "Avaliação de Impacto" na proteção de dados (art. 35 (1) c/c considerando 91, primeira

frase do GDPR). Essa avaliação tem o objetivo de descobrir quais medidas precisam ser tomadas em caso de tratamento de dados arriscado para estabelecer um estado de conformidade com a proteção de dados (SCHWICHTENBERG, 2020, p. 7).

Recapitulando, o GDPR não regulamenta expressamente o uso de vigilância por vídeo ou com tecnologia de reconhecimento facial, cuja permissão de uso, suas condições e limitações estão regulamentadas no AI Act. Porém, os dados biométricos coletados por procedimentos técnicos especiais são legalmente definidos como dados sensíveis. Além disso, o GDPR estabelece disposições legais sobre procedimento de tomada de decisão exclusivamente automatizada, incluindo a criação de perfis, que pode estar relacionado ao uso da tecnologia de reconhecimento facial. Também foi prevista a obrigação de realizar uma Avaliação de Impacto da Proteção nesses casos que envolvem altos riscos, como o uso de novas tecnologias.

4. ANÁLISE COMPARATIVA E APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM RELAÇÃO AO RECONHECIMENTO FACIAL

A tecnologia de reconhecimento facial ainda não está especificamente regulamentada no ordenamento jurídico brasileiro. Atualmente, está em vigor no Brasil a Lei Geral de Proteção de Dados (LGPD). Nessa perspectiva, cumpre apresentar o panorama da legislação de proteção de dados no Brasil, bem como destacar as normas da LGPD que podem ser relevantes na preservação das garantias constitucionais de privacidade e liberdade na regulamentação do uso do reconhecimento facial.

Depois que Edward Snowden fez revelações importantes sobre as atividades de vigilância internacional do governo norte-americano, as Nações Unidas promulgaram uma resolução sobre a proteção de dados (DÖRR; DIERSCH, 2017, p. 468). Em 2013, a então presidente do Brasil, Dilma Rousseff, e a chanceler alemã, Ângela Merkel, apresentaram a Resolução 68/167 - "O direito à privacidade na era digital" - à Assembleia Geral da ONU, que consagrou o direito à privacidade na Internet como um direito humano fundamental e que deveria estar sujeito às mesmas condições da proteção de dados no mundo off-line (CANTO, 2019, p. 7).

A entrada em vigor do GDPR ocorreu em 2018 na Europa, servindo de inspiração o legislador brasileiro, que promulgou a nova Lei Geral de Proteção de Dados (LGPD), em vigor desde 18 de setembro de 2020 (AGÊNCIA SENADO, 2020). Importantes ajustes na

LGPD foram implementados para evitar que o comércio com países europeus, bem como que a competitividade e a inovação na economia brasileira fossem prejudicados pelo baixo nível de proteção de dados (DUARTE, 2019, p. 7).

Os princípios para o tratamento de dados pessoais estão elencados no artigo 6º da LGPD: o princípio da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não-discriminação, responsabilização e prestação de contas, todos eles com conteúdo expressamente disposto nos incisos I a X do referido artigo 6º.

No GDPR, os dados referentes à face do indivíduo são considerados, expressamente, dados sensíveis. Na LGPD, os dados sensíveis são definidos no artigo 5º, II, como:

> 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.

Diferentemente do GDPR, o artigo 5º, II, da LGPD não apresenta exemplo expresso de dados biométricos. Além disso, o processamento de dados pessoais por meio da tecnologia de reconhecimento facial também pode ocorrer exclusivamente por meio de procedimentos automatizados de tomada de decisão, incluindo a definição de perfis (*profiling*) (ALMADA, 2019, p. 7). Da mesma forma que o GDPR (artigo 22), esse procedimento também é regulamentado pela legislação brasileira, mas o nível de proteção é menor.

Conforme o artigo 20 da LGPD, o titular dos dados tem o direito de solicitar a revisão das decisões exclusivamente automatizadas, incluindo as de criação de perfis. A LGPD estabelece, em seu artigo 20 § 1º, que, a pedido do titular dos dados, há a obrigação do controlador de fornecer informações sobre os critérios e procedimentos utilizados para o tratamento de dados pessoais por meio de decisões automatizadas, observado o sigilo comercial e industrial.

Cabe ressaltar que a LGPD foi alterada pela Lei 13.853/2019, que excluiu o § 3º do artigo 20 da LGPD, o qual trazia a exigência de revisão realizada por pessoa natural. Na versão original, a revisão da decisão só poderia ocorrer por intermédio de uma decisão humana. Após a alteração legal, também se tornou possível que a revisão seja realizada mediante outros procedimentos advindos de outras decisões exclusivamente automatizadas. Na explicação de MARRAFON e MEDON:

> O art. 22 da GDPR europeia é tão sensível a isso que, inversamente à LGPD brasileira, dispõe que o tratamento automatizado de dados deve ser sempre

> excepcional, sendo admitido tão somente nas exceções legais, ressalvado sempre o direito à revisão humana.
>
> O que se quer garantir é que importantes decisões da vida humana não sejam delegadas a máquinas pretensamente neutras, que acabam apenas por reforçar os preconceitos que já existem na sociedade. (MARRAFON; MEDON, 2019)

Assim, enquanto o GDPR proíbe, a princípio, o tratamento de dados sensíveis por meio de processos decisórios exclusivamente automatizados, com exceções definidas, no Brasil, esse tipo de processamento de dados é permitido através do direito de revisão da decisão a pedido do titular dos dados (ALMADA, 2019, p. 6). Isso significa que, por exemplo, o processamento de dados que envolva tecnologia de reconhecimento facial e seja totalmente automatizado é, a princípio, permitido no Brasil.

O titular dos dados tem apenas o direito de solicitar uma revisão, que também pode ser realizada por processos de tomada de decisão exclusivamente automatizada. Este procedimento pode envolver dados especialmente sensíveis, como o perfil biométrico ou associações religiosas, étnicas ou políticas.

Consequentemente, uma medida prejudicial e discriminatória contra o titular dos dados pode ser a consequência desse processamento exclusivamente automatizado, porque o nível de proteção em comparação com o GDPR é menor e uma revisão da decisão por outras decisões igualmente e exclusivamente automatizadas pode não ser suficiente para a proteção dos direitos da pessoa afetada, porque o software pode estar comprometido por erros técnicos ou uma base inadequada para a decisão.

É certo que a LGPD exige que o controlador forneça informações claras e adequadas a respeito dos parâmetros e procedimentos utilizados na tomada de decisão automatizada, quando for solicitada a revisão pelo titular dos dados (artigo 20, *caput* e § 1º). Contudo, esse dever acaba sendo mitigado pela escusa em realizar a revisão sob a justificativa de se observar segredo comercial e/ou industrial (artigo 20, 1º, LGPD).

Nesses casos, a Autoridade Nacional de Proteção de Dados (ANPD) poderá, consoante o artigo 20 § 2º da LGPD, realizar uma auditoria de tratamento discriminatório em decisão automatizada (BIONI; LUCIANO, 2019).

Quanto a essa temática, o GDPR prevê que devem ser fornecidas informações sobre a lógica do processamento automatizado, seu significado e consequências para o controlador em caso de não conformidade (BIONI; LUCIANO, 2019). Nessa linha, o GDPR impõe a obrigação de realizar avaliação de impacto na proteção de dados em casos particularmente arriscados.

Como exemplo, o artigo 35, (3), (a), do GDPR menciona, expressamente, a criação de um perfil pessoal (*profiling*).

No entanto, não existe tal obrigação na legislação brasileira (LGPD). Assim, a obrigação de realizar uma Avaliação de Impacto na proteção de dados no Brasil depende de regulamentação posterior, pois atualmente não há um capítulo específico separado para isso, como nos regulamentos europeus (BIONI; LUCIANO, 2019). Sem essa obrigação, os riscos não são previstos antecipadamente, dificultando que sejam tomadas medidas para salvaguardar os interesses e direitos legítimos dos titulares dos dados (GRÄBER; NOLDEN, 2018, Rn. 2).

No ordenamento jurídico brasileiro, ainda não há previsão legal explícita sobre o uso de sistemas de reconhecimento facial (até a presenta data, o marco regulatório da Inteligência Artificial – PL nº 2.338/2023 – foi aprovado no Senado Federal e aguarda apreciação na Câmara dos Deputados). Portanto, são aplicáveis os dispositivos gerais da LGPD para o uso de biometria facial. Com efeito, inúmeros dispositivos da LGPD podem ser usados para regular o uso dessa tecnologia, por exemplo, no caso de processos exclusivamente automatizados de tomada de decisão, incluindo a criação de perfis. Mas em comparação com o GDPR, o nível de proteção da LGPD é menor.

O uso da tecnologia de biometria facial em locais públicos, proibido pelo AI Act e sem regulamentação expressa no Brasil, fortalece a vigilância e controle, mas ao mesmo tempo, traz riscos às garantias de privacidade e liberdade ao permitir interpretar as expressões faciais do rosto humano e identificar as emoções dos indivíduos (EKMAN; KELTNER, 1970, p. 152), facilitando a manipulação social, além de potencializar tratamentos discriminatórios.

Semelhante ao GDPR, os dados biométricos são considerados dados sensíveis na LGPD, e são especialmente protegidos (artigo 5º, II da LGPD). Igualmente, informações como crenças religiosas e políticas, raça, gênero e outros dados sensíveis são fáceis de coletar através do uso de tal tecnologia. Isso pode resultar em séria violação dos direitos e liberdades fundamentais dos titulares dos dados, e consequente ameaça à privacidade, além de discriminação e processo judicial por diferentes motivos.

Em princípio, segundo o artigo 11 da LGPD, o processamento de dados sensíveis é inadmissível e só pode ocorrer em certos casos excepcionais. O tratamento desses dados depende, por exemplo, do consentimento específico e explícito do titular dos dados e só é permitido com a devida observância do princípio da finalidade (artigo 11, inciso I da LGPD).

Entretanto, essa limitação é praticamente impossível ou ineficaz no contexto de uso de reconhecimento facial em locais de acesso público.

O consentimento deve ser uma manifestação livre, informada e inequívoca para uma finalidade específica, consoante o artigo 5, inciso XII da LGPD. Em geral, a falta de consentimento é explicitamente proibida no tratamento de dados consoante o artigo 8 § 3º da LGPD. O princípio da transparência deve ser considerado mediante a obtenção do consentimento de forma clara e inequívoca (artigo 9º § 1º da LGPD). O processamento de dados especialmente sensíveis sem o consentimento do titular dos dados é admitido somente em hipóteses restritas, caso indispensável (artigo 11, II, LGPD). Por exemplo, se necessário para proteger a vida ou a segurança física da pessoa envolvida, ou de terceiros, será permitido (artigo 11, II, alínea "e", LGPD). No entanto, não são razoáveis o emprego de tais argumentos para permitir o uso do reconhecimento facial de maneira pública e geral.

Por motivos de segurança, a simples vigilância por vídeo e a gravação, sem qualquer tecnologia adicional de reconhecimento facial, poderiam ser usadas, desde que comprovada a necessidade. Basta pensar, por exemplo, na utilização em um local perigoso onde crimes são cometidos constantemente. Nesse caso, esses dados podem ser transferidos diretamente para a autoridade policial com a devida observância das salvaguardas adequadas para a proteção dos dados pessoais dos titulares dos dados.

5. REFLEXÕES SOBRE A POSSÍVEL EXTENSÃO DE MEDIDAS PROTETIVAS COM BASE NAS GARANTIAS CONSTITUCIONAIS À INTIMIDADE E PROTEÇÃO À VIDA PRIVADA

Como cediço, a Constituição brasileira protege os direitos à intimidade e à vida privada (artigo 5º, X, XI, XII, CF/88) e à não-discriminação (artigo 5º, *caput,* VIII, CF/88), os quais se conectam e compõem um núcleo fundamental de garantias da liberdade (artigo 5º, IV, VI, VII, CF/88), uma vez que fomentam a autonomia e rejeitam a intervenção arbitrária pelo Estado ou pelos outros particulares nas determinações pessoais de cada cidadão.

Esses direitos fundamentais irradiam valores normativos que impõem diretrizes interpretativas a toda a ordem jurídica, em especial devido à centralidade da Constituição e sua força normativa irradiante, advinda do processo de constitucionalização do direito.

No entanto, o uso da tecnologia de reconhecimento facial pode constituir uma intrusão grave na vida privada de um titular de dados e, em particular, nos direitos de proteção de dados dos indivíduos, violando seriamente os direitos e liberdades fundamentais estruturantes da ordem constitucional brasileira.

Diante do contexto brasileiro, é aconselhável que os legisladores restrinjam o uso da tecnologia de reconhecimento facial, especialmente por entidades privadas em locais de acesso público e só permitam seu uso em casos excepcionais e devidamente justificados, seguindo a linha preventiva prevista no AI Act europeu.

Os princípios de necessidade, finalidade, adequação e transparência devem ser aplicados como pré-requisitos para o uso de sistemas biométricos faciais. Por exemplo, é desejável que o responsável pela coleta e tratamento dos dados defina com clareza a finalidade do uso da tecnologia de reconhecimento facial antes de implementá-la. Se por algum motivo legítimo, a finalidade tiver que ser alterada, o responsável é obrigado a informar aos titulares dos dados, além de ter que tomar outras medidas essenciais, como, por exemplo, obter novamente o consentimento da pessoa interessada, especificamente para a nova finalidade.

Tão logo a finalidade seja atingida, os dados armazenados devem ser excluídos imediatamente. Isso também se aplica se houver um interesse predominantemente legítimo do titular dos dados. Também é aconselhável permitir a tecnologia de reconhecimento facial em alguns casos com o consentimento explícito dos titulares dos dados para uma finalidade específica, por exemplo, ao comprar mercadorias em uma loja automatizada que usa a tecnologia de Identificação por Radiofrequência – RFID - (CHIANG; YOU; LIN, 2016, p. 1).

Da mesma maneira, é possível permitir o uso sem o consentimento dos titulares de dados quando houver um interesse público substancial, sob a observação de salvaguardas adequadas para garantir os direitos e interesses fundamentais do titular dos dados, como proteção à vida segurança de uma pessoa, em um processo de ponderação tendo em vista cada situação específica e suas circunstâncias.

Se um processo de tomada de decisão exclusivamente automatizada utilizar a tecnologia de reconhecimento facial, incluindo a criação de perfis, e isso ocorrer sem o envolvimento de um ser humano, gerando efeitos legais ou consequências jurídicas adversas significativas para os titulares dos dados, o processamento de dados deverá, em princípio, ser proibido, semelhantemente à regulamentação da União Europeia.

Ao contrário do que está atualmente previsto LGPD brasileira, o direito de revisão da decisão deve seguir o exemplo da GDPR e só poderá ser exercido por pessoas naturais

(MARRAFON; MEDON, 2019). Somente em casos isolados a verificação por meio de um procedimento automatizado deve ser permitida, sendo necessário comprovar que o desempenho dos algoritmos supera o de especialistas humanos e, ainda assim, deve restar preservada a possibilidade de auditoria desses critérios e procedimentos em caso de suspeita de violação a garantias fundamentais.

O titular dos dados deve receber informações suficientes sobre a utilização de novas tecnologias, como a de reconhecimento facial, assim como o tratamento dos seus dados. A pessoa afetada deve ser adequadamente informada sobre a lógica e os efeitos do procedimento automático, como um dever do órgão responsável, independentemente de solitação.

Além disso, semelhante à GDPR, a pessoa responsável deve ser obrigada a fornecer informações essenciais quanto ao uso de tais tecnologias. Deve, então, informar suficientemente os titulares dos dados sobre o escopo completo de utilização do procedimento e suas implicações, antes mesmo de usar o sistema.

Seguindo a linha protetiva, o legislador brasileiro deve, de forma semelhante ao que determina a GDPR, impor ao responsável pelo tratamento de dados a obrigação de realizar uma Avaliação de Impacto na proteção de dados, bem como realizar uma revisão obrigatória. Dessa forma, os riscos potenciais podem ser detectados antecipadamente e as salvaguardas podem ser desenvolvidas e asseguradas para proteger os interesses legais dos envolvidos (GRÄBER; NOLDEN, 2018, Rn. 2)

A adequação com a finalidade e a obrigação de exclusão dos dados armazenados também é significativamente relevante, quando a finalidade especificada tiver sido alcançada e os dados não forem mais necessários. Assim que os dados forem atrelados a uma pessoa específica, o titular dos dados também deve ser informado de maneira clara.

Em outras palavras, é salutar que o legislador brasileiro se inspire nas disposições da GPDR em relação à proteção de dados captados mediante o uso de reconhecimento fácil, a fim de aperfeiçoar a atual LGPD por meio da adoção de medidas de proteção importantes nela inspiradas e devidamente contextualizadas.

6. CONSIDERAÇÕES FINAIS

O objetivo do presente trabalho foi realizar uma análise da proteção de dados obtidas do uso da tecnologia de reconhecimento facial, em especial sob a perspectiva do GDPR e da

LGPD, bem como indicar diretrizes ao legislador brasileiro para possíveis salvaguardas contra o uso não autorizado dessa tecnologia. Para tanto, foram examinadas teorias, doutrinas e leis sobre a proteção de dados entre o Brasil e a Europa.

Ainda que o AI ACT já esteja em vigor na Europa, regulando o uso do reconhecimento facial, demonstrou-se que ainda há espaço para a aplicação do GPDR europeu nas questões específicas de proteção dos dados originados do uso dessa tecnologia. No Brasil, a aplicação da LGPD faz ainda mais sentido, em razão da ausência de legislação vigente acerca da utilização de mecanismos de Inteligência Artificial, ao menos até o momento de elaboração deste estudo.

Assim, como resultado da pesquisa, constatou-se que os regulamentos gerais de proteção de dados devem ser aplicados a fim de assegurar melhores medidas protetivas em relação aos dados, sensíveis ou não, obtidos mediante o uso das ferramentas de reconhecimento facial.

Verificou-se, também, que o legislador brasileiro deve buscar mecanismos de aperfeiçoamento da legislação no país, de modo a ofertar maior proteção e contemplar com maior eficácia as medidas preventivas necessárias ante a progressiva majoração de riscos advinda do acelerado desenvolvimento tecnológico das ferramentas de reconhecimento facial. Tais medidas são necessárias para assegurar a efetividade dos direitos e garantias fundamentais à intimidade, à vida privada, à não-discriminação e demais garantias de liberdade e autonomia da vontade.

REFERÊNCIAS

AGÊNCIA SENADO. **Lei Geral de Proteção de Dados entra em vigor**. 2020. Redação. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Acesso em: 30/09/2023. Citado na página 10.

ALMADA, M. Revisão humana de decisões automatizadas. In: **Pós- Debate**. [s.n.], 2019. Disponível em: https://www.academia.edu/41483884/RevisÃc˘o_humana_de_decisÃµes_automatizadas. Acesso em: 30/09/2023.

BIBO NUNES. Projeto de Lei 4612/2019. **Câmara dos Deputados**, Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1794019&filename=PL%204612/2019. Acesso em: 29/09/2023.

BIONI, B.; LUCIANO, M. O Princípio da Precaução para a Regulação da Inteligência Artificial: Seriam as Leis de Proteção de Dados seu Portal de Entrada? In: FRAZÃO, A.;

MULHOLLAND, C. (Ed.). **Inteligência Artificial e Direito – Ética, Regulação e Responsabilidade**. São Paulo: [s.n.], 2019. Disponível em: https: //brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: 30/09/2023.

BUCHNER; PETRI. DSGVO Art. 6. In: KÜHLING, J.; BUCHNER, B. (Ed.). **Datenschutzgrundverordnung / BDSG**. Bonn: 3. Auflage, 2020. Citado na página 13.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). **Biometrie - Gesichtserkennung**. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf? blob=publicationFile&v=1. Acesso em: 29/09/2023.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). **Grundsätzliche Funktionsweise biometrischer Verfahren**. Disponível em: https://www.bsi.bund.de/dok/6614840. Acesso em: 29/09/2023.

CANTO, M. Made in Surveillance: A regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal. In: BRUNO, F.; NATANSOHN, G. (Ed.). **VI Simpósio Internacional Lavits 2019**: Assimetrias e (in)visibilidades: Vigilância, gênero e raça. Salvador: [s.n.], 2019. p. 1 – 15. Disponível em: http://lavits.org/wp-content/uploads/2019/12/Canto-2019-LAVITS.pdf. Acesso em: 29/09/2023.

CHELLAPPA, R.; SINHA, P.; PHILLIPS, P. J. Face Recognition by Computers and Humans, Computador. **Computer**, IEEE, v. 43, n. 2, p. 46 – 55, 2010.

CHIANG, H.; YOU, W.; LIN, S. Development of smart shopping carts with customer-oriented service. In: **2016 International Conference on System Science and Engineering (ICSSE)**. [S.l.]: IEEE, 2016. p. 1 – 2.

COMISSÃO EUROPEIA. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras Harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. 2021. COM/2021/206 final.** Disponível em: **https://eur-lex.europa.eu/legal-**content/PT/TXT/?uri=CELEX:52021PC0206. Acesso: 29/09/2023.

CORRÊA, V. S.; VALE, G. M. V. Ação econômica e religião: Igrejas como empreendimentos no Brasil. **Revista de Administração Contemporânea**, v. 21, p. 1 – 18, 2017.

COX, I. J.; GHOSN, J.; YIANILOS, P. N. Feature-based face recognition using mixture-distance. In: **Proceedings CVPR IEEE Computer Society Conference on Computer Vision and Pattern Recognition**. [S.l.]: IEEE, 1996. p. 209 – 216.

DIE LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ NIEDERSACH-SEN. **Biometrie und Datenschutz**. 2018. Niedersachsen-Portal. Disponível em: https://lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz- 55984.html. Acesso em: 29/09/2023.

DÖRR, J.; DIERSCH, V. Zur Rechtfertigung von Whistleblowing: Eine ordnungsethische und legitimitätstheoretische Perspektive der Whistleblower-Fälle Carl von Ossietzky und Edward Snowden. **Zeitschrift für Politik**, p. 468 – 492, 2017.

DUARTE, Júlia Tupinambá. **A aplicação da tutela da proteção de dados pessoais no caso das portas interativas digitais do metrô de São Paulo.** Trabalho de Conclusão de Curso (Bacharelado em Direito). Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro: Rio de Janeiro, 2019.

DUDEN - **Dictionary of Medical Terms**. 9. ed. Mannheim: Dudenverlag, 2016.

EKMAN, P.; KELTNER, D. Universal facial expressions of emotion. **California Mental Health Research Digest**, v. 8, n. 4, p. 151 – 158, 1970.

EUROPEAN PARLIAMENT. **EU AI Act: first regulation on artificial intelligence**. 2023. Disponível em: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. Acesso em: 30/09/2023.

GATES, K. A. IDENTIFYING THE 9/11 'FACES OF TERROR' The promise and problem of facial recognition technology. **Cultural Studies**, v. 20, n. 4-5, p. 417 – 440, 2006.

GRÄBER; NOLDEN. BDSG § 67. In: PAAL, B. P.; PAULY, D. A. . (Ed.). **DatenschutzGrund-verordnung / Bundesdatenschutzgesetz**. München: 2. Auflage, 2018.

HIRSCHBERG, T. **Fake Detection bei dem Fingerabdruck**. [S.l.], 2017. Disponível em: https://www.h-brs.de/files/20171215_fbinf_mclab_17-01-08_hirschberg_mk.pdf. Acesso em: 09/11/2020.

IBGE. **Conheça o Brasil - População: Educação.** 2020. Disponível em: https://educa.ibge.gov.br/jovens/conheca-o-brasil/populacao/18317-educacao.html. Acesso em: 29/09/2023.

INSTITUTO IGARAPÉ. **Reconhecimento facial no Brasil. Desde 2011 vem sendo utilizado o Reconhecimento Facial no Brasil.** 2017. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 29/09/2023.

KIRBY, M.; SIROVICH, L. Application of the Karhunen-Loeve procedure for the characterization of human faces 1990, 103. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 12, n. 1, p. 103 – 108, 1990.

LISBOA, V. **Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio**. Rio de Janeiro: Agência Brasil, 2019.

MARRAFON, Marco Aurélio. Medón, Filipe. **Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados.** São Paulo: Revista Consultor Jurídico, 2019. Disponível em: https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd/ Acesso: 19/12/2023.

MARTINI, M. Art. 22. In: PAAL, B. P.; PAULY, D. A. (Ed.). **Datenschutz-Grundverordnung**. München: [s.n.], 2018.

PHILLIPS, P. J.; RAUSS, P. J.; DER, S. Z. FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results. **MD: Army Research Laboratory, 1996.**, Adelphi, 1996. Disponível em: https://www.nist.gov/system/files/documents/2021/04/27/feret3.pdf. Acesso em: 29/09/2023.

PHILLIPS, P. J. *et al.* FRVT 2006 and ICE 2006 large-scale results. **National Institute of Standards and Technology**, NISTIR, v. 7408, n. 1, 2007. Disponível em: https://face-rec.org/vendors/FRVT2006andICE2006LargeScaleReport.pdf. Acesso em: 29/09/2023.

SCHULZ, S. Datenschutz-Grundverordnung. In: GOLA, P. (Ed.). **Datenschutz-Grundverordnung**. Munique: C.H. Beck, 2018.

SCHWICHTENBERG, S. BDSG § 67. In: KÜHLING, J.; BUCHNER, B. (Ed.).

Datenschutzgrundverordnung / BDSG. Bonn: 3. Auflage, 2020. Citado na página 9.

TURK, M.; PENTLAND, A. Eigenfaces for Recognition. **Journal of Cognitive Neuroscience**, v. 3, n. 1, p. 71 – 83, 1991.

ZHAO, W.; CHELLAPPA, R.; PHILLIPS, P. J. Face Recognition: A Literature Survey. **ACM Computing Surveys (CSUR)**, v. 35, n. 4, p. 399 – 458, 2003.