UNIVERSIDADE PRESBITERIANA MACKENZIE

GIOVANNA MONTEIRO DA SILVA

OS LIMITES IMPOSTOS PELO DIREITO AO ANONIMATO E O DIREITO À PRIVACIDADE NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PELOS ENTES PÚBLICOS E PRIVADOS

SÃO PAULO

2023

GIOVANNA MONTEIRO DA SILVA

OS LIMITES IMPOSTOS PELO DIREITO AO ANONIMATO E O DIREITO À PRIVACIDADE NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PELOS ENTES PÚBLICOS E PRIVADOS

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADOR: Dr. Paulo Cezar Neves Junior

SÃO PAULO

2023

GIOVANNA MONTEIRO DA SILVA

OS LIMITES IMPOSTOS PELO DIREITO AO ANONIMATO E O DIREITO À PRIVACIDADE NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PELOS ENTES PÚBLICOS E PRIVADOS

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovada em: ___/____/2023.

BANCA EXAMINADORA

_____

Orientador (a): Dr. Paulo Cezar Neves Junior
Universidade Presbiteriana Mackenzie

_____

Examinador (a): Dr. Danilo Brum de Magalhães Júnior
Universidade Presbiteriana Mackenzie

_____

Examinador (a): Dr. Denise Neves Abade
Universidade Presbiteriana Mackenzie

OS LIMITES IMPOSTOS PELO DIREITO AO ANONIMATO E O DIREITO À PRIVACIDADE NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PELOS ENTES PÚBLICOS E PRIVADOS

Giovanna Monteiro da Silva

Resumo: O estudo realizado no presente trabalho visa analisar a utilização irrestrita do reconhecimento facial pelos entes públicos e privados e a aplicação dos direitos à privacidade e ao anonimato como mecanismos de limitação desta inteligência artificial, sendo um tema de exímia relevância na atualidade, visto se tratar de uma inovação tecnológica recente e que vem sendo mundialmente adotada. Assim, foi identificada a necessidade de regulamentação do reconhecimento facial, respeitando algumas balizas do direito à privacidade e o direito ao anonimato, como a necessidade de consentimento para utilização desta tecnologia, assim como a transparência e o direito de acesso na coleta de dados biométricos, possibilitando que os titulares entendam como os dados vão ser coletados e utilizados. Com isso, se estabelece uma situação de equilíbrio entre os benefícios do reconhecimento facial, como uma maior comodidade e segurança, e a proteção dos direitos individuais da pessoa humana. Para tanto, foram utilizados os métodos e técnicas de pesquisa bibliográfica e documental, de forma qualitativa.

Palavras-chave: Reconhecimento Facial. Direito ao anonimato e à privacidade. Inteligência Artificial. Limites. Regulamentação.

Abstract: The study carried out in this work aims to analyze the unrestricted use of facial recognition by public and private entities and the application of the rights to privacy and anonymity as mechanisms for limiting this artificial intelligence, which is an extremely relevant topic today, given that it is a recent technological innovation that has been adopted worldwide. Thus, the need to regulate facial recognition was identified, respecting some of the guidelines of the right to privacy and the right to anonymity, such as the need for consent to use this technology, as well as transparency and the right of access when collecting biometric data, enabling data subjects to understand how their data will be collected and used. This establishes a balance between the benefits of facial recognition, such as greater convenience and security, and the protection of individual human rights. To this end, we used the methods and techniques of bibliographical and documentary research, in a qualitative manner.

Keywords: Facial Recognition. Right to anonymity and right to privacy. Artificial Intelligence. Limits. Regulation.

Sumário: 1. Introdução. 2. Reconhecimento Facial: Funcionamento, Alcance e Problemas Derivados. 3. O Direito à Privacidade na Era Digital. 4. Um Novo Prisma do Direito ao Anonimato. 5. Limitação ao Reconhecimento Facial: utilização do direito à privacidade e direito ao anonimato na regulamentação. 6. Conclusão. 7. Referências Bibliográficas.

1. Introdução

Com o advento da era digital e a expansão das novas tecnologias, a utilização das inovações tecnológicas vem impactando diretamente a vida das pessoas e da sociedade como um todo, uma vez que têm sido amplamente empregadas pelos órgãos públicos e privados. Tais tecnologias podem trazer diversos benefícios, como mais assertividade e conveniência, além de uma maior sensação de segurança.

Todavia, é inegável que esse sentimento de segurança não é absoluto, já que as novas inteligências artificiais estão sendo utilizadas de maneira indiscriminada, causando uma extrema exposição de nossas vidas, falta de privacidade e um grande senso de impunidade, já que muitas das novas tecnologias sequer possuem uma regulamentação específica, representando um grande risco à liberdade e intimidade dos indivíduos.

Uma das preocupações que cercam o reconhecimento facial é o seu uso pelo Estado e por empresas privadas como um meio de vigilância para monitorar e identificar os cidadãos, tendo em vista que pode resultar em violações dos direitos fundamentais da pessoa humana e levar à proibição desta tecnologia em muitas cidades no mundo, como na Alemanha.

Frisa-se que referida tecnologia depende da coleta de dados que subsidiam a tecnologia biométrica que reconhece as características faciais dos indivíduos, propiciando sua identificação. Por essa razão, é importante refletir sobre como e quais dados pessoais são armazenados pelas empresas privadas e entidades governamentais e até que ponto esses dados são confiáveis ou estão passíveis de manipulação, já que para a obtenção dos referidos dados, a privacidade, liberdade e intimidade dos indivíduos poderão ser violadas, sob o pretexto de uma “maior segurança”.

A partir de um estudo aprofundado da implementação das tecnologias de reconhecimento facial pelos entes públicos e privados, serão avaliados seu funcionamento e seus possíveis efeitos ocasionados na sociedade. Ainda, será realizada uma análise sobre a necessidade ou não de uma legislação que regulamente o presente instituto e a possibilidade de

uso do direito à privacidade e ao anonimato como abalizadores no exercício desta inteligência artificial.

Em linhas gerais, o artigo pretende fomentar a discussão sobre a aplicação das tecnologias de identificação biométrica, tal qual identificar como o direito à privacidade e o direito ao anonimato seriam utilizados como limitadores aptos a garantir os direitos fundamentais dos indivíduos em uma eventual regulamentação do reconhecimento facial. Para tanto, será utilizado o método qualitativo de pesquisa bibliográfica e documental, por meio do qual a investigação bibliográfica levará em conta as principais vertentes jurídicas e entendimentos contemporâneos sobre o reconhecimento facial e seus limites, bem como a aplicação dos direitos ao anonimato e à privacidade como limitadores deste tipo de inteligência artificial.

2. Reconhecimento Facial: Funcionamento, Alcance e Problemas Derivados

Com o desenvolvimento de diversas tecnologias de reconhecimento facial e a coleta de dados pessoais cada vez mais presente na nossa sociedade, muitos países passaram a se pautar em mecanismos de controle social e vigilância, proporcionando uma falsa sensação de segurança aos cidadãos.

Nesse contexto, tais sociedades viabilizaram o desenvolvimento mais acelerado dos sistemas de reconhecimentos faciais baseados em Inteligência Artificial. Esse avanço se justifica na medida que houve um fluxo maior de viajantes internacionais ao redor do globo, notadamente após os ataques terroristas do 11 de Setembro nos Estados Unidos da América. Em virtude desses eventos, as agências governamentais passaram a se utilizar de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas através da identificação dos indivíduos, a fim de garantir que nenhuma ameaça conhecida seja permitida, pois, argumenta-se, isso pode colocar em risco os cidadãos de uma sociedade.[1]

Adentrando no funcionamento das tecnologias de reconhecimento facial, elas se baseiam na captura e análise de características faciais de um indivíduo. Utilizando amplas bases de dados e valendo-se de conexões de internet ultravelozes, as tecnologias de reconhecimento facial identificam e catalogam detalhes de cada indivíduo a fim de processar imagens obtidas

[1] VU, Brandon. **A Technological and Ethical Analysis of Facial Recognition in the Modern Era**, 2018, p. 11-12. Disponível em: https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era. Acesso em: 22 set. 2023.

em um computador, smartphone ou câmera de vigilância; os dados processados podem ser usados, então, para uma extensiva gama de propósitos.[2]

De modo geral, o sistema de reconhecimento facial funciona por intermédio da captação e digitalização das características faciais de um indivíduo, por meio do qual será identificado pontos referenciais, como as proporções entre os olhos, distâncias entre características-chave e contornos faciais, elaborando uma "assinatura facial". Logo após, o software de reconhecimento facial irá comparar o rosto identificado com outras assinaturas faciais previamente coletadas e armazenadas, para uma avaliação da similaridade.

Por fim, para determinar a correspondência entre as assinaturas faciais, o sistema irá identificar o indivíduo associado à assinatura e fornecer as informações pertinentes. No caso de erro na identificação da pessoa, é certo que a similaridade não atendeu aos pontos referenciais previamente fixados.

A tecnologia de reconhecimento facial funciona, portanto, como um comparativo entre a imagem detectada e uma vasta base de dados no qual as próprias imagens assumem um papel de fonte de informação. Temos como exemplo a China, onde mais de 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhões de habitantes do país.[3]

Esta realidade não foge do que vem ocorrendo no Brasil, em que empresas privadas e órgãos públicos utilizam as tecnologias de identificação biométrica facial com o argumento de gerar uma maior segurança na sociedade, mesmo sem qualquer regulação específica para o uso do reconhecimento facial na segurança pública. Destaca-se o projeto "Rio+Seguro"[4], lançado pela prefeitura do Rio de Janeiro, por meio do qual os agentes públicos se utilizaram de GPS e câmeras no patrulhamento, para auxiliar no reforço da segurança.

O que tem gerado grandes preocupações na implementação de inteligências de reconhecimento facial é exatamente as possíveis violações ao direito à privacidade e ao anonimato que essa tecnologia pode propiciar ao ser utilizada pelo Estado e pelos órgãos

---

[2] NABEEL, Fahad. **Regulating Facial Recognition Technology in Public Places**. Centre for Strategic and Contemporary Research, 2019, p. 1-2. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places. Acesso em: 20 jul. 2023.

[3] LENTINO, Amanda. This Chinese facial recognition start-up can identify a person in seconds. **CNBC Disruptor 50**, 17 may 2019. Disponível em: https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html#:~:text=One%20of%20the%20companies%20making,in%20a%20matter%20of%20seconds. Acesso em: 20 out. 2023.

[4] GLOBO.COM. Prefeitura lança projeto de segurança nos bairros de Copacabana e Leme, Zona Sul do Rio. **Bom Dia Rio**, 27 nov. 2017. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/prefeitura-do-rio-lanca-projeto-de-seguranca-em-copacabana.ghtml. Acesso em: 22 set. 2023.

privados como um meio de controle da vida em sociedade. Além disso, os dados biométricos podem ser utilizados de forma indevida, sendo passíveis de manipulação, uma vez que são armazenados em bancos de dados dos quais o cidadão não tem acesso, ou até mesmo alvos de vazamento de informações sensíveis e falhas tecnológicas.

Um caso paradigma no qual houve a captação de dados pessoais biométricos de diversos consumidores e apresenta grandes indícios de violações aos direitos fundamentais dos indivíduos é a ação interposta contra a Concessionária da Linha 4 do Metrô de São Paulo, em razão da utilização de dados dos consumidores por meio das "Portas Interativas Digitais".[5] Tais portas têm a capacidade de discernir emoções, gênero e faixa etária dos indivíduos posicionados diante do sensor, sem qualquer obtenção prévia de consentimento dos usuários.

A grande questão nesse caso é a falta de informações sobre os critérios, condições e propósitos da implementação do sistema de reconhecimento facial, que poderiam ser utilizados para fins publicitários, visto que as "Portas Interativas Digitais" estavam sempre posicionadas acima de uma propaganda. Ou seja, para além da falta de consentimento dos usuários, os seus dados biométricos sensíveis poderiam ser vendidos para terceiros, sem qualquer aviso prévio.

Como resultado, verifica-se uma infinidade de empecilhos que inviabilizam a utilização do reconhecimento facial pelas instituições públicas e privadas, uma vez que essa tecnologia muitas vezes tem seu uso vinculado a uma forma constante de observação e vigilância da vida das pessoas, podendo ocasionar violações aos direitos fundamentais, além de alimentar uma imensa fonte de dados biométricos de uma população que sequer possui a ciência de estar sendo filmada.

3. O Direito à Privacidade na Era Digital

A partir do advento da era digital, o direito à privacidade passou por um extenso processo evolutivo, uma vez que anteriormente estava intrinsicamente ligado ao espaço físico e ao círculo pessoal e íntimo da pessoa humana.

A consolidação da proteção da privacidade teve seu momento seminal com a publicação do intitulado artigo *"The Right to Privacy"* no ano de 1890, pela renomada revista jurídica Harvard Law Review, um distinto periódico associado à prestigiosa faculdade norte-americana, no qual os autores, Samuel D. Warren e Louis D. Brandeis, delinearam os

[5] VIATROLEBUS. **Via Quatro lança portas interativas digitais nas plataformas.** Metrô SP, Assessoria Via Quatro, 12 abr. 2018. Disponível em: https://viatrolebus.com.br/2018/04/viaquatro-lanca-portas-interativas-digitais-nas-plataformas/. Acesso em: 8 nov. 2023.

argumentos e fundamentos legais que lançaram as bases para o reconhecimento do direito à privacidade nos Estados Unidos e, por extensão, em muitos outros sistemas legais ao redor do mundo.

É certo que nos anos de 1890, os Estados Unidos passavam por um cenário caótico de avanços tecnológicos, como a popularização da fotografia instantânea e a disseminação de jornais e revistas, que trouxeram consigo desafios para a privacidade individual. Com o desenvolvimento da fotografia instantânea, tornou-se mais fácil o registro de imagens em tempo real, e esse ponto, alicerçado ao jornalismo sensacionalista que encontrava-se em ascensão, propiciou a invasão de espaços privados e a exposição de detalhes da vida pessoal das pessoas, sem seu consentimento, buscando capturar imagens de pessoas em momentos de vulnerabilidade ou luto, o que causava angústia e indignação pública, unicamente com o intuito de aumentar suas vendas através de histórias chocantes e fotos sensacionalistas.

Portanto, é inegável que o artigo *"The Right to Privacy"* e o fatídico ano de 1890 marcaram significativamente a história e consolidação da privacidade individual, contribuindo para diversos debates acadêmicos e jurisprudenciais, que ao longo dos anos têm desempenhado um papel fundamental na formação das leis e práticas relacionadas à privacidade e proteção de dados pessoais.

No seu conceito inaugural, portanto, o direito à privacidade estava intrinsecamente ligado à salvaguarda da vida íntima, familiar e pessoal de cada indivíduo. Primordialmente, representava um direito à intimidade contra as interferências do Estado e de outros cidadãos, impondo apenas a obrigação de se abster de interferir. Todavia, com o aumento das tecnologias e o compartilhamento de dados, esse conceito passou a ser insuficiente para a proteção do indivíduo. O intercâmbio de informações, onde há o recolhimento, armazenamento e utilização dos dados pessoais, impulsionaram o avanço do direito à privacidade, abrangendo também a proteção de dados pessoais, como a biometria.

Atualmente, a privacidade encontra-se em expansão, a fim de proteger dados pessoais, como características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa, informações presentes na internet e acompanhar a evolução tecnológica. Assim, o direito à privacidade transcende a questão de apenas “ser deixado em paz” e abrange deveres de caráter positivo por parte dos indivíduos e do Estado.

A partir disso, verifica-se o caráter positivo da privacidade, em que cada indivíduo possuí o direito de obstar a intromissão de estranhos em sua esfera íntima e privada e de determinar como suas informações pessoais são coletadas, armazenadas e utilizadas, além de impor ao Estado a implementação de medidas aptas a garantir a privacidade dos cidadãos,

protegendo-os contra intromissões tanto de particulares quanto de outros Estados. Isso destaca a importância das leis de privacidade, regulamentações e órgãos reguladores na proteção dos direitos individuais.

Nessa toada, o direito à privacidade é assegurado como um direito fundamental na Constituição Federal Brasileira, estando previsto no art. 5º, inciso X da Constituição Federal de 1988, que dispõe sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa. Além da Carta Magna, a Lei Infraconstitucional nº 12.965/2014, mais conhecida como o "Marco Civil da Internet", também assegura a proteção à privacidade em seu art. 3º, inciso II e em seu art. 7º, inciso I, sendo que esse último garante aos usuários da internet o direito à inviolabilidade da intimidade e da vida privada, inclusive o sigilo das comunicações online, salvo por ordem judicial.

Todavia, tanto a Constituição Federal quanto a legislação brasileira não trazem um conceito objetivo e detalhado a respeito do direito à privacidade, deixando tal conceituação para a jurisprudência e a doutrina jurídica. A inexistência de uma definição precisa em relação à privacidade reflete a natureza complexa e multifacetada desses conceitos, os quais podem sofrer variações em função do contexto e das mudanças sociais e tecnológicas.

Por outro prisma, como destaca Leonardi, ao longo do século XX, o conceito de privacidade passou por uma série de desenvolvimentos e interpretações que ajudaram a moldar o entendimento desse direito fundamental. Essas conceituações devem ser plurais e não taxativas, sendo que “o método tradicional de conceituar a privacidade [...] dificulta a compreensão do que está ou não incluído no seu âmbito de proteção, prejudicando a valoração da dimensão de seu peso, em caso de colisão com outros direitos ou interesses”.[6]

Já para André de Carvalho Ramos:

> [...] o direito à privacidade consiste na faculdade de se optar por estar só e não ser perturbado em sua vida particular, formando uma esfera de autonomia e exclusão dos demais e evitando que, sem o consentimento do titular ou por um interesse público, nela se intrometam terceiros.[7]

Mesmo sendo trazido prioritariamente em seu viés negativo na lei constitucional, o direito à privacidade está em constante mudança, acompanhando os nuances da sociedade e sem a sua devida proteção, qualquer outro direito da personalidade corre sérios riscos de se

---

[6] LEONARDI, Marcel. **Tutela da privacidade na internet.** 1.ª ed. São Paulo: Saraiva, 2011. p. 78.
[7] RAMOS, André de Carvalho. **Curso de direitos humanos**. 9.ª ed. São Paulo: Saraiva, 2016. p. 565.

tornarem irrelevantes para o titular, pois a intrusão na esfera pessoal pode comprometer a autonomia e a dignidade do indivíduo.

Portanto, o direito à privacidade deve ser assegurado como um patamar mínimo invulnerável que todos devem desfrutar, merecendo atenção e proteção cuidadosa de todos os atores sociais, incluindo órgãos governamentais, empresas e a própria sociedade como um todo.

4. Um Novo Prisma do Direito ao Anonimato

No ordenamento jurídico brasileiro, o anonimato encontra-se intimamente ligado à liberdade de expressão, sendo limitado pelo artigo 5º, inciso IV da Constituição Federal de 1988, o qual dispõe que "é livre a manifestação do pensamento, sendo vedado o anonimato".

Essa vedação foi pensada como uma forma de viabilizar a responsabilidade que indivíduos podem causar ao expressarem sua opinião, como danos à honra e à imagem de terceiros. Como Edson Ricardo Saleme leciona: "O que se quer alcançar com a vedação do anonimato é a possibilidade do abuso de direito na manifestação de pensamento, com violação dos direitos da personalidade de terceiros, tais como: vida privada, honra ou intimidade."[8]

Seguindo esse pensamento, a identificação passou a ser indissociável à liberdade de expressão, uma vez que se o anonimato fosse permitido nessa situação, a impunidade se tornaria algo comum. Assim sendo, a "liberdade de manifestação do pensamento tem seu ônus, tal como o de o manifestante identificar-se, assumir claramente a autoria do produto do pensamento manifestado, para, em sendo o caso, responder por eventuais danos a terceiros".[9]

Em contraposição, embora esteja expressa a vedação do anonimato no texto constitucional, é possível verificar no ordenamento jurídico brasileiro que a proibição ao anonimato não é absoluta, possuindo diferentes oportunidades em que a anonimização é empregada para proteger direitos e interesses defendidos na Constituição Federal.

Um grande exemplo de ampliação do direito ao anonimato é o art. 14 da Constituição Federal de 1988, que assegura aos indivíduos que a soberania popular será exercida pelo voto direto e secreto, com o intuito de evitar vícios no seu direito de escolha. No desenrolar da Ação Direta de Inconstitucionalidade (ADI) n.º 4543, por exemplo, o Plenário do Superior Tribunal Federal firmou entendimento de que "A garantia da inviolabilidade do voto impõe a necessidade de se assegurar ser impessoal o voto para garantia da liberdade de manifestação, evitando-se coação sobre o eleitor".

---

[8] SALEME, Edson Ricardo. **Direito constitucional**. 4.ª ed., rev. e atual. São Paulo: Manole, 2021. *E-book*, p.139.
[9] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 36.ª ed. São Paulo: Malheiros, 2012, p. 245.

Já a Lei de Acesso à Informação (Lei nº 12.527/2011), prevê a proteção do sigilo da fonte quando se trata de informações que podem expor o denunciante a riscos ou retaliações indevidas. Outro caso passível de aplicação do direito ao anonimato concerne nas denúncias de irregularidades ou crimes, sendo o sigilo um grande alicerce para preservação e proteção do denunciante.

Neste sentido, quando analisado sob uma ótica ampliada, o anonimato transcende sua vedação e revela-se como um importante instrumento de otimização e proteção de direitos fundamentais dos indivíduos, como a liberdade de expressão, a privacidade e a proteção aos dados pessoais.[10]

É relevante mencionar que o ambiente na qual estava inserida a Constituição de 1988 é muito diferente dos dias atuais, uma vez que a internet tinha recém-chegado ao Brasil e não possuía essa presença na vida das pessoas, além de não existir uma preocupação excessiva com a proteção dos dados pessoais. Assim, a vedação ao anonimato pode ser vista como uma medida destinada a promover a responsabilidade individual na comunicação pública, que muitas vezes eram compartilhadas por meio de rádio, televisão e jornais.

No entanto, o anonimato passou a ser visto de uma forma complexa com as novas tecnologias chegando cada vez mais rápido no mercado mundial, além do aumento do compartilhamento de dados pessoais, já que constantemente cedemos voluntaria e involuntariamente nossos dados pessoais ao governo e instituições privadas.

Conforme Miriam Wimmer e Lucas Borges de Carvalho[11], o direito ao anonimato possui uma fundamentação constitucional de natureza multidimensional, englobando três fundamentos essenciais, quais sejam: (i) liberdade de expressão; (ii) integridade física e moral; e (iii) privacidade e proteção de dados pessoais. Assim, quando associado a essas três perspectivas, o anonimato passa a representar-se como um meio viabilizador de direitos fundamentais.

Seguindo a análise dos referidos autores, o primeiro fundamento, plenamente conhecido e utilizado, refere-se à capacidade de exercer a liberdade de expressão, mesmo que de forma anônima. Para fins ilícitos, há a vedação ao anonimato no âmbito da liberdade de expressão, porém o anonimato pode e deve ser utilizado de forma lícita, garantindo a

---

[10] QUEIROZ, Rafael Mafei Rabelo. Liberdade de expressão na internet: a concepção restrita de anonimato e a opção pela intervenção de menor intensidade. **Suprema – Revista de Estudos Constitucionais**, v. 1, n. 1, p. 241-266, jan./jun. 2021. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/24/21. Acesso em: 22 set. 2023.

[11] WIMMER, Miriam; CARVALHO, Lucas Borges de. O papel e os limites do anonimato: em busca de uma interpretação constitucionalmente adequada. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 27, n. 2, p. 1-16, abr./jun. 2022. Disponível em: https://ojs.unifor.br/rpen/article/view/13041/6855. Acesso em: 22 set. 2023.

possibilidade de manifestação de qualquer indivíduo. Isso é fundamental para promover a diversidade de vozes na sociedade, garantindo que as pessoas não se sintam inibidas em expressar suas opiniões por medo de retaliação ou estigmatização. O segundo fundamento está intimamente relacionado com o primeiro, na medida que busca a salvaguarda da integridade física e moral, não apenas de indivíduos isolados, mas também de grupos de pessoas que, por exemplo, possam ser alvos de ameaças ou retaliações devido às suas manifestações públicas.

Por fim, o último fundamento trazido por Miriam Wimmer e Lucas Borges de Carvalho encontra-se vinculado à privacidade e à proteção de dados. Como visto anteriormente, o direito à privacidade está intimamente ligado a não violação da vida privada, leia-se a intimidade. Já com relação à proteção de dados, o anonimato é um meio funcional para que o indivíduo escolha se quer ou não compartilhar seus dados pessoais, fortalecendo a questão do consentimento no tratamento de dados.

Assim, o direito ao anonimato é uma ferramenta legítima que permite às pessoas protegerem sua privacidade e controlarem o uso de suas informações pessoais por terceiros, resguardando o seu direito de permanecer no anonimato e proteger os seus dados, como uma simples biometria.

A Suprema Corte Americana, inclusive, decidiu por unanimidade no caso McIntyre v. Ohio Elections Comm'n[12] que o anonimato é um importante direito fundamental decorrente da liberdade de expressão, enfatizando a importância do anonimato como um componente essencial da liberdade de expressão política nos Estados Unidos.

Da mesma forma, o Tribunal Constitucional Chileno já entendeu pela necessidade do anonimato em espaços públicos na "23ª sentença do Rol n° 1894-2011-CPR"[13], de 12 de julho de 2011, sob o fundamento de que a privacidade pode ocorrer não apenas em lugares mais reservados, como também em espaços públicos onde se realizam atos concretos com a intenção de subtrair-se à observação alheia.[14]

Alan Westin em seu livro *Privacy and Freedom*[15] defende que o conceito de privacidade individual é uma disseminação de diferentes estados de privacidade que as pessoas

---

[12] UNITED STATES. U. S. Supreme Court. **McIntyre v. Ohio Elections Comm'n, 514 U.S. 334**. Argued: 12 oct. 1994. Decided: 19 apr. 1995. Disponível em: https://supreme.justia.com/cases/federal/us/514/334/. Acesso em: 22 set. 2023.

[13] DERECHO CHILE. **T. Constitucional sobre a constitucionalidade do registo privado de "cibercafés". Acórdão n.º 1894-2011-CPR**, de 12 de julho de 2011. Disponível em: https://derecho-chile.cl/sentencia-del-tribunal-constitucional-sobre-la-constitucionalidad-de-un-registro-privado-de-los-cibercafes/. Acesso em: 22 set. 2023.

[14] MONREAL, Eduardo Novoa. **Derecho a la vida privada y libertad de información**: **un conflicto de derechos**. 2.ª ed. México: Siglo Veintiuno, 1981, p 51 e 202-204.

[15] WESTIN, Alan; SOLOVE, Daniel. **Privacy and Freedom**. NewYork: Ig Publishing, 1967, p. 31.

podem experimentar em suas vidas. Westin identifica, portanto, quatro estados básicos de privacidade: solidão, intimidade, anonimato e reserva. Neste contexto, o estado de anonimato se apresenta como um componente fundamental da privacidade individual.

No estado de anonimato, o indivíduo se encontra e se expressa em locais públicos, porém, possui a expectativa de que sua identidade permanecerá oculta, não sendo identificado pessoalmente, mesmo que esteja consciente de que está sendo observada. Assim, embora o indivíduo esteja em um local público, ainda resta um certo grau de privacidade vinculado a ele. Primeiramente, porque grande parcela das pessoas que estão naquele local nunca vai saber quem é determinado indivíduo, desde que não seja uma figura pública, e segundamente pois o seu anonimato está resguardado.

É nesse aspecto que o anonimato precisa ser notadamente conhecido e aplicado, uma vez que passou a assumir uma considerável posição na era da hiperconectividade e do rápido avanço tecnológico, como um contrapeso essencial contra a potencial vigilância estatal e o uso abusivo de informações por empresas privadas. Assim, o simples fato de ter sua identidade violada pode propiciar que seus dados pessoais fiquem vulneráveis e suscetíveis a abusos.

Como se verifica no caso alemão, o novo governo se comprometeu a banir o reconhecimento facial público e outras formas de vigilância biométrica. O anúncio foi feito por meio do acordo de coalizão entre os partidos Social-Democrata (SPD), Os Verdes e Liberal Democrático (FDP), sendo que no documento afirma-se que os partidos defendem que "o direito ao anonimato, tanto nos espaços públicos quanto na internet, deve ser garantido".[16]

O que se apresenta, portanto, é a dicotomia entre a proibição do anonimato e a sua utilização como uma garantia do sigilo dos dados de identificação. A concepção de anonimato não deve mais estar entrelaçada como uma restrição ao direito de livre expressão, mas como um meio viabilizador de direitos fundamentais.

5. Limitação ao Reconhecimento Facial: utilização do direito à privacidade e o direito ao anonimato na regulamentação

Como observado anteriormente, as tecnologias de vigilância e reconhecimento facial passaram a ser um elemento comum no mundo hiperconectado atual e possuem o condão de impactar significativamente a maneira como vivemos nossas vidas. Como afirma Norris, a

[16] NOYAN, Oliver. New German government to ban facial recognition and mass surveillance. **Euractiv Intelligence**, 1.º dez. 2021. Disponível em: https://www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/. Acesso em: 22 set. 2023.

transição para uma sociedade digital e conectada resultou em um aumento significativo da sociedade de vigilância.[17]

Dentro desse contexto, o reconhecimento facial pode ser utilizado de forma benéfica na sociedade, sendo um grande alicerce no monitoramento e segurança pública, fornecendo uma maior comodidade e sensação de segurança ao indivíduo, já que permite a identificação de pessoas de forma rápida e precisa, auxilia na prevenção de crimes, dissuadindo ações criminosas em razão da presença das câmeras de reconhecimento facial e inibe a prática de fraudes, tendo em vista que o reconhecimento facial pode ser empregado para identificação de indivíduos em transações financeiras.

Um exemplo notável de aplicação do reconhecimento facial trazendo resultados benéficos é o Estado chinês, onde esse tipo de tecnologia desempenhou um papel essencial na manutenção de níveis mais baixos de criminalidade. Os indicadores como o número de homicídios por 100 mil habitantes, na China são notavelmente inferiores aos índices da Europa Ocidental[18], como França e Reino Unido, sendo equivalentes ao nível de segurança da Suíça, com aproximadamente 0,7 homicídios por grupo de 100 mil pessoas. Esses números contrastam significativamente com a situação no Brasil, onde o indicador de homicídios por 100 mil habitantes é alarmantemente elevado, atingindo 29,8/100 mil, conforme dados do Instituto de Pesquisas Econômicas Aplicadas (IPEA).

Todavia, é importante lembrar que o uso do reconhecimento facial também gera preocupações legítimas sobre privacidade, proteção de dados e *surveillance*, implicando consequências na expectativa de privacidade, anonimato e autonomia individual. Rodotà, nesse sentido, reconhece diversas razões que justificam a necessidade de utilização de todas as oportunidades oferecidas pelas novas tecnologias com o propósito de salvaguardar a sociedade contra a criminalidade, devendo-se buscar o equilíbrio entre a perspectiva individualista da privacidade e a satisfação das exigências da sociedade.[19]

A utilização do reconhecimento facial pode e deve ser implementada quando necessária aos órgãos públicos e privados. Todavia, o grande desafio das tecnologias de

---

[17] NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: LYON, David. **Surveillance as social sorting: privacy, risk, and digital discrimination**. New York: Routledge, 2003, p. 253.

[18] ZMOGINSKI, Felipe. A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial. **Tilth Uol – Inteligência Artificial**, 19 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm?cmpid=copiaecola. Acesso em: 22 set. 2023.

[19] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008, p. 147.

vigilância decorre principalmente do seu emprego de forma discricionária e dos possíveis abusos por parte de entidades governamentais e corporativas com relação à manipulação de dados.

A capacidade de identificar instantaneamente um indivíduo por meio de suas características faciais, a captura e o acesso às quantidades significativas de dados, inclusive dados sensíveis, levanta questões importantes relacionadas ao direito à proteção de dados e à privacidade, uma vez que as próprias imagens passaram a ser uma fonte de informação. O avanço tecnológico, representado pelo reconhecimento facial, tem o potencial de desafiar os princípios fundamentais que sustentam esses direitos individuais.

Diante dessa expansão das ferramentas de análise e coleta massiva de informações pessoais por parte de empresas e órgãos governamentais, muitas vezes sem a devida transparência e sem conexão direta com o propósito original da coleta, dados aparentemente irrelevantes, que não estão relacionados a erros ou condutas inadequadas, podem ser agregados, possibilitando a realização de inferências sobre um indivíduo. Isso inclui a criação de perfis, a previsão de comportamentos e a revelação de informações sensíveis, conforme observado por Solove.[20]

Atualmente, o uso do reconhecimento facial por parte do Estado, mesmo com o objetivo de intensificar a segurança, permite a ele que observe tudo e a todos, sem o indivíduo saber se está, de fato, sendo gravado, propiciando o controle da sociedade, pelo simples temor de estarem sob observação. A operacionalização desta tecnologia passa despercebida, já que não há a necessidade de contato humano-máquina.

Assim, corpos anônimos são transformados em sujeitos digitais, sendo identificados e relacionados às suas personas virtuais constantes nas bases de dados eletrônicas, acarretando o cerceamento do direito dos cidadãos de terem sua privacidade preservada, bem como o direito da pessoa de escolher aquilo que está disposta a revelar aos demais.[21] Por outro lado, se questiona se há um direito à privacidade em lugares públicos, onde se apresenta uma expectativa de se manter no anonimato.

Em virtude da instalação de tecnologias de reconhecimento facial em ambientes públicos e da facilidade de acesso a dados pessoais, a preservação do anonimato se revela uma

---

[20] SOLOVE, Daniel J. **Understanding Privacy**. Harvard University Press, GWU Law School Public Law Research Paper n.º 420, 13 jul. 2014, p. 766-777. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888. Acesso em: 20 out. 2023.

[21] NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: LYON, David. **Surveillance as social sorting: privacy, risk, and digital discrimination**. New York: Routledge, 2003, p. 278.

empreitada complexa, já que estar sob constante observação em locais públicos limita a sensação de relaxamento e liberdade que as pessoas procuram, especialmente em espaços abertos. Contudo, todo cidadão desfruta de um certo grau de anonimato, mesmo que se encontre em lugares públicos, uma vez que a maioria das pessoas ao seu redor geralmente não tem informações sobre sua identidade, a menos que seja uma pessoa amplamente reconhecida ou pública.

Assegurar o anonimato significa que uma pessoa pode se envolver em atividades públicas enquanto compartilha espaços com outras, ciente de que está sob observação, mas que não espera ser identificada ou reconhecida. Assim, o anonimato é um mecanismo legítimo para a proteção da privacidade e dos dados pessoais no emprego das tecnologias de reconhecimento facial, possuindo o condão de reduzir os riscos de terceiros utilizarem indevidamente seus dados pessoais, os quais podem escolher consentir com o compartilhamento ou a utilização de sua biometria.

Ou seja, no contexto do direito à privacidade, cabe ao indivíduo a prerrogativa de decidir se deseja ou não compartilhar seus conjuntos de dados, informações, expressões e referências pessoais, e, caso opte pela divulgação, tem o direito de determinar quando, de que maneira, onde e para quem realizar essa divulgação.[22] Proporcionar a transparência no processamento de dados é fundamental para garantir as liberdades individuais e aumentar a confiabilidade dos usuários no uso de sistemas de reconhecimento facial, tanto em lugares públicos como privados.

É nesse aspecto que caberia a limitação da inteligência de reconhecimento facial, enfocando a transparência na coleta de dados pessoais por meio da vigilância e garantindo o acesso do indivíduo a esses dados, a fim de equilibrar os benefícios do reconhecimento facial com as preocupações relacionadas à privacidade e ao direito ao anonimato. A transparência na coleta de dados é essencial para garantir que as pessoas estejam cientes de como suas informações estão sendo obtidas e utilizadas. Isso implica no dever das organizações, sejam elas governamentais ou privadas, em comunicar claramente os propósitos da coleta de dados por meio do reconhecimento facial, bem como os métodos empregados. A divulgação transparente permite que as pessoas tomem decisões informadas sobre o consentimento ou a recusa de ter seus dados capturados.

Nesse caso, é fundamental que tais avisos estejam redigidos em linguagem clara e compreensível no próprio local da utilização da tecnologia, de modo a facilitar a compreensão

[22] TAVARES, André Ramos. **Curso de Direito Constitucional**. 10.ª ed. São Paulo: Saraiva, 2012, p. 529-535.

dos fins para os quais os dados serão utilizados, como por exemplo, na autenticação de pessoas e na segurança dos sistemas. Isso pode incluir a exposição de avisos em locais visíveis e a disponibilização de links para políticas de privacidade relacionadas em sites e aplicativos. Ou seja, para que o reconhecimento facial esteja de acordo com a Lei Geral de Proteção de Dados, é necessário priorizar a transparência na coleta dos dados, oportunizando que os usuários tenham acesso a todas as informações pertinentes ao sistema de vigilância.

A inclusão desses avisos prévios não apenas cumpre as exigências legais de transparência, mas também aumenta a confiança do público em relação ao uso responsável da tecnologia de reconhecimento facial, já que eles podem procurar se politizar sobre esses sistemas e se proteger de eventuais abusos.

Além disso, é de suma importância proteger o direito fundamental de acesso dos indivíduos aos seus próprios dados. Isso porque, as pessoas devem ter a capacidade de acessar, revisar e, se necessário, corrigir as informações que foram coletadas sobre elas. Esse controle sobre seus dados pessoais confere aos indivíduos um maior grau de autonomia sobre suas informações e lhes permite tomar medidas viáveis a proteger sua privacidade, se assim desejarem. Como Rodotà defende, o direito de acesso não é apenas um meio para as pessoas adquirirem informações, mas também um instrumento que os indivíduos podem mobilizar para promover efetivamente a implementação de princípios relacionados à proteção de dados pessoais.[23]

Rodotà ainda argumenta que é necessário conceder às pessoas o poder de ter um controle direto e constante sobre as entidades que coletam informações, independentemente de qualquer violação de seus direitos.

Dessa forma, a fim de resguardar o direito ao anonimato e o direito à privacidade, o reconhecimento facial deve respeitar algumas balizas norteadoras desses direitos, como garantir ao indivíduo a oportunidade de consentir com a implementação dessas tecnologias de vigilância, bem como assegurar que ele tenha acesso à realização do processo de coleta de biometria. Além disso, é imperativo que as práticas de coleta de dados biométricos sejam transparentes e acessíveis, permitindo que os indivíduos compreendam plenamente de que forma esses dados estão sendo coletados e como serão utilizados. Estas salvaguardas são essenciais para equilibrar os benefícios potenciais dessas tecnologias com a proteção dos direitos individuais à privacidade e ao anonimato.

---

[23] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008, p. 60.

Outrossim, no que concerne ao direito à privacidade, Rodrigo Natálicio dos Santos e Cristiane Helena de Paula Lima Cabral[24] atestam o crescente fortalecimento nas práticas de segurança e privacidade de dados em todo o mundo, como sendo um reflexo da nossa crescente dependência da tecnologia e da coleta de informações pessoais. Assim, diversas regulamentações têm sido desenvolvidas com o objetivo de proteger os indivíduos e seus dados. Essas regulamentações são uma resposta direta à preocupação tanto dos órgãos reguladores quanto das empresas e dos cidadãos em relação aos riscos associados à manipulação indevida de dados pessoais.

Regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil representam exemplos de esforços substanciais para assegurarem que as organizações que coletam, processam e armazenam informações pessoais, os faça de forma ética e transparente. Essas normas seguem o mesmo sentido anteriormente trazido, do direito de acesso e controle aos dados que são coletados, permitindo que estejam cientes de como suas informações estão sendo utilizadas e, frequentemente, conferindo-lhes o direito de consentir ou recusar o uso de seus dados. Isso não apenas protege os direitos individuais, mas também fomenta a confiança do público nas empresas e instituições que operam em um ambiente digital em constante evolução.

Assim, sem uma regulamentação específica sobre a utilização do reconhecimento facial no Brasil, seu uso pode acarretar problemas irreversíveis, propiciando falhas algorítmicas e violações aos direitos fundamentais dos indivíduos. Como se observa no exemplo da cidade de Curitiba/PR[25], a prefeitura curitibana vem se valendo do reconhecimento facial, instalado em rodoviárias da capital, cemitérios municipais e até monitorando entradas e saídas da cidade, identificando veículos irregulares ou com alerta de furto ou roubo, mesmo sem lei municipal específica regulando o uso da tecnologia.

A utilização irrestrita do reconhecimento facial em Curitiba levou a vereadora Carol Dartora a apresentar um Projeto de Lei com o intuito de limitar a implementação dessa tecnologia na cidade paranaense. No entanto, o projeto foi arquivado com a justificativa de que

---

[24] SANTOS, Rodrigo Natálicio dos; CABRAL, Cristiane Helena de Paula Lima. Reconhecimento Facial: Análise a partir da Constituição Brasileira e da Lei Geral de Proteção de Dados. **Revista Brasileira de Direito e Gestão Pública**, v. 8, n. 5, p. 1127–1142, 2021. Disponível em: https://www.gvaa.com.br/revista/index.php/RDGP/article/view/8599. Acesso em: 23 abr. 2023.

[25] COLOMBO, Mariah. Curitiba usa reconhecimento facial como ferramenta na segurança pública sem ter regulação específica: 'Sociedade de controle', critica especialista. **G1 – Paraná RPC**, 2 out. 2023. Disponível em: https://g1.globo.com/pr/parana/noticia/2023/10/02/curitiba-usa-reconhecimento-facial-como-ferramenta-na-seguranca-publica-sem-ter-regulacao-especifica-sociedade-de-controle-critica-especialista.ghtml. Acesso em: 22 out. 2023.

a medida era desproporcional, pois proibia o uso dessas tecnologias de maneira generalizada, sem levar em consideração possíveis necessidades do Poder Público.

Além disso, encontra-se em tramitação o Projeto de Lei n° 2338/2023, chamado de Marco Legal da Inteligência Artificial, o qual adota uma abordagem regulatória baseada em riscos e direitos, estabelecendo uma regulação assimétrica para os agentes regulados. Isso significa que há obrigações mais rigorosas para os agentes ou operações consideradas de alto risco, em consonância com a abordagem adotada na União Europeia através do EU AI Act.

O texto também estipula que o uso de sistemas de IA para identificação biométrica à distância pelo poder público[26], de maneira contínua e em locais públicos, somente pode ser realizado com base em uma legislação específica e autorização judicial. Isso deve estar relacionado a casos de atividade criminal individualizada, incluindo: a) a perseguição a condenados com pena de reclusão superior a 2 anos; b) a busca por vítimas de crimes ou pessoas desaparecidas; e c) a investigação de crimes em flagrante. Portanto, o emprego de reconhecimento facial em áreas públicas, como as encontradas em *smart cities*, deve ser abordado com cautela, levando em consideração, principalmente, preocupações relacionadas ao potencial de viés algorítmico.

O Comitê Europeu para a Proteção de Dados (EDPB) também adotou orientações sobre o uso da tecnologia de reconhecimento facial no contexto da aplicação da lei. Essas orientações oferecem instruções aos legisladores nacionais e da União Europeia, e também às autoridades encarregadas da aplicação da lei, com diretrizes sobre a aplicação e utilização dos sistemas de reconhecimento facial.

Em tais diretrizes, o EDPB[27] destacou determinados casos que violam o *General Data Protection Regulation* (GDPR), os quais devem ser evitados: (i) a utilização do reconhecimento facial em espaços acessíveis ao público; (ii) a classificação de titulares em grupos com base em etnia, gênero, orientação política ou sexual ou outros motivos de discriminação; (iii) a análise biométrica para inferir as emoções dos indivíduos e; (iv) o uso de banco de dados que coletam imagens online, especialmente aquelas provenientes de redes sociais.

É imprescindível considerar essas instruções em potenciais normas de reconhecimento facial no Brasil, já que qualquer um dos casos supramencionados pode ocasionar abusos ao

---

[26] LIBERMAN, Tania. A regulamentação da IA no Brasil. **Jota**, 6 ago. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulamentacao-da-ia-no-brasil-06082023. Acesso em: 22 set. 2023.

[27] EUROPEAN DATA PROTECTION BOARD. **O CEPD adota orientações sobre o cálculo das coimas e a utilização da tecnologia de reconhecimento facial no domínio da aplicação da lei**, Bruxelas, 16 may 2022. Disponível em: https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-calculation-fines-guidelines-use-facial-recognition_pt. Acesso em: 20 out. 2023.

direito à privacidade e ao anonimato. Um especial cuidado deve ser dado nos casos de inferência de emoções dos indivíduos, já que tais informações podem ser exploradas para fins publicitários, bem como na utilização de banco de dados contendo imagens online, uma vez que indivíduos que compartilham suas fotos em redes sociais não esperam que estas imagens sejam utilizadas como meio para sua vigia.

Por fim, conforme Patricia Peck e Bruna Michele Wozne Godoy[28] lecionam, se houver a utilização de reconhecimento facial pelos entes públicos ou privados, de acordo com a LGPD, é imperativo implementar os seguintes mecanismos: (i) incorporar o *Privacy by Design* (PbD), assegurando a implementação de medidas de segurança desde a concepção até a execução, conforme descrito no artigo 46º, § 2º; (ii) registrar o tratamento no Registro de Operações de Tratamento de Dados Pessoais (ROPA), conforme estipulado no artigo 37º; (iii) garantir que o uso da análise biométrica esteja em conformidade com os princípios estabelecidos pela legislação, especialmente aqueles relacionados à transparência, necessidade e não discriminação, conforme mencionado no artigo 6º; (iv) realizar uma Avaliação de Impacto à Proteção de Dados Pessoais (RIPD) para identificar e mitigar riscos aos direitos fundamentais e liberdades civis dos titulares, em conformidade com o artigo 38º; (v) cumprir o dever de transparência por meio de avisos claros e visíveis, como o uso de identificadores em vias públicas e placas em locais específicos; e (vi) gerenciar o tratamento de dados pessoais sensíveis com propósitos específicos, evitando o uso para discriminação, e estabelecer uma Comissão de Ética Algorítmica em conjunto com a entidade pública para abordar questões de tendenciosidade e implementar melhorias de forma regular.

Dessa forma, é possível concluir que o uso do reconhecimento facial para fins de monitoramento apresenta um dilema complexo entre a proteção da segurança pública e a preservação dos direitos fundamentais à privacidade e ao anonimato. Por um lado, a capacidade de identificação de pessoas de maneira rápida pode ser uma ferramenta valiosa na investigação de atividades prejudiciais à sociedade e na prevenção de crimes. Isso pode justificar, em alguns casos, a intervenção do Estado para limitar o exercício de direitos individuais em nome de interesses estatais ou coletivos difusos.

Por outro lado, a coleta de dados biométricos de forma indiscriminada e sem uma regulamentação específica pode ocasionar em incontáveis violações aos direitos fundamentais dos indivíduos, como a privacidade e o anonimato. Assim, em uma eventual implementação

[28] PECK, Patrícia; GODOY, Bruna Michele Wozne. Privacidade e Tecnologias de Reconhecimento Facial – Coexistência pacífica? **Tech Compliance**, 2022. Disponível: https://techcompliance.org/reconhecimento-facial/. Acesso em: 10 out. 2023.

pelo governo brasileiro da tecnologia de reconhecimento facial, os limites impostos pela transparência, consentimento e acessibilidade devem ser respeitados.

Portanto, é essencial que haja uma regulamentação rigorosa e transparente para governar o uso do reconhecimento facial, garantindo que seja usado de maneira proporcional e estritamente necessário para alcançar os objetivos legítimos de segurança pública. Além disso, a proteção de dados e a fiscalização adequada são cruciais para proteger os direitos individuais, ao mesmo tempo em que permitem que as autoridades cumpram seu papel na aplicação da lei. O desafio reside em encontrar um equilíbrio sensato entre a segurança e a proteção da privacidade e o anonimato, garantindo que o uso do reconhecimento facial seja uma ferramenta eficaz e responsável para o bem-estar da sociedade como um todo.

6. Conclusão

Como demonstrado, o reconhecimento facial traz um sistema inovador de vigilância, com o potencial de trazer facilidades para a sociedade e ser um grande alicerce na segurança pública e privada.

Uma tecnologia de reconhecimento facial é basicamente um programa de software projetado para detectar e distinguir rostos humanos em fotografias ou vídeos. Com o auxílio de vastas bases de dados e o uso de conexões de internet de alta velocidade, essas tecnologias de reconhecimento facial são capazes de identificar e registrar características individuais de cada pessoa, permitindo assim o processamento de imagens capturadas por computadores, smartphones ou câmeras de vigilância. Os dados processados podem, então, ser utilizados para uma ampla variedade de finalidades.[29]

Todavia, sem uma regulamentação específica contendo balizadores aptos a garantir os direitos fundamentais do indivíduo e a aplicação indiscriminada do reconhecimento facial, como vem ocorrendo neste país, esta inteligência artificial se tornará um grande inimigo da dignidade da pessoa humana. Conquanto o Brasil busque acompanhar a modernização, é certo que as evoluções legislativas não possuem o condão de acompanhar as novas tecnologias, como o reconhecimento facial. Assim, mesmo com o advento da Lei Geral de Proteção de Dados do

[29] NABEEL, Fahad. **Regulating Facial Recognition Technology in Public Places**. Centre for Strategic and Contemporary Research, 2019, p. 1-2. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places. Acesso em: 20 jul. 2023.

ano de 2018, esta se torna insuficiente para a proteção da privacidade e do anonimato na utilização de sistemas de vigilância.

Portanto, é essencial encontrar um equilíbrio entre o aproveitamento das vantagens do reconhecimento facial e a proteção dos direitos e privacidade das pessoas, por meio da implementação de regulamentações apropriadas e específicas e do monitoramento cuidadoso de seu uso.

Nesse contexto, importante destacar o extenso processo evolutivo que o direito à privacidade vem passando, principalmente com as novas tecnologias chegando em nossas vidas. Primeiramente, o direito à privacidade estava intrinsicamente ligado ao conceito clássico de *"the right to be left alone"*. Para Danilo Doneda[30], a garantia do direito à privacidade se baseia na distinção entre as atividades que são adequadas para a esfera pública e as que devem ser mantidas no mundo privado de cada indivíduo. Consequentemente, nessa ideia de privacidade, existe uma escolha criteriosa sobre quais informações podem ser compartilhadas publicamente e quais devem permanecer dentro do âmbito privado.

Esse conceito é incorporado pela Constituição Federal Brasileira, em seu artigo 5º, inciso X, dispondo sobre uma garantia da inviolabilidade da vida privada. A privacidade pode ser entendida como um direito que se baseia na liberdade negativa do indivíduo, permitindo-lhe que escolher quais aspectos de sua vida fazem parte de sua esfera privada e, portanto, são protegidos por esse direito.[31]

Em contraponto, essa concepção tradicional de privacidade passou a ser insuficiente nos tempos modernos para proteger os direitos dos indivíduos, sendo deixada de lado para abarcar também o controle do indivíduo sobre seus próprios dados pessoais, ou seja, o direito a controlar o uso do que os outros fazem das informações que nos dizem respeito.[32] Esse desenvolvimento reflete a crescente necessidade e importância de garantir a proteção dos dados pessoais em um cenário mundial cada vez mais digitalizado e revestido de tecnologias, sendo que a coleta e a utilização indevida de informações privadas têm causado preocupações e impulsionando críticas tanto para a sociedade quanto para a legislação vigente.

O surgimento de tecnologias avançadas e a proliferação de plataformas de vigilância impulsionaram a coleta massiva de dados, levantando questões sobre como esses dados são

---

[30] DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 126-127.
[31] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008, p. 320.
[32] *Ibidem*, p. 74.

utilizados, compartilhados e protegidos, sendo que o debate em torno das regulamentações e das salvaguardas para a proteção dos dados pessoais ganhou importância significativa, já que poderiam ocasionar violações à privacidade.

Em sentido amplo da esfera privada, são estabelecidas restrições à divulgação pública de informações pessoais de um indivíduo, o que inclui preservar sua identidade. Em paralelo, a proteção de dados pessoais tem como propósito assegurar que os indivíduos possam exercer controle sobre como suas informações são utilizadas por organizações tanto públicas quanto privadas. Nessa senda, a privacidade passa a se materializar também na forma da necessidade de anonimato, ou seja, a necessidade de adotar uma identidade preferida, que pode incluir um nome, gênero e idade distintos daqueles correspondentes aos dados reais do indivíduo. Isso demanda a proteção de uma identidade nova, de uma esfera íntima construída, como uma condição para o desenvolvimento da própria personalidade e para alcançar plenamente a liberdade existencial.[33]

Dessa forma, o anonimato se dissocia apenas da ideia de vedação constitucional, prevista no art. 5º, inciso IV da Constituição Federal, e passa a ser vista como o direito de permanecer no anonimato, de não ser identificado. Segundo Miriam Wimmer e Lucas Borges de Carvalho, no terceiro fundamento constitucional do anonimato, isto é, analisado junto ao direito à privacidade e a proteção de dados pessoais, o anonimato passa a ser visto como um viabilizador de direitos fundamentais, sendo uma ferramenta legítima para a proteção da privacidade dos indivíduos e garantindo que estes tenham controle sobre o uso de suas informações pessoais por terceiros.

Há de se mencionar que a vedação ao anonimato não será descartada e será aplicada quando utilizada para fins ilícitos, como uma medida essencial para assegurar a responsabilização e a transparência em situações em que o anonimato é explorado de forma prejudicial. Contudo, não se pode ampliar excessivamente essa vedação, a fim de considerar os possíveis benefícios que o direito ao anonimato pode oferecer. Reconhece-se que há, pelo menos, um interesse mínimo no anonimato como um direito para usar pseudônimos e proteger dados de identificação pessoal. Essa abordagem equilibrada visa proteger os direitos individuais e impede o uso indevido do anonimato.

Para que as pessoas possam se sentir seguras ao se portarem em público, o anonimato é essencial, protegendo o direito de não ser identificado ou vigiado pelo Estado ou por empresas

---

[33] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008, p. 116.

privadas. No entanto, o anonimato em locais públicos também pode levantar questões relacionadas à segurança pública e à responsabilidade individual. Em certos contextos, a identificação de pessoas em espaços públicos é necessária para garantir a segurança coletiva e prevenir atividades ilícitas, como por exemplo, na utilização do reconhecimento facial pelo Estado e órgãos privados.

Portanto, resta primordial estabelecer um equilíbrio entre os recentes avanços tecnológicos com a preservação do direito ao anonimato e da privacidade e a garantia da segurança pública. Esse equilíbrio deve ser alcançado por meio da formulação de políticas e leis adequadas que respeitem os direitos individuais e a proteção de dados, a fim de preservar a privacidade e a segurança dos cidadãos em um ambiente hiperconectado e em constante evolução.

Para isso, impor restrições cuidadosas ao uso de tecnologias biométricas, com foco na transparência durante a coleta de dados pessoais, o consentimento e acesso do indivíduo a esses dados são uma forma de alcançar essa harmonia. É de exímia importância assegurar a transparência no processamento de dados, uma vez que permite que as pessoas compreendam o modo como suas informações são adquiridas e utilizadas, promovendo a confiança dos titulares dos dados no sistema ao fornecer-lhes pleno conhecimento das informações coletadas e a oportunidade de consentir com o uso de seus dados faciais.

Assim, as organizações públicas e privadas devem fornecer informações claras e precisas sobre como implementar tecnologias de vigilância em locais específicos, facilitando a compreensão dos usuários aos fins para os quais seus dados estão sendo empregados. A acessibilidade desses avisos também é fundamental, garantindo que estejam prontamente disponíveis nos locais de captura de dados biométricos, além de garantir que os titulares tenham controle sobre suas informações pessoais.

Ou seja, o direito de acesso dos indivíduos aos seus próprios dados deve ser preservado. Já que se torna fundamental que os titulares possam acessar, revisar e, se necessário, corrigir as informações coletadas a seu respeito, proporcionando maior autonomia em relação às suas informações, permitindo-lhes tomar medidas adequadas para proteger sua privacidade, conforme desejado.

Assim, considerando tanto as leis vigentes quanto as propostas em andamento, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e o Marco Legal da Inteligência Artificial, destacam a importância de proteger os direitos individuais no uso do reconhecimento facial. O desafio mais importante recai na necessidade de encontrar pontos de equilíbrio entre a necessidade de

implementação da vigilância para segurança da sociedade, a salvaguarda dos direitos individuais, como a privacidade e o anonimato e o cumprimento das possíveis regulamentações dessa inteligência artificial.

Dessa forma, é evidente que a regulamentação transparente e eficaz é essencial para governar o uso do reconhecimento facial, garantindo que seu emprego seja responsável e proporcional. Esse equilíbrio sensato é vital para garantir a proteção da privacidade e do anonimato dos indivíduos, ao mesmo tempo em que possibilita que as autoridades desempenhem seu papel na manutenção da ordem pública.

Adotando as orientações do Comitê Europeu para a Proteção de Dados (EDPB) propostas no "*Guidelines on the use of facial recognition technology in the area of law enforcement"*[34], alguns usos da tecnologia de reconhecimento facial devem ser evitados ou até mesmo banidos a fim de garantir os direitos individuais de cada ser humano, como a análise biométrica para inferir as emoções dos indivíduos e o uso de banco de dados que coletam imagens online, especialmente aquelas provenientes de redes sociais.

Ainda, levando em consideração as disposições da Lei Geral de Proteção de Dados Brasileira, tem-se que alguns mecanismos são inevitáveis para a implementação do reconhecimento facial no Brasil, como conduzir um *Privacy by Design* (PbD) para construção de medidas de segurança desde a concepção até a execução, registrar o tratamento no Registro de Operações de Tratamento de Dados Pessoais (ROPA), assegurar que o uso da análise biométrica esteja em conformidade com os princípios estabelecidos pela legislação, especialmente aqueles relacionados à transparência, necessidade e não discriminação, a realização de uma Avaliação de Impacto à Proteção de Dados Pessoais (RIPD) para identificar e mitigar riscos aos direitos fundamentais e liberdades civis dos titulares, cumprir o dever de transparência por meio de avisos claros e visíveis, já anteriormente suscitado.

Com isso, temos a possibilidade de execução de tecnologias de reconhecimento facial no ordenamento jurídico brasileiro, com regulamentações que restringem e supervisionam o uso dessa tecnologia, salvaguardando, ao mesmo tempo, os direitos essenciais à privacidade e ao anonimato. Esses direitos estão intrinsecamente interligados, pois a proteção da privacidade individual muitas vezes depende do anonimato e da capacidade de controlar a divulgação e o acesso aos dados pessoais.

---

[34] GUIDELINES on the use of facial recognition technology in the area of law enforcement. Version 1.0. **European Data Protection Board**, 12 may 2022, p. 1-49. Disponível em: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf. Acesso em: 22 set. 2023.

Para a preservação da confiança dos usuários e a garantia da segurança e proteção dos direitos individuais é essencial estabelecer regulamentações eficazes que guiem o uso responsável das tecnologias de vigilância, promovendo a transparência, o acesso aos dados e o respeito à privacidade de cada indivíduo.

7. Referências Bibliográficas

AMARAL, Artur Leão; PASCOAL, Rafael Boffa; MORAIS, Samir José Pereira. **Considerações sobre anonimato e privacidade em uma realidade hiperconectada**, p. 1-6. Disponível em: file:///C:/Users/lucri/Downloads/17647-1125627452-1-PB.pdf. Acesso em: 22 set. 2023.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8ª ed. São Paulo: Saraiva, 2015. *E-book*.

BONOTTO, Ana Carolina Garcia. **O anonimato na ordem jurídico-constitucional brasileira e suas implicações na internet**. 2017. Dissertação (Mestrado em Direito) - Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2017. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/9094/2/Ana_Cristina_Bonotto.pdf. Acesso em: 22 set. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência Estudos Jurídicos e Políticos**, Florianópolis, v. 38, n. 76, p. 213–240, 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213/34870. Acesso em: 31 out. 2023.

CAPANEMA, Walter Aranha. **O direito ao anonimato: uma nova interpretação do art. 5º, IV, CF**. Disponível em: https://www.academia.edu/3436841/O_direito_ao_anonimato_uma_nova_interpreta%C3%A7%C3%A3o_do_art_5o_IV_CF. Acesso em: 23 abr. 2023.

COLOMBO, Mariah. Curitiba usa reconhecimento facial como ferramenta na segurança pública sem ter regulação específica: 'Sociedade de controle', critica especialista. **G1 – Paraná RPC**, 2 out. 2023. Disponível em: https://g1.globo.com/pr/parana/noticia/2023/10/02/curitiba-usa-reconhecimento-facial-como-ferramenta-na-seguranca-publica-sem-ter-regulacao-especifica-sociedade-de-controle-critica-especialista.ghtml. Acesso em: 22 out. 2023.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. **Revista de Direito, Governança e Novas Tecnologias**, Belém, v. 5, n. 2, p. 1-21, jul./dez. 2019. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5777/pdf. Acesso em: 22 set. 2023.

DERECHO CHILE. **T. Constitucional sobre a constitucionalidade do registo privado de "cibercafés". Acórdão n.º 1894-2011-CPR**, de 12 de julho de 2011. Disponível em:

https://derecho-chile.cl/sentencia-del-tribunal-constitucional-sobre-la-constitucionalidad-de-un-registro-privado-de-los-cibercafes/. Acesso em: 22 set. 2023.

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

EUROPEAN DATA PROTECTION BOARD. **O CEPD adota orientações sobre o cálculo das coimas e a utilização da tecnologia de reconhecimento facial no domínio da aplicação da lei**, Bruxelas, 16 may 2022. Disponível em: https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-calculation-fines-guidelines-use-facial-recognition_pt. Acesso em: 20 out. 2023.

GARCIA, Pedritta Marihá. Projeto que veda tecnologia de reconhecimento facial na pauta da CCJ. **Câmara Municipal de Curitiba**, 3 mar. 2023. Disponível: https://www.curitiba.pr.leg.br/informacao/noticias/projeto-que-veda-tecnologia-de-reconhecimento-facial-na-pauta-da-ccj. Acesso em: 15 set. 2023.

GLOBO.COM. Prefeitura lança projeto de segurança nos bairros de Copacabana e Leme, Zona Sul do Rio. **Bom Dia Rio**, 27 nov. 2017. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/prefeitura-do-rio-lanca-projeto-de-seguranca-em-copacabana.ghtml. Acesso em: 22 set. 2023.

GUIDELINES on the use of facial recognition technology in the area of law enforcement. Version 1.0. **European Data Protection Board**, 12 may 2022, p. 1-49. Disponível em: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf. Acesso em: 22 set. 2023.

HAJE, Lara. Governo quer lei para regular vigilância estatal por meio de reconhecimento facial. **Agência Câmara de Notícias**, 3 abr. 2019. Disponível em: https://www.camara.leg.br/noticias/554826-governo-quer-lei-para-regular-vigilancia-estatal-por-meio-de-reconhecimento-facial/. Acesso em: 22 set. 2023.

LENTINO, Amanda. This Chinese facial recognition start-up can identify a person in seconds. **CNBC Disruptor 50**, 17 may 2019. Disponível em: https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html#:~:text=One%20of%20the%20companies%20making,in%20a%20matter%20of%20seconds. Acesso em: 20 out. 2023.

LEONARDI, Marcel. **Tutela da privacidade na internet.** 1.ª ed. São Paulo: Saraiva, 2011. p. 78.

LIBERMAN, Tania. A regulamentação da IA no Brasil. **Jota**, 6 ago. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulamentacao-da-ia-no-brasil-06082023. Acesso em: 22 set. 2023.

MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no direito brasileiro (Right to Anonymity on the Internet: Foundations and Legal Outlines for Its Protection in the Brazilian Law). **Revista de Direito Civil Contemporâneo**, v. 23, ano 7, p. 95-140, 13 nov. 2020. Disponível em: https://deliverypdf.ssrn.com/delivery.php?ID=127087120097028115071094099084012030002

20410170310270780990940271060090671271170010300011210051220421261070260830861100180230750460340130640880750190650821070180171000860360120920190211070880301270641090851171271180220250300930690940021060810740280840 95&EXT=pdf&INDEX=TRUE. Acesso em: 22 set. 2023.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS - QUALIS A2**, v. 41, n. 134, 2014. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/206. Acesso em: 5 nov. 2023.

MAGRO, Diogo Dal; FORTES, Vinícius Borges. O Reconhecimento Facial nas Smart Cities e a Garantia dos Direitos à Privacidade e à Proteção de Dados Pessoais. **Revista de Direito Internacional**, v. 18, n. 2, 2021. Disponível em: https://www.publicacoes.uniceub.br/rdi/article/view/7677. Acesso em: 23 abr. 2023.

MARASCIULO, Marilia. Reconhecimento facial: prós e contras da tecnologia que veio para ficar. **Revista Galileu**, 21 mar. 2022. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html. Acesso em: 22 set. 2023.

MELO, Mariana Cunha e. **Anonimato, Proteção de Dados e Devido Processo Legal: Por Que e Como conter uma das maiores ameaças ao Direito à Privacidade no Brasil**. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf. Acesso em: 22 set. 2023.

MONREAL, Eduardo Novoa. **Derecho a la vida privada y libertad de información**: **un conflicto de derechos**. 2.ª ed. México: Siglo Veintiuno, 1981.

NABEEL, Fahad. **Regulating Facial Recognition Technology in Public Places**. Centre for Strategic and Contemporary Research, 2019, p. 1-2. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places. Acesso em: 20 jul. 2023.

NEGRI, Sérgio Marcos Carvalho de Ávila; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon Silva. O Uso de Tecnologias de Reconhecimento Facial baseadas em Inteligência Artificial e o Direito à Proteção de Dados. **Revista de Direito Público**, Brasília-DF, v. 17, n. 93, p. 82-103, maio/jun. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740. Acesso em: 30 out. 2023.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: LYON, David. **Surveillance as social sorting: privacy, risk, and digital discrimination**. New York: Routledge, 2003, p. 247-281.

NOYAN, Oliver. New German government to ban facial recognition and mass surveillance. **Euractiv Intelligence**, 1.º dez. 2021. Disponível em: https://www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/. Acesso em: 22 set. 2023.

OLIVEIRA, José Sebastião de; SALDANHA, Rodrigo Róger. O Anonimato como um Novo Conceito de Intimidade e Proteção dos Direitos da Personalidade: A Antinomia entre o Uso do Anonimato para fins lícitos e a Vedação Constitucional ao Anonimato. **Revista Jurídica Cesumar**, v. 22, n. 2, p. 363-379, maio/ago. 2022. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/11005/7163. Acesso em: 22 set. 2023.

ORTEGA, Pepita. Desembargadora mantém suspensão de sistema de reconhecimento facial no Metrô de SP. **Estadão Conteúdo**, São Paulo, 18 abr. 2022. Disponível em: https://www.cnnbrasil.com.br/nacional/desembargadora-mantem-suspensao-de-sistema-de-reconhecimento-facial-no-metro/ Acesso em: 24 de abr. 2023.

PACHECO, Vinícius Maia. **Emprego de Anonimato para Melhoria de Privacidade no Consumo de Serviços em SaaS**. 2013. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília-DF, 2013.

PECK, Patrícia; GODOY, Bruna Michele Wozne. Privacidade e Tecnologias de Reconhecimento Facial – Coexistência pacífica? **Tech Compliance**, 2022. Disponível: https://techcompliance.org/reconhecimento-facial/. Acesso em: 10 out. 2023.
PINHEIRO, Patrícia Peck. **Direito Digital**. 7.ª ed. São Paulo: Saraiva, 2021. *E-book*.

QUEIROZ, Rafael Mafei Rabelo. Liberdade de expressão na internet: a concepção restrita de anonimato e a opção pela intervenção de menor intensidade. **Suprema – Revista de Estudos Constitucionais**, v. 1, n. 1, p. 241-266, jan./jun. 2021. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/24/21. Acesso em: 22 set. 2023.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 9.ª ed. São Paulo: Saraiva, 2016. p. 565.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de janeiro: Renovar, 2008.

SALEME, Edson Ricardo. **Direito constitucional**. 4.ª ed., rev. e atual. São Paulo: Manole, 2021. *E-book.*

SANTOS, Rodrigo Natálicio dos; CABRAL, Cristiane Helena de Paula Lima. Reconhecimento Facial: Análise a partir da Constituição Brasileira e da Lei Geral de Proteção de Dados. **Revista Brasileira de Direito e Gestão Pública**, v. 8, n. 5, p. 1127–1142, 2021. Disponível em: https://www.gvaa.com.br/revista/index.php/RDGP/article/view/8599. Acesso em: 23 abr. 2023.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3.ª ed. rev. e atual. São Paulo: Atlas, 2014. *E-book.*

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 36.ª ed. São Paulo: Malheiros, 2012.

SILVAR, Gustavo Businhani da; RODRIGUES, Bruno da Silva. **Problemas derivados do uso de reconhecimento facial**, P. 1-13. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/e71ac334-395b-421a-b4e2-4a526721c42b/content. Acesso em: 22 set. 2023.

SOLOVE, Daniel J. **Understanding Privacy**. Harvard University Press, GWU Law School Public Law Research Paper n.º 420, 13 jul. 2014, p. 766-777. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888. Acesso em: 20 out. 2023.

SPALER, Mayara Guibor; REIS, Rafael Almeida Oliveira. Limites do direito fundamental à privacidade frente a uma sociedade conectada. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, ano 3, n. 3, dez. 2018. Disponível em: https://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_11.pdf. Acesso em: 22 set. 2023.

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

TAVARES, Letícia Antunes. O direito à privacidade em suas mais exclusivas esferas: a intimidade e a vida privada na era informacional. *In*: LOUREIRO, Francisco Eduardo; DE PRETTO, Renato Siqueira; KIM, Richard Pae (org.). **A vida dos direitos nos 30 anos da Constituição Federal**. 1.ª ed. São Paulo: Escola Paulista da Magistratura, 2019, p. 453-472. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/A-vida-dos-direitos-nos-30-anos-da-Constituicao-Federal.pdf. Acesso em: 22 set. 2023.

UNITED STATES. U. S. Supreme Court. **McIntyre v. Ohio Elections Comm'n, 514 U.S. 334**. Argued: 12 oct. 1994. Decided: 19 apr. 1995. Disponível em: https://supreme.justia.com/cases/federal/us/514/334/. Acesso em: 22 set. 2023.

VELASCO, Nara. Privacidade: Direito A Intimidade Na Era Digital. **Revista Ciência e Sociedade**, Macapá, n. 1, v. 1, 2016. Disponível em: http://periodicos.estacio.br/index.php/cienciaesociedade/article/view/2104/1232. Acesso em: 30 out. 2023.

VIATROLEBUS. **Via Quatro lança portas interativas digitais nas plataformas.** Metrô SP, Assessoria Via Quatro, 12 abr. 2018. Disponível em: https://viatrolebus.com.br/2018/04/viaquatro-lanca-portas-interativas-digitais-nas-plataformas/. Acesso em: 8 nov. 2023.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sérgio Antônio Fabris, 2007.

VU, Brandon. **A Technological and Ethical Analysis of Facial Recognition in the Modern Era**, 2018, p. 11-12. Disponível em: https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era. Acesso em: 22 set. 2023.

WESTIN, Alan; SOLOVE, Daniel. **Privacy and Freedom**. NewYork: Ig Publishing, 1967.

WIMMER, Miriam; CARVALHO, Lucas Borges de. O papel e os limites do anonimato: em busca de uma interpretação constitucionalmente adequada. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 27, n. 2, p. 1-16, abr./jun. 2022. Disponível em: https://ojs.unifor.br/rpen/article/view/13041/6855. Acesso em: 22 set. 2023.

ZMOGINSKI, Felipe. A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial. **Tilth Uol – Inteligência Artificial**, 19 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm?cmpid=copiaecola. Acesso em: 22 set. 2023.

Universidade Presbiteriana Mackenzie | Faculdade de Direito 70 anos

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Giovanna Monteiro da Silva
discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº 31975364, período matutino, turma 10A, tendo realizado o TCC com o título:
Os limites impostos pelo direito ao anonimato e o direito à privacidade na utilização do reconhecimento facial pelos entes públicos e privados
sob a orientação do(a) Professor(a) Paulo Cezar Neves Junior
declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 09 de 11 de 2023.

G. Monteiro

Assinatura do discente