REVISTA DE DIREITO DO TRABALHO, PROCESSO DO TRABALHO E DIREITO DA SEGURIDADE SOCIAL

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

ARTIGO

TECNOLOGIA E TUTELA DOS DIREITOS HUMANOS: UMA ANÁLISE DA AUTODETERMINAÇÃO INFORMATIVA NO CENÁRIO DE RECONHECIMENTO FACIAL

Jairo Santos Correia[1]

Marcos Marcílio Eça Santos[2]

RESUMO

Esse estudo busca analisar como o avanço do reconhecimento facial afeta o direito humano à proteção de dados pessoais sensíveis, e quais são os desafios e implicações para a tutela dos direitos humanos? Para tal apresenta-se a seguinte hipótese se a expansão do reconhecimento facial pode resultar em uma diminuição da privacidade, comprometendo o direito fundamental à proteção de dados e, por conseguinte, a autodeterminação informativa. A metodologia empregada será a revisão integrativa da literatura de natureza exploratória na doutrina, na legislação, e na jurisprudência dos tribunais superiores. Constatou-se que as lacunas normativas comprometem o direito humano à autodeterminação informativa, assim na coleta, armazenamento e tratamento de informações biométricas é necessário boa-fé, e seus deveres jurídicos anexos de lealdade, transparência, informação, e consentimento prévio. Bem como há riscos de discriminação algorítmica que afetam principalmente determinados grupos, por exemplo, negros, mulheres, e crianças estão sujeitos, falsos positivos. Além disso, constatou-se a ausência de transparência no uso da tecnologia em estádios de futebol, o que pode ensejar o vazamento e, por conseguinte, a comercialização dessas informações. Dessa forma, torna-se necessário que a LGPD seja alterada para endurecer a tutela dos dados biométricos e coibir a comercialização dessas informações a fim de salvaguardar a autodeterminação informativa de acordo com o PL 36/2025. Para além da regulamentação específica é necessário o controle humano sobre a coleta, o armazenamento e o tratamento dessas informações através de auditorias frequentes, independentes e revisões humanas periódicas com a finalidade de proteger o consentimento livre, informado e desembaraçado. Não obstante o dever da ANPD de fiscalizar e, por conseguinte, sancionar abusos e uso indevido de tais informações.

Palavras-chave: Autodeterminação informativa; Reconhecimento facial; Direitos humanos.

[1] Pós-graduando em Direitos Humanos e Sociais pela Universidade do Estado da Bahia, Bacharel em Direito pela Universidade do Estado da Bahia - Campus XIX – Camaçari – Bahia. E-mail: jairo.scorreia@gmail.com
[2] Professor orientador deste trabalho. E-mail: mmarcilio@uneb.br

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

ABSTRACT

This analyze aimed to investigate how the advancement of facial recognition technology affects the human right to the protection of sensitive personal data, as well as the challenges and implications this poses for the safeguarding of human rights. To this end, the following hypothesis is presented: the expansion of facial recognition systems may result in a reduction of privacy, thereby compromising the fundamental right to data protection and, consequently, informational self-determination. The methodology employed is an integrative literature review with an exploratory approach, based on legal doctrine, legislation, and jurisprudence from higher courts. The findings reveal that normative gaps undermine the human right to informational self-determination. Therefore, in the collection, storage, and processing of biometric data, the principles of good faith must prevail, along with its associated legal duties of loyalty, transparency, access to information, and prior consent. The study also identified risks of algorithmic discrimination, particularly affecting specific groups such as Black people, women, and children, who are especially vulnerable to false positives. Furthermore, there is a lack of transparency in the use of facial recognition technology in football stadiums, which raises concerns about potential data breaches and, consequently, the commercial exploitation of such information. In light of these issues, it becomes essential to amend the Brazilian General Data Protection Law (LGPD) to strengthen the protection of biometric information and prohibit its commercialization, in accordance with Bill 36/2025. Beyond specific regulation, it is crucial to ensure human oversight of data collection, storage, and processing, through frequent independent audits and periodic human reviews, in order to safeguard free, informed, and unburdened consent. In addition, the Brazilian Data Protection Authority (ANPD) has the duty to monitor, and, when necessary, sanction abuses and the improper use of personal data.[3]

Keywords: Informational self-determination; Facial recognition; Human rights.

1. INTRODUÇÃO

O presente trabalho busca analisar como o avanço do reconhecimento facial afeta o direito humano à proteção de dados pessoais sensíveis, e quais são os desafios e implicações para a tutela dos direitos humanos?. Para tal apresenta-se a seguinte hipótese se a expansão do reconhecimento facial pode resultar

[3] Tradução escrita com auxílio de tecnologia de inteligência artificial (ChatGPT)

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

em uma diminuição da privacidade, comprometendo o direito fundamental à proteção de dados e, por conseguinte, a autodeterminação informativa.

Nesse cenário, em decorrência das transformações tecnológicas, é crucial entender como as práticas de vigilância digital que usam de inteligência artificial para a coleta, processamento, armazenamento e compartilhamento de informações biométricas, mais especificamente o reconhecimento facial, impacta os direitos humanos, qual seja, á privacidade e suas nuances, a saber, à hora, à intimidade, à vida privada, à proteção de dados e a autodeterminação informativa e visando aprimorar as políticas públicas e garantir um equilíbrio entre o emprego de novas tecnologias e a preservação dos valores fundamentais.

Todavia, o direito à proteção de informações seja no espaço físico ou digital que outrora associava-se diretamente à privacidade, hoje, é uma prerrogativa autônoma em virtude da Emenda Constitucional 115 de 2022. Desse modo, consiste a proteção de dados em direito civil e político - integrando, a primeira e a quarta dimensão da classificação dos direitos humanos, que visa tutelar informações que identificam pessoas e podem colocar em risco sua segurança se forem usadas de forma inadequada, vazadas ou comercializadas. Assim, da tutela de dados deriva a autodeterminação informativa.

Nessa direção, a Lei 14.597/2023, denominada Lei Geral do Esporte, estabelece a obrigatoriedade dos estádios com capacidade com mais vinte mil pessoas utilizarem biometria por reconhecimento facial. Outrossim, a biometria por reconhecimento facial já pode ser usada para diversos fins, quais sejam, nos condomínios, em metrôs, transporte público, nas ruas, em shows e eventos, no mobile banking- uma das formas de acessar os serviços a bancários através do sistema remoto e pelos órgão de segurança pública, a fim de monitorar as pessoas, para ajudar a encontrar pessoas desaparecidas, e por conseguinte identificar criminosos reincidente e inibir a criminalidade ensejando a vigilância em massa. Ou seja, o reconhecimento facial é um fato cada vez mais presente no cotidiano das pessoas.

Sendo assim, esses dados devem ser tratados com boa-fé, de forma transparente e responsável, inclusive observando o consentimento que é uma das condições para a coleta, ratamento e armazenamento de informações pessoais segundo com a Lei Geral de Proteção de Dados (LGPD) a fim de evitar discriminações, vazamento e comercialização.

Nessa linha de raciocínio, propõe-se como objetivo geral analisar o impacto da tecnologia de reconhecimento facial na tutela dos direitos humanos, com fulcro no direito essencial à proteção de informações pessoais.

Entendem-se como objetivos específicos: traçar breves considerações sobre a existência e o desenvolvimento dos direitos humanos, bem como identificar em qual(is) dimensão(ões) a proteção de

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

dados se encaixa no primeiro tópico; investigar os fundamentos humanos do direito a privacidade e suas nuances, a saber, autodeterminação informativa e proteção de dados pessoais no segundo tópico; analisar o uso do reconhecimento facial e as implicações éticas e legais no terceiro tópico; e estudar as diretrizes para uma regulamentação eficaz que concilie a segurança proporcionada pelo reconhecimento facial com a preservação do direito humano à proteção de dados no último tópico.

Nesse sentido, a metodologia empregada será a revisão integrativa da literatura de natureza exploratória na doutrina, na legislação, na resolução do Conselho Nacional de Justiça (CNJ) e na jurisprudência dos tribunais superiores. Por fim, ressalta-se que a temática é de grande relevância prática e social.

2. BREVES CONSIDERAÇÕES SOBRE A EXISTÊNCIA DOS DIREITOS HUMANOS.

A origem dos direitos humanos remonta à antiguidade e atualmente está diretamente ligada à concepção de dignidade humana, cláusula nuclear de todo o ordenamento jurídico, isto é, inerente à pessoa humana, independentemente de sua origem, nacionalidade, ideologia ou posição social. Sendo assim, consiste no reconhecimento ético e, por conseguinte normativo da condição humana, fundado em princípios gerais como liberdade, igualdade, justiça e solidariedade (RAMOS, 2024).

Apesar da codificação dos direitos humanos tenha se dado no pós-Segunda Guerra Mundial, tendo como marco normativo, qual seja, a Declaração Universal dos Direitos Humanos (DUDH) de 1948, seu fundamento já existia outrora e emanava do jusnaturalismo, das revoluções liberais de combate ao absolutismo e ao feudalismo e dos movimentos de emancipação social (RAMOS, 2024).

Sendo assim, “a Declaração foi redigida com o intuito de proclamar definitivamente os direitos fundamentais da humanidade, o respeito inviolável à dignidade do ser humano” (MONDAINI, 2020, p.157). Segundo Comparato “no tocante aos direitos humanos, reconhece-se hoje que eles constituem um “sistema objetivo de valores”, formando a base e´tica da sociedade” (2013, p.67).

Nesse caminho, esse conjunto racional de princípios “asseguram uma vida digna, na qual o indivíduo possui condições adequadas de existência, participando ativamente da vida de sua comunidade” (RAMOS, 2024, p.9). Nesse sentido, a DUDH consagrou “três princípios axiológicos fundamentais em matéria de direitos humanos: a liberdade, a igualdade e a fraternidade” (COMPARATO, 2013, p.66), desses valores derivam as três dimensões clássicas dos direitos humanos, quais sejam, os direitos civis e políticos, os direitos sociais, econômicos e culturais e os direitos difusos, (apesar da Declaração não ter tratado especificamente desta última dimensão) que não são meros direitos programáticos. Ou seja, a existência

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

desses direitos, não é apenas declaratória, mas sim normativa, exigindo concretização por meio de políticas públicas e instituições que assegurem sua efetividade.

Para Bauman:

> As únicas duas coisas úteis que se espera e se deseja do "poder público" são que ele observe os "direitos humanos" isto é, que permita que cada um siga seu próprio caminho, e que permita que todos o façam "em paz" - protegendo a segurança de seus corpos e posses [...] (2001. p.45)

Nessa conjuntura, na primeira dimensão de direitos, predomina a visão do indivíduo como um ente autônomo em relação ao Estado, consignado pelas liberdades civis e políticas, como o direito à vida, à liberdade, à privacidade e à propriedade, entre outros. Com a segunda geração, ganha relevo a efetivação dos direitos sociais, econômicos e culturais, orientados à promoção da igualdade material entre os indivíduos, como à saúde, o trabalho digno e à moradia. Por sua vez a terceira dimensão é composta pelos direitos de solidariedade e fraternidade, voltados à proteção de interesses coletivos e difusos ou metaindividuais - vão além do indivíduo-, como à paz, ao meio ambiente ecologicamente equilibrado e à comunicação (ARAKAKI; VIERO, 2018).

Nesse caminho, a quarta dimensão está relacionada à globalização dos direitos humanos, consiste nos direitos ao pluralismo político, à informação e à democracia participativa ou direta (RAMOS, 2024). Não obstante, para alguns autores a quarta geração é composta pelas prerrogativas ligadas à pesquisa genética, à bioética, aos neurodireitos, e o acesso a internet. Ademais, os avanços cibernéticos estariam no conjunto da quinta dimensão de direitos, porém Bonavides defende que o direito à paz diante da sua relevância estaria na quinta geração de direitos humanos e não na terceira dimensão. Embora Cançado Trindade sustente a preponderância do princípio da indivisibilidade e da interdependência dos direitos humanos uma vez que essas prerrogativas se complementam mutuamente, assim, a teoria das gerações ou dimensões encontra-se obsoleta.

Nesse contexto, atualmente, a tutela dos direitos humanos enfrenta novos desafios impostos pelo desenvolvimento tecnológico, em especial aquele que envolvem a coleta, o armazenamento, e o tratamento de dados pessoais em larga escala, feito por mecanismo de inteligência artificial (IA) essa que é considerada a "nova na arena dos Direitos Humanos" (PINTO; NOGUEIRA, 2023, p.308).

Inclusive, o reconhecimento facial, fomenta o debate sobre o equilíbrio entre segurança pública, eficiência estatal e a defesa de direitos fundamentais, como a privacidade, a salvaguarda de informações pessoais e a autodeterminação informativa. Sendo, portanto a preservação dos dados biométricos um direito

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

humano e primordial híbrido uma vez que constitui uma não intervenção arbitrária - prestação negativa de defesa, pois está intrinsecamente ligado a privacidade (autodeterminação informativa), e ao mesmo tempo prestação positiva ligada a obrigação de fazer por parte do Estado, mediante políticas públicas.

Sendo assim compete ao Legislativo, Executivo e Judiciário no âmbito de suas respectivas funções assegurar "sua máxima eficácia e efetividade concreta, tanto na condição de direito subjetivo negativo [...], quanto, por força de sua dimensão objetiva, levando a sério os respectivos deveres de proteção" (SARLET, 2020, p.27). Logo, o direito à tutela das informações pessoais sensíveis, mais especificamente, dados biométricos em face do reconhecimento facial compõe a quarta geração de direitos humanos, apesar de fazer parte também do campo da privacidade que está na primeira dimensão.

3. A PRIVACIDADE E SEUS FUNDAMENTOS: DA TUTELA DE DADOS E DA AUTODETERMINAÇÃO INFORMATIVA

A privacidade é direito público subjetivo de primeira dimensão, compõe o grupo das prerrogativas civis e políticas, consiste em obrigação de não fazer por parte do Estado, assim, o sujeito de direitos deverá ser livre para exercer sua privacidade sem interferência do Estado e suas nuances são: a intimidade, a honra, a imagem, a vida privada, a salvaguarda de dados e a autodeterminação informativa. Não obstante à privacidade também integra o conjunto dos direitos a personalidade e "não possui um conteúdo fixo, ele é capaz de oferecer proteção diferenciada de acordo com a intervenção na vida privada. Logo, sua abstração se torna sinônimo de adaptabilidade" (MENDES, 2020, p. 16).

Nesse contexto o art. 5º, X, XII, XII da Constituição Federal de 1988 (CF/88) consagra o direito essencial à privacidade em consonância com o art. 12º da DUDH, com o art. 8º Convenção Europeia dos Direitos do Homem, com o art. 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, e com o art. 11º do Pacto de São José da Costa Rica ou Convenção Americana de Direitos Humanos, promulgada no Brasil mediante o Decreto nº 678 de 06 de novembro de 1992. Dessa maneira, é um valor universal e relevante para a humanidade.

Embora, "o Código Civil explicite, em seu artigo 21, a proteção da privacidade apenas sob a alcunha da vida privada [...]" (DE CHAVES; DE SÁ; JANINI, 2024, p.8) Ou seja, o direito à privacidade possui várias nuances e não se limita ao que está expresso nesse texto normativo, pois implicitamente há outros contornos para além desse artigo, como por exemplo a autodeterminação informativa e isso é reflexo da evolução dessa prerrogativa. Uma vez que com o decurso do tempo vão emergindo outros aspectos que merecem

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

tutela jurídica e despertam o interesse e a preocupação da doutrina e por consequência são levados até o legislador que deverá se debruçar sobre o tema e dar uma resposta a sociedade positivando o anteparo jurídico específico para salvaguardar essa nova nuance da privacidade.

Nesse caminho, à privacidade inicialmente associada à proteção da intimidade e, por conseguinte à autodeterminação informativa, passou por uma redefinição diante das transformações tecnológicas que impactam diretamente a tutela dos direitos fundamentais, ou seja, o conceito de privacidade tornou-se mais liquido e complexo devido aos avanços da inteligência artificial (VIEIRA, 2023).

Destarte, o desenvolvimento de inteligências artificiais capazes de coletar, processar, armazenar e compartilhar grandes volumes de informações, a saber, big data, em tempo real ampliou os desafios regulatórios, exigindo a reformulação das normativas nacionais e internacionais para conciliar a custódia da privacidade com a segurança pública e a eficiência tecnológica. Isso porque: “qual é o poder que o indivíduo tem sobre o fluxo dos dados pessoais de sua titularidade, visto que, na virtualização das relações humanas apresenta, há a tendência de serem esmaecidos os limites entre o público e o privado” (VIEIRA, 2023, p.7). Destarte, “à privacidade também está em risco” (PINTO; NOGUEIRA, 2023, p.309).

> Com esses conjuntos gigantescos de dados disponíveis, isso significa que as pessoas estão compartilhando informações sem precedentes que prefeririam manter privadas. A vigilância em massa de câmeras, o reconhecimento facial e a coleta descontrolada de dados de mídia social tem sido usados para ameaçar as oportunidades das pessoas, minar sua privacidade ou rastrear de forma generalizada suas atividades, muitas vezes sem seu conhecimento ou consentimento (PINTO; NOGUEIRA, 2023, p.309).

Nesse contexto, o reconhecimento da privacidade como um direito inalienável e imprescritível, inclusive no plano internacional, deve ser revisitado à luz dos novos ricos presentes nos meios digitais, que não apenas permitem a coleta massiva de dados pessoais, mas também reforçam riscos como discriminação algorítmica, hipervigilância estatal, vazamento e a comercialização de informações (PINTO; NOGUEIRA, 2023). Deste modo, a tutela da privacidade atualmente requer abordagem multidisciplinar, capaz de sopesar as vantagens das inovações tecnológicas com a preservação dos direitos fundamentais.

> A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por lhe dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão (FERRAZ JR, 2022, p.1).

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Ou seja, à privacidade para além de ser um direito básico é um princípio que norteia o ordenamento jurídico, e ganha novos contornos com o desenvolvimento das tecnologias, assim “a sua compreensão foi ampliada para incluir a proteção de dados pessoais, como reconhecido pelo STF, que entendeu que o direito à privacidade abrange também o direito à autodeterminação informativa” (PEREIRA, OLIVEIRA, 2025, p.17). Nessa perspectiva a prerrogativa da privacidade possui vários aspectos, seja como direito da personalidade, fundamental ou humano, assim, protegida em diferentes regulamentos (DE CHAVES; et al., 2024).

Todavia, a tutela do direito à privacidade não é absoluta e admite mitigações em determinadas circunstâncias, a saber:

> [...] a publicação de matéria que fosse de interesse geral ou público [...]; publicação de fatos de cunho privado se realizada dentro de circunstâncias autorizadas pela lei [...]; não teria o condão de impossibilitar a divulgação oral sem danos ao titular; e também não alcançaria a publicação de fatos da vida privada promovida pelo próprio titular (NUNES, 2022. p.87).

Por exemplo, para participar de programas de televisão como Big Brother Brasil ou A Fazenda nos quais as pessoas por vezes abrem mão de aspectos da sua privacidade por determinado tempo em virtude do sonho de ganhar dinheiro, fama ou projeção nacional, esses são exemplos clássicos de vigilância digital. Porém, “a vigilância de hoje ocorre de maneira mais discreta, tornando a oposição mais difícil e tendente a criar servos dóceis” (MARINI; COLVARA. 2024. p.12)

Nesse caminho, a Carta Maior foi modificada através do poder constituinte derivado reformador para incluir a defesa das informações, sejam elas físicas ou virtuais como direito basilar autônomo reforçando a autodeterminação informativa das pessoas. Nessa perspectiva, “dá uma resposta convincente à abordagem crítica da relatividade da esfera privada, pois se trata exclusivamente do poder do titular do direito, e não mais da atribuição de dados à esfera privada” (MENDES, 2020. p.16).

Dessa forma o “direito à autodeterminação informativa está relacionado com o exercício do direito fundamental à proteção de dados pessoais” (VIEIRA, 2023. p. 16), isto é, a liberdade que as pessoas têm para decidir o que fazer com suas informações pessoais sem a interferência do Estado ou da sociedade, sobretudo em relação aos seus dados pessoais sensíveis. Não obstante, “o Estado deve prover meios de proteger à privacidade dos cidadãos, pois este se constitui em um direito fundamental, associado ao desenvolvimento livre da personalidade” (SOUSA; SILVA. 2020. p.11).

Segundo Harari:

> Se você concentrar toda a informação relativa a 1 bilhão de pessoas numa única base de dados, desconsiderando qualquer preocupação com privacidade, será capaz de instruir

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

> muito mais algoritmos do que se respeitasse a privacidade individual e tivesse em sua base de dados apenas informações parciais sobre 1 milhão de pessoas (2018. p.63)

Ou seja, o respeito à privacidade parece ser um empecilho ao desenvolvimento de tecnologia artificial de coleta massiva de informações privadas, pois quanto mais informações disponíveis de forma indiscriminada mais os algoritmos conseguem trabalhar para processá las. O reconhecimento facial, por sua vez, espécie de dado biométrico que utiliza de uma série de métodos, tecnologias e de cruzamento de informações estatísticas para identificar uma pessoa através de seus traços físicos "(tais como impressão digital, face, íris, geometria e vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura etc.)" (CEBRIAN; PRUDENTE; GUEDES; DA SILVA; SÁ; MORAES, 2024, p.12), tem sido amplamente empregado em setores como segurança pública, controle de acesso e personalização de serviços.

Nesse sentido, sobre o conceito de reconhecimento facial: "[...] são o conjunto de ferramentas digitais usadas para executar tarefas em imagens ou vídeos de rostos humanos" (SHARFI, 2023. p. 223). Nessa senda, o art. 5º, II da LGPD, disciplina que dado pessoal sensível é aquele que identifica a pessoa natural no que diz respeito a sua:

> 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 (BRASIL, 2018).

Sendo assim, o reconhecimento facial é uma modalidade de biometria e, por conseguinte, dado pessoal sensível. Nessa direção, assevera o art. 2º da LGPD um conjunto de princípios a serem observados na tutela dos dados pessoais, a saber:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Desta forma, "o Brasil ingressa no grupo de nações que possuem uma legislação específica para salvaguardar os dados pessoais e à privacidade de seus cidadãos" (LIMA, 2023. p.41). Ademais, a LGPD inspirou-se em outras legislações alienígenas como o Regulamento Geral em relação a Proteção de Dados

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

(GDPR) na União Europeia que vigora desde maior 2018 e o Califórnia Consumer Privacy Act of 2018 (CCPA) nos Estados Unidos da América que entrou em vigor em junho de 2018 (LIMA, 2023).

Assim, “o direito à proteção de dados pessoais, representa um amadurecimento das concepções de vida privada e de intimidade, e juntamente com o direito à autodeterminação informativa, passa a integrar o núcleo dos direitos da personalidade” (NUNES, 2022. p.88) Além do mais, no plano internacional a regulamentação do tratamento de dados pessoais ganhou reforço com o compromisso firmado na União Europeia, denominado de Convenção 108 + do Conselho da Europa.

Entretanto antes mesmo do advento da LGPD o Marco Civil da Internet Lei n.º 12.965/2014 trouxe contribuição significativa para a tutela da privacidade na internet no Brasil, “como a necessidade de consentimento do titular das informações para o seu tratamento, a transparência no uso dos dados, [...] e a responsabilização das empresas em caso de violação” (CORREIA, 2023. p. 37).

Nessa senda, o reconhecimento facial, enquanto tecnologia biométrica avançada tem sido empregado na segurança pública, permitindo a identificação automatizada de indivíduos por meio da análise de características faciais. Seu funcionamento baseia-se na conversão de informações biométricas do rosto de pessoas em códigos numéricos únicos, que são comparados por grandes bancos de dados para validação da identidade (COSTA; OLIVEIRA, 2019).

Nessa direção, a incorporação da inteligência artificial nesse processo potencializa a acurácia das análises, viabilizando investigações criminais mais rápidas e precisas, além de auxiliar na localização de foragidos e na construção de perfis comportamentais (YAROVENKO; SHAPOVALOVA; ISMAGILOV, 2021). Porém, a tecnologia não é totalmente isenta de erros, pois pode haver falso positivo na análise automatizada dos dados bem como discriminação algorítmica, em virtude alguns grupos de pessoas, como por exemplo, negros, asiáticos, crianças e idosos serem identificados como suspeito sem ser.

Além disso, apesar da LGPD e da Constituição Federal de 1988 ter consagrado a proteção de informações pessoais como um direito fundamental, revela-se imprescindível a criação de normas específicas que regulem a utilização de algoritmos de inteligência artificial para o reconhecimento facial automatizado em espaços públicos e privados. Essa necessidade decorre dos potenciais riscos associados a essa tecnologia, especialmente no que concerne à segurança e aos direitos de minorias e grupos sociais marginalizados, até porque “existe uma monetização no tratamento dos dados pessoais, ou seja, no reconhecimento de que essas informações pessoais são uma commodity na contemporaneidade” (NUNES, 2022. p.86).

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Nessa direção, a preocupação encontra respaldo nas diretrizes adotadas pela União Europeia e mencionadas anteriormente, as quais enfatizam a urgência de limites normativos mais claros para mitigar essas vulnerabilidades (DE MACEDO, 2023).

Consequentemente, essa expansão tecnológica ao mesmo tempo em que possui vantagens “uma vez que diferentes empresas e órgãos governamentais vêm adotando esse tipo de tecnologia como forma de proteção de indivíduos e dados” (SOUZA, 2020, p.18), suscita desafios éticos e jurídicos, especialmente no que concerne à privacidade e à defesa de informações sensíveis. Por exemplo, na ausência de conhecimento ou consentimento explícito na coleta de informações biométricas - e por vezes consentimento viciado - e a possibilidade de uso indevido dessas bases de dados evidenciam riscos à autodeterminação informativa dos cidadãos. Ademais, a falibilidade dos algoritmos, quando treinados com conjuntos de dados enviesados, pode resultar em falhas de identificação e discriminação sistêmica, reforçando estereótipos e ampliando desigualdades sociais (ATTANASIO; STEFFEN, 2023).

Dessa forma, o uso do reconhecimento facial requer uma regulamentação específica que pondere a relevância do emprego de recursos tecnológicos com o respeito aos direitos humanos, combatendo violações. Não obstante, muitos casos envolvendo a tutela da autodeterminação informativa, podem ser resolvidos com a aplicação da interpretação sistemática do arcabouço normativo em vigor atualmente, a saber, Código de Defesa do Consumidor, Lei de Acesso a Informação, LGP, Marco Civil da Internet (MCI), a Lei do Cadastro Positivo, Código Penal, entre outras normas (SHARFI, 2023).

4. O USO DO RECONHECIMENTO FACIAL E AS IMPLICAÇÕES ÉTICAS E LEGAIS

Na seara civil a tecnologia de inteligência artificial de coleta de informações biométricas da face pode ser usada para diversas finalidades, quais sejam, identificar animais, identificar pessoas através de drones, controle de benefícios e gratuidades no transporte público coletivo, controle da frequência de alunos nas escolas e de trabalhadores, autenticação de aplicativos financeiros no mobile banking- uma das formas de acessar os serviços a bancários através do sistema remoto, senha ou PIN de smartphones, como senha bancária, para celebrar negócios jurídicos e até mesmo como assinatura, reflexo de um mundo cada vez mais digital e:

> Em uma sociedade que é comprovadamente menos formalista, na qual as pessoas não mais se individualizam por sua assinatura de próprio punho, mas, sim, pelos seus tokens, chaves, logins e senhas, ID's, certificações digitais, reconhecimentos faciais, digitais e

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

> oculares e, até mesmo, pelos seus hábitos profissionais, de consumo e de vida captados a partir da reiterada e diária coleta de seus dados pessoais, e na qual se admite a celebração de negócios jurídicos complexos e vultosos até mesmo por redes sociais ou por meros cliques, o papel e a caneta esferográfica perdem diariamente o seu valor e a sua relevância, devendo ser examinados em conjunto com os demais elementos que permitam aferir ser aquela a real vontade do contratante. (REsp n. 1.633.254/MG, relatora Ministra Nancy Andrighi, Segunda Seção, julgado em 11/3/2020, DJe de 18/3/2020.)

A saber, no controle de fronteiras e aeroportos- possibilita maior eficiência nos processos de verificação de identidade, concessão de entrada, registro de saída e procedimentos como embarque e check-in, além de viabilizar a identificação de pessoas sujeitas a restrições legais ou mandados judiciais pendentes (CEBRIAN; PRUDENTE; GUEDES; DA SILVA; SÁ; MORAES, 2024).

Nesse sentido, nas transações financeiras e pagamentos, a biometria facial e digital “pode ser utilizada para autorizar e confirmar transações financeiras ou pagamentos, proporcionando uma camada extra de segurança” (CEBRIAN et al., 2024, p.14). Por exemplo, o sistema gov.br do governo federal brasileiro utiliza a tecnologia biométrica como forma de autenticação do usuário em duas etapas. Além disso, no comércio, permite a personalização de anúncios e promoções com base nos interesses e no comportamento do consumidor, viabilizando experiências mais individualizadas ao ingressar em estabelecimentos comerciais (CEBRIAN, et al., 2024,).

Ademais, as tecnologias biométricas viabilizam o controle de acesso a edificações, espaços restritos e instituições públicas, além de otimizar o monitoramento da jornada de trabalho, garantindo maior precisão e segurança. Todavia, seu uso crescente levanta preocupações sobre o equilíbrio entre as vantagens do avanço tecnológico e a salvaguarda da privacidade e seus desdobramentos.

Nesse cenário, “as técnicas de reconhecimento facial conseguem extrair o indivíduo da massa, identificá-lo e segui-lo” (PINTO; NOGUEIRA, 2023. p.81) assim, a responsabilidade civil das entidades que tratam dados pessoais se torna imprescindível, não apenas para reparar os danos, mas também para garantir conformidade com os direitos constitucionais e o princípio da boa-fé objetiva e seus deveres jurídicos anexos, a saber, transparência, confiança, lealdade, informação, assistência, cooperação, consentimento e etc. Porém, não há legislação que consiga proteger totalmente a autodeterminação informativa das pessoas, por isso a relevância do comportamento ético por parte de órgãos públicos e entidades privadas na coleta dessas informações.

Em 2023 a União, a Caixa Econômica Federal, a Empresa de Tecnologia e Informações da Previdência Social (DATAPREV), e a Autoridade Nacional de Proteção de Dados (ANPD) foram condenados pela Justiça

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Federal de São Paulo pelo vazamento de milhares de dados de usuários do sistema Caixa Tem no bojo da Ação Civil Pública, processo nº 5028572-20.2022.4.03.6100. Logo a responsabilidade civil deve ser revisitada e adaptada para danos ocorridos no ambiente digital na perspectiva de reparação e prevenção aos danos causados.

Nessa conjuntura, a autodeterminação informativa se consagra como direito humano na atualidade, sobretudo à luz da LGPD e do MCI, pois garante ao titular de direitos o controle sobre suas informações pessoais, prezando pelo consentimento informado e pela boa fé no tratamento, armazenamento e coleta das informações.

Contudo, a coleta e utilização indevida dessas informações pessoais, como exemplificado por práticas de comercialização sem autorização ou o uso de biometria sem consentimento específico, configuram graves violações dessa autonomia, refletindo-se tanto em danos patrimoniais quanto extrapatrimoniais. Isto é, a coleta massiva de dados pela economia digital reduz as liberdades (de expressão, informação e comunicação) e a privacidade (DE MACEDO, 2023). Entretanto, esse conjunto de dados pode ser usado de forma benéfica, por exemplo, para prever tendências, reconhecer padrões e estabelecer métricas a fim de otimizar determinadas profissões, até mesmo na advocacia através da jurimetria.

Não obstante, “as críticas envolvem a necessidade de transparência no uso da tecnologia, de garantias das liberdades individuais e no risco de aplicações com desvios discriminatórios”(PINHEIRO, 2021. p.95). Isto é, não pode-se conceber a suplantação de direitos fundamentais indisponíveis pela ausência de clareza no emprego das tecnologias. Por isso a LGPD, disciplina elementos relevantes como “os princípios, os usos, as hipóteses permitidas, os casos de anonimização e a revisão do tratamento automatizado, são fundamentais para evitar abusos” (PINHEIRO, 2021, p.95).

Nessa direção,

> O assunto privacidade não é de fácil explanação e apresenta um nível de complexidade típico da sociedade atual, em que ao mesmo tempo que se valoriza o poder do indivíduo também se amplia o uso de escutas, câmeras, GPS, softwares de rastreamento4. (PINHEIRO, 2021, p. 84)

Isto é, as novas tecnologias elevaram o nível de complexidade do direito à privacidade, e mais especificamente, o direito à proteção de dados, não obstante o grau de importância da prerrogativa, visto que é essencial a todos. Ademais, “o impacto da qualidade das informações que representam essas categorias nos usos futuros desses dados” (BRANCO; TEFFÉ, 2025, p.363).

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Por sua vez, na seara penal, a utilização de tecnologias de reconhecimento facial por exemplo pode ser usada para identificar cerimoniosos e coibir a criminalidade para combater fraudes, identificar vítimas, fazer flagrante de delito de alguns crimes, encontrar pessoas desaparecidas, “a IA também pode produzir um reconhecimento facial que poderá fundamentar uma decisão sobre liberdade provisória” (PINTO; NOGUEIRA, 2023, p.72) apesar de na segurança pública provoca preocupações quanto à privacidade, transparência no uso dessas informações.

Nesse caminho, a vigilância massiva pode contribuir para a discriminação algorítmica - reproduzindo preconceitos e gerando tratamento diferenciado, por exemplo, a depender do estereotipo da pessoa e por vezes pessoas negras, asiáticas e mulheres podem ser alvo de discriminação em decorrência da má apuração da ferramenta e altos níveis de erros, mesmo que haja a utilização do aprendizado de máquina, onde a ferramenta aprende pela repetição da verificação dos padrões dos rostos humanos “porque o aprendizado de máquina funciona melhor quanto mais informação for capaz de analisar” (HARARI 2018, p.63) e por vezes esses erros estão na programação da máquina. Além disso, esse risco é acentuado quando a tecnologia é utilizada por forças de segurança, uma vez que pode gerar abordagens indevidas e apreensão de pessoas inocentes que eventualmente foram identificadas de forma errônea pela tecnologia.

> Aqui, os vieses algorítmicos são considerados tendências ou distorções presentes em algoritmos de IA, que resultam em decisões injustas ou equivocadas. Alguns exemplos incluem algoritmos de seleção de candidatos que tendem a favorecer candidatos de raças e gêneros dominantes, sistemas de reconhecimento facial que têm dificuldade em reconhecer pessoas negras e sistemas de crédito que têm menos chances de conceder empréstimos a pessoas de raças minoritárias (PINTO; NOGUEIRA, 2023, p.86)

Ou seja, o uso enviesado de algoritmos ou a falha nos sistemas de reconhecimento facial, intensificam os impactos dessa violação, criando riscos à identidade e à integridade dos indivíduos, ao mesmo tempo em que revelam a necessidade de uma regulamentação mais efetiva para a preservação dos dados biométricos.

Porém, “o aprendizado de máquina pode nos ajudar a detectar padrões de corrupção para apoiar a defesa, [...] e analisar evidências de violações dos direitos humanos para a justiça de transição” (PINTO; NOGUEIRA, 2023, p.308). Isto é, a tecnologia de inteligência artificial pode auxiliar no combate a ofensa de prerrogativas fundamentais, embora apenas emule ou reproduza o aprendizado humano.

Nessa conjuntura, a precisão dos sistemas de reconhecimento facial revela uma sensível vulnerabilidade diante de variáveis técnicas e contextuais que interferem diretamente em seu desempenho. Por exemplo, fatores como condições de iluminação inadequadas, plano de fundo desfavorável e posicionamento irregular

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

do indivíduo na imagem demonstram potencial para comprometer a acurácia do processo de identificação. Ademais, a homogeneidade fenotípica acentua tal fragilidade, especialmente quando as imagens são extraídas de registros audiovisuais, cenário que intensifica a probabilidade de ocorrência de falsos positivos (LIMA, 2023), bem como falso negativo - onde a tecnologia pode não identificar que a pessoa é ela mesma.

Nesse contexto, o sistema pode, equivocadamente, associar um rosto analisado a uma pessoa distinta daquela retratada na imagem original, evidenciando um risco concreto à segurança jurídica e o resguardo de direitos fundamentais (LIMA, 2023). Por vezes, a falta de diversidade na base de treinamento das inteligências artificiais compromete a precisão dos modelos, reforçando padrões discriminatórios históricos e agravando desigualdades estruturais, ou seja “expondo a fragilidade de algoritmos que, ao replicar preconceitos e estereótipos, tornam-se instrumentos de injustiça” (LIMA, 2023, p.59).

Nesse sentido é necessário revisões humanas ao sistema de reconhecimento facial que deve ser usado como forma de apoio e não como método absoluto para identificação de pessoas, assim na interação entre tecnologia e decisões humanas torna imprescindível uma abordagem ética e rigorosa na aplicação dessas ferramentas, demandando auditorias independentes e mecanismos de controle para evitar a consolidação de injustiças sistêmicas.

Em especial, na área da segurança pública, o emprego da tecnologia deverá ser marcado pelos princípios da boa-fé, da proporcionalidade e a observância dos direitos humanos, de modo a mitigar os riscos de discriminação e garantir que sua aplicação ocorra dentro dos limites Ordemento Jurídico.

Nesse ponto, importante ponderar a distinção entre: a verificação “consiste na comparação direta da imagem de uma pessoa desconhecida e uma imagem de referência de uma pessoa conhecida” (SOUZA, 2020, p. 5), por exemplo, para desbloquear o celular, computadores etc; e a identificação “consiste em uma comparação da imagem de uma pessoa desconhecida com todas as imagens de um banco de dados de indivíduos conhecidos” (SOUZA, 2020, p. 5),- muito utilizado em casos forenses.

Nesse contexto, a empresa Tools for Humanity, está desenvolvendo um projeto que usa padrões da íris humana para criar um código de validação impossível de ser desbloqueado por IA. Essa mesma entidade criou uma supercâmera capaz de coletar esses dados biométricos da íris das pessoas e distinguir humanos e robôs. Para isso está atraindo pessoas que fornecem o “escaneamento” da sua íris para o experimento em troca de dinheiro ou criptomoedas. Porém a ANPD, interveio, aplicando a medida preventiva de suspensão do pagamento para a coleta da íris, por entender que há grave violação do consentimento do titular de informações pessoais, uma vez que esse consentimento não fora livre nem desembaraçado, além de não permitir o apagamento posterior dessas informações, tratando-se de dados sensíveis.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Portanto, o uso de reconhecimento facial requer cautela e ética a fim de preservar, sobretudo a privacidade das pessoas tendo em vista que estão sujeitas a vazamentos, roubos dos dados pessoais e, por conseguinte, a violação de direitos humanos, pois por vezes esse sistema não pede permissão para fazer a captura e escaneamento das imagens, inclusive essas fotos podem ser usadas para fazer deepfake, isto é ,“tenta-se imitar as características acústicas da voz, as feições e movimentos do rosto para parecer uma imagem real” (MENEZES, 2024. p. 16).

5. DIRETRIZES PARA UMA REGULAMENTAÇÃO EFETIVA

Nessa linha de raciocínio tramita no Congresso Nacional um projeto de lei que prevê maior rigor na defesa dos dados biométricos e proíbe a comercialização de informações sensíveis, qual seja, o Projeto de Lei 36/2025. Esse projeto prevê alterar alguns artigos da LGPD com o objetivo de endurecer a tutela das informações pessoais sensíveis, a saber:

> XII-A – Dado biométrico sensível: dado pessoal resultante de tratamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa, que permita ou confirme sua identificação única, tais como impressão digital, reconhecimento facial, íris, voz ou DNA. XII-B – Comercialização de dados biométricos sensíveis: qualquer forma de transferência, cessão, aluguel, venda ou disponibilização, mediante pagamento ou contraprestação de qualquer natureza, de dados biométricos sensíveis (BRASIL, 2025).

Nessa direção o art. 7º da Resolução 332 do Conselho Nacional de Justiça (CNJ) disciplina que as decisões judiciais fundamentadas em IA devem:

> preservar a igualdade, a não discriminação, a pluralidade e a solidariedade, auxiliando no julgamento justo, com criação de condições que visem eliminar ou minimizar a opressão, a marginalização do ser humano e os erros de julgamento decorrentes de preconceitos (BRASIL, 2020. p.1)

Por seu turno, a Defensoria Pública do Estado de São Paulo através do Núcleo Especializado de Cidadania e Direitos Humanos questionou o uso da tecnologia na ação da Prefeitura de São Paulo de monitoramento através de câmeras com reconhecimento facial para identificar criminosos e coibir furtos no carnaval de São Paulo de 2025 denominada de “Smart Sampa” e requereu o seguinte:

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

> 1.Não sejam utilizadas tecnologias de reconhecimento facial e outros sistemas biométricos para identificar indivíduos que participam pacificamente de um bloco; 2. Não sejam utilizadas tecnologias digitais para categorizar, perfilar ou identificar remotamente indivíduos, inclusive por meios biométricos, durante manifestações, uma vez que são discriminatórias e inconsistentes com a obrigação dos responsáveis pela manutenção da ordem de facilitar manifestações pacíficas; 3. O uso de tecnologias digitais tenha como objetivo exclusivo permitir o direito à liberdade de reunião pacífica; 4. Seja garantido um registro transparente e auditável de todas as decisões pertinentes sobre tecnologias digitais; [...] (DEFENSORIA PÚBLICA DE SÃO PAULO. 2025. p. 5 e 6 Oficio nº 020/2025 DPE SP.).

Nesse contexto o Colendo Supremo Tribunal Federal (STF), firmou Tese de Repercussão Geral no julgamento do ARE 1467470 RG/SP, na qual entendeu que de acordo com a constituição é importante saber se o reconhecimento pessoal por meio fotográfico está sendo realizado no processo penal está conformidade com o art. 226 do Código de Processo Penal em observância aos princípios do devido processo legal, da ampla defesa e da vedação às provas ilícitas.

Por sua vez o CNJ na Resolução nº 484/2022 estabeleceu as diretrizes para o uso do reconhecimento pessoal por meio fotográfico e registrou que “o reconhecimento de pessoas equivocado é uma das principais causas de erro judiciário” (BRASIL, 2022. p.1) o que acende o alerta sobre o reconhecimento feito por inteligência artificial, uma vez que o reconhecimento feito por ser humano já não é totalmente seguro, quiçá, o feito por máquinas inclusive quando essas máquinas são enviesadas por quem alimenta a sua programação.

Entretanto, a Lei nº 14.597 de 2023, denominada de Lei Geral do Esporte no art. 148 impôs o reconhecimento facial de pessoas em estádio de futebol com capacidade acima de vinte mil pessoas, exceto para menores de dezesseis anos, de acordo com o art. 158, XII da mesma lei, o que, por sua vez, exigirá altos investimentos financeiros na estrutura desses estádios para atender as determinações legais. Dessa forma, o uso da biometria contribuiria para dar mais segurança aos torcedores, diminuir as filas facilitando a entrada das pessoas nos estádios e, por conseguinte, combater crimes como assédio sexual.

Não obstante, “os dados biométricos coletados nos estádios são compartilhados entre diversas empresas sem qualquer transparência a respeito da garantia da privacidade e segurança dessas informações” (SOUZA, 2024. p.43). Desta forma não se sabe ao certo o que é feito com essas informações coletadas em estádios de futebol, o que revela a vulnerabilidade dos torcedores que são obrigados a ceder seus dados sem consentimento ou informação. Nessa senda:

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

> a situação torna-se ainda mais assustadora quando damos conta que crianças e adolescentes também têm seus dados coletados pelos clubes e compartilhados por inúmeras empresas sem o devido consentimento dos responsáveis e, igualmente, sem qualquer garantia de privacidade e protocolos de segurança de dados (SOUZA, 2024. p.43).

Ou seja, dados sensíveis de menores de dezoito anos são coletados, processados, armazenados e utilizados inclusive para publicidade sem o consentimento prévio de seus pais o que macula o Estatuto da Criança e do Adolescente (ECA), o postulado da privacidade e a LGPD. “Embora alguns torcedores apontem elementos positivos na adoção do controle de dados biométricos para acesso aos estádios, [...] não são dependentes dessa tecnologia” (SOUZA, 2024, p.45) Isso porque a tecnologia é uma relevante ferramenta de segurança e monitoramento em espaços privados e públicos.

Aliás, há décadas os jogos de futebol, entre outros esportes são transmitidos em tempo real pela televisão e, por vezes, gravados, nos quais há a captura da imagem de torcedores que estão assistindo a partida, possibilitando o reconhecimento de tais espectadores - ainda que em escala bem menor que a tecnologia de reconhecimento biométrico. Para mais, atualmente essas transmissões também são veiculadas pela rede mundial de computadores através das redes sociais, bem como de serviços de streaming.

Por outro lado, não é o que concluiu a pesquisa do Centro de Estudos de Segurança e Cidadania, pelo contrário segundo o estudo o uso da tecnologia de reconhecimento facial nos estádios “serve a um amplo processo de datificação, [...] falta de segurança no armazenamento dos dados, viés racial tecnológico e a hipervulnerabilização de crianças e adolescentes” (SOUZA, 2024, p.45). Inclusive no relatório os pesquisadores sugeriram alguns pontos para a garantia dos direitos humanos, dentre eles destaca-se que “todos os torcedores sejam devidamente informados e forneçam consentimento explícito antes de terem seus dados coletados e processados por sistemas de reconhecimento facial” (SOUZA, 2024, p.45).

Sendo assim, o consentimento se revela essencial quando o assunto é coleta de informações biométricas, haja vista a sensibilidade desses dados como preconiza a LGPD, a fim de preservar a autodeterminação informativa dos sujeitos de direitos, inclusive em alguns casos o consentimento é “a única base legal viável a justificar o tratamento de dados pessoais” (NUNES, 2022. p.232).

Nesse contexto de acordo com o II, "g", artigo 11, da LGPD, há fundamento para o uso da tecnologia para tratamento de dados biométricos, a saber, para “garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, [...]” (BRASIL, 2018).

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Destarte, a norma de Regulamentação da Inteligência Artificial da União Europeia veda o uso da tecnologia em situações que exponham as pessoas a danos físicos ou psicológicos severos, a saber, a coleta de dados biométricos em tempo real com a finalidade de vigilância em massa (CRUZ, 2023, p. 5). Ademais, a Convenção 108+ do Conselho da Europa, define no art. 6º que "o tratamento de dados biométricos que identifiquem uma pessoa de forma inequívoca só será permitido se estiverem previstas na lei garantias apropriadas que complementem as previstas na presente Convenção" (CONSELHO DA EUROPA, 2018, p.4).

Todavia, a efetividade normativa de qualquer proposta legislativa depende, de forma indissociável, de sua aplicação coerente e de sua aptidão para se ajustar às transformações contínuas do contexto tecnológico e social (CRAVO; CUNDA; RAMOS, 2021). Diante disso, impõe-se a necessidade de uma atuação coordenada entre os diversos atores envolvidos - incluindo o Estado, a iniciativa privada, a sociedade civil e os especialistas na área tecnológica - , no sentido de construir um marco regulatório sólido e ao mesmo tempo adaptável, capaz de enfrentar, com profundidade e abrangência, os múltiplos impactos advindos do uso da inteligência artificial (CRUZ, 2023).

Nesse sentido, estamos diante da "necessidade de se prever em lei a revisão humana das decisões automatizadas como imperativo ético para exercício do Direito a não discriminação" (DE MACEDO, 2023, p.2). Não obstante o dever da Autoridade Nacional de Proteção de Dados de fiscalizar, criar e implementar padrões técnicos mínimos para viabilizar a efetiva custódia dos direitos humanos no que diz respeito aos dados biométricos em face do avanço do reconhecimento facial.

Ademais, do ponto de vista ético o desenvolvimento da inteligência artificial do reconhecimento facial deve submeter-se em quaisquer casos a verificação do ser humano, não sendo aceitável que decisões automatizadas com potencial de afetar direitos fundamentais ou comprometer a vida das pessoas sejam tomadas sem a intervenção de um agente humano (DE MACEDO, 2023).

Isso porque os sistemas de IA, por mais avançados que sejam, carecem de competências essenciais à justiça, como a capacidade de avaliar a adequação contextual de suas previsões, realizar juízos de igualdade, inclusive material ou ponderar valores em face das singularidades do caso concreto, pois sua atuação baseia-se em emulações e critérios pouco transparentes, sobretudo quando moldados por interesses enviesados de seus desenvolvedores, o que por vezes pode gerar discriminação (DE MACEDO, 2023).

Por essa razão, a definição das hipóteses em que decisões automatizadas possam prescindir da cognição e da sensibilidade humanas deve ser regulada com rigor, mediante previsão legal expressa e

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

criteriosa análise de risco, assegurando-se, em qualquer cenário, a primazia da dignidade humana nos processos de automação (DE MACEDO, 2023).

Ademais, o reconhecimento facial apresenta desafios significativos para a defesa da privacidade e dos dados pessoais. Outrossim, a hipótese de que sua expansão pode comprometer esses direitos se confirma diante das lacunas regulatórias e do risco de uso abusivo. No entanto, diretrizes adequadas podem mitigar tais riscos e permitir uma utilização responsável da tecnologia. Posto isto, é essencial um esforço conjunto entre governos, sociedade civil e setor privado para garantir que o avanço tecnológico ocorra sem ofensas aos direitos fundamentais.

Logo, o desenvolvimento de tecnologias mais precisas e menos discriminatórias deve ser incentivado, inclusive a cooperação internacional também se faz essencial para harmonizar padrões regulatórios.

6. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

O presente trabalho almejou analisar como objetivo geral o impacto da tecnologia de reconhecimento facial na tutela dos direitos humanos, com fulcro no direito fundamental à proteção de dados pessoais por meio da revisão integrativa da literatura de natureza exploratória utilizando-se de livros digitais e físicos, sites de notícias e do governo, periódicos digitais, bem como julgados relevantes dos tribunais superiores relacionados a temática.

Cumpre registrar que os objetivos específicos foram os seguintes: inicialmente traçar breves considerações sobre a existência e o desenvolvimento dos direitos humanos, bem como identificar em qual(is) dimensão(ões) a tutela de dados se encaixa no primeiro tópico; investigar os fundamentos humanos do direito à privacidade e suas nuances, a saber, autodeterminação informativa e proteção de dados pessoais no segundo tópico; analisar o uso do reconhecimento facial e as implicações éticas e legais no terceiro tópico; e estudar as diretrizes para uma regulamentação eficaz que concilie a segurança proporcionada pelo reconhecimento facial com a preservação do direito humano à salvaguarda de dados no último tópico.

Constatou-se que as lacunas normativas comprometem o direito humano à autodeterminação informativa, assim na coleta, armazenamento e tratamento de informações biométricas é necessário boa-fé, e seus deveres jurídicos anexos de lealdade, transparência, informação, e consentimento prévio. Bem como há riscos de discriminação algorítmica que afetam principalmente determinados grupos negros, mulheres, e crianças estão sujeitos a falsos positivos. Além disso, constatou-se a ausência de transparência

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

no uso da tecnologia em estádios de futebol, o que pode ensejar o vazamento e, por conseguinte, a comercialização dessas informações. Dessa forma, torna-se necessário que a LGPD seja alterada para endurecer a tutela dos dados biométricos e coibir a comercialização dessas informações a fim de salvaguardar a autodeterminação informativa de acordo com o PL 36/2025. Para além da regulamentação específica é necessário o controle humano sobre a coleta, o armazenamento e o tratamento dessas informações através de auditorias frequentes, independentes e revisões humanas periódicas com a finalidade de proteger o consentimento livre, informado e desembaraçado. Não obstante o dever da ANPD de fiscalizar e, por conseguinte, sancionar abusos e uso indevido de tais informações.

Isso posto, evidencia-se que, a hipótese de que a expansão do reconhecimento facial pode resultar em uma diminuição da privacidade, comprometendo o direito cardinal à proteção de dados e, por conseguinte, a autodeterminação informativa, foi respondida uma vez que a autodeterminação informativa deriva da privacidade e está sendo mitigada pela comercialização, uso indiscriminado e massivo de informações pessoais como no caso da empresa Tools for Humanity que coletava as informações da íris das pessoas em troca de dinheiro ou criptomoedas, no caso do vazamento de dados do Caixa Tem do governo federal ou mesmo na coleta de dados biométricos de crianças em estádio de futebol sem consentimento prévio dos responsáveis.

Espera-se que este trabalho contribua para discussão teórica acerca da temática que é relativamente nova, que está em constante modificação e que ainda não possui um marco regulatório específico apesar do arcabouço normativo existente que é composto pela LGPD, o CC, o MCI, o CDC, a Lei do Cadastro Positivo entre outras normas que pode ser aplicadas ao caso concreto para a solução de conflitos mediante interpretação sistemática.

Ressalta-se, que, em virtude da a complexidade e atualidade do tema bem como das mudanças sociais e das transformações tecnológicas, o presente estudo não esgotou todas as fontes de pesquisa e os desdobramentos da temática. Assim, recomenda-se a quem porventura no futuro se interessar pelo assunto investigar sobre os impactos psicológicos e sociais do uso de tecnologias biométricas em populações vulneráveis como idosos, pessoas negras, crianças, comunidades periféricas à luz dos direitos humanos.

Ademais, recomenda-se a pesquisa sobre a atuação da ANPD em face das lesões no que tange ao uso do reconhecimento facial. Inclusive a comparação entre legislações internacionais sobre a matéria mostra-se relevante na construção de normas mais efetivas em observância à dignidade da pessoa humana.

Por fim, espera-se que novas pesquisas reforcem o compromisso com a abordagem ética, crítica, dialética e empática a fim de contribuir para o equilíbrio entre a necessidade de avanço tecnológico e o respeito à autodeterminação informativa das pessoas.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

7. REFERÊNCIAS BIBLIOGRÁFICAS

ARAKAKI, Fernanda F S.; VIERO, Guérula M. **Direitos humanos**. Porto Alegre: SAGAH, 2018. E-book. p.25. ISBN 9788595025370. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595025370/. Acesso em: 07 mai. 2025.

ATTANASIO, Maria Julia Santos. **Reconhecimento facial e inteligência artificial: um estudo de caso sobre o racismo estrutural e suas consequências dentro do processo penal**. 2023. Disponível em: Reconhecimento facial e inteligência artificial: um estudo de caso sobre o racismo estrutural e suas consequências dentro do processo penal. Acesso em: 7 mar. 2025

BACCARIN, Cínthia. **Limitações aos sistemas de reconhecimento facial no setor privado: boas práticas em proteção de dados biométricos faciais**. 2023. Dissertação. Disponível em: https://repositorio.unesp.br/items/c34debb0-9646-4dec-9cad-cc2442328e17. Acesso em: 18 mar 2025

BASTOS, Elisio Augusto Velloso; ESTEVES, Vitória Barros. **Tecnologias de reconhecimento facial: um estudo a partir do contexto de vigilância digital e sutil**. 2021. Disponível em: Tecnologias de reconhecimento facial | Direitos Democráticos & Estado Moderno. Acesso em 8 mar. 2025

BAUMAN, Zygmund. **Modernidade líquida** / Zygmunt Bauman; tradução, Plínio Dentzien. — Rio de Janeiro: Jorge Zahar Ed., 2001. Disponível em: Bauman Modernidade Liquida Acesso em: 7 mar. 2025

BLUM, Rita Peixoto F. **O Direito à Privacidade e a Proteção dos Dados do Consumidor**. 2. ed. São Paulo: Grupo Almedina, 2022. E-book. p.36. ISBN 9786556277066. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556277066/. Acesso em: 09 mai. 2025.

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). **Inteligência artificial e socie dade conectada**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2025. 368p. Disponível em: Livro-Inteligencia-Artificial-e-Sociedade-Conectada.pdf. Acesso em: 09 mai. 2025.

BRASIL. **Autoridade Nacional de Proteção de Dados. ANPD determina suspensão de incentivos financeiros por coleta de íris**. Gov.br, Brasília, 17 jun. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos financeiros-por-coleta-de-iris. Acesso em: 24 jun. 2025.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

BRASIL. Conselho Nacional de Justiça (CNJ). **Resolução nº 332/2020**. Disponível em: original191707202008255f4563b35f8e8.pdf. Acesso em 8 mar. 2025

BRASIL. Conselho Nacional de Justiça (CNJ). **Resolução nº 484/2022**. Disponível em: original2118372022122763ab612da6997.pdf. Acesso em 8 mar. 2025 BRASIL. Lei 14.597 de 14 de julho de 2023. Lei Geral do Esporte. 2024. Disponível em: L14597 Acesso em: 19 de abr. 2025

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, ano CLI, n. 77, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jun. 2025.

BRASIL. **Projeto de Lei nº 36/2025** de 03 de fevereiro de 2025, estabelece alterar a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados LGPD), para proibir a oferta mediante pagamento de disponibilidade de dados biométricos sensíveis e estabelecer medidas mais rigorosas de proteção a esses dados. Disponível em: prop_mostrarintegra. Acesso em: 23 mai. 2025.

BRASIL. Superior Tribunal de Justiça. **REsp n. 1.633.254/MG**, relatora Ministra Nancy Andrighi, Segunda Seção, julgado em 11/3/2020, DJe de 18/3/2020. Disponível em: STJ - Jurisprudência do STJ. Acesso em: 19 de abr. 2025

BRASIL. Superior Tribunal de Justiça. **ARE 1467470 RG / SP**. Relator(a): Min. Luís Roberto Barroso. Data de julgamento: 28/02/2025. Disponível em: 4- STF reconhecimento pessoal-em-processo-penal.pdf. Acesso em: 8 mar. 2025

BRASIL. Supremo Tribunal Federal. **ADIn 6393 MC**-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11 11-2020 PUBLIC 12-11-2020. Disponível em: Decisão histórica: STF reconhece direito autônomo à proteção de dados. Acesso em: 7 mar. 2025.

BRASIL. **Autoridade Nacional de Proteção de Dados. ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos e na entrada de estádios por 23 clubes de futebol**. Brasília, DF: ANPD, 03 maio 2024. Disponível em: https://www.gov.br/anpd/pt br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol. Acesso em: 19 abr. 2025.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

CEBRIAN, Fabiana S. P. Faraco; PRUDENTE Gustavo do Amaral; GUEDES, Marcelo Santiago; DA SILVA, Maria Carolina Ferreira; SÁ, Maria Luiza Duarte; MORAES, Thiago Guimarães. **Biometria e reconhecimento facial**. 2024. 1ª edição. Publicação digital – PDF Disponível em: www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos orientativos/radar-tecnologico-biometria-anpd.pdf. Acesso em 8 mar. 2025

COMPARATO, Fábio K. **Rumo à justiça**, 2ª edição. Rio de Janeiro: Saraiva, 2013. E-book. p.51. ISBN 9788502178588. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502178588/. Acesso em: 07 mai. 2025.

CONJUR. **STF julgará validade do reconhecimento pessoal em processo penal**. Disponível em: Acesso em: https://www.conjur.com.br/2025-mar-17/stf-julgara-validade-do reconhecimento-pessoal-em-processo-penal/ Acesso em: 07 mai. 2025

CORREIA, Jairo Santos. **A tutela dos dados pessoais do consumidor no mercado digital: uma análise do cadastro positivo à luz da LGPD**. 2023. Disponível em: A tutela dos dados pessoais do consumidor no mercado digital: uma análise do cadastro positivo à luz da LGPD. Acesso em: 07 jan. 2025

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. **Uso do Reconhecimento Facial em Sistemas de Vigilância e suas Implicações no Direito à Privacidade**. Revista de Direito, Governança e Novas Tecnologias, Belém, v.5, p.1-21. 2019. Disponível em: researchgate.net/profile/Ramon-Costa 3/publication/339398596_O_uso_de_tecnologias_de_reconhecimento_facial_em_sistemas_de _vigilancia_e_suas_implicacoes_no_direito_a_privacidade/links/5e4f35bd92851c7f7f490541/ O-uso-de-tecnologias-de-reconhecimento-facial-em-sistemas-de-vigilancia-e-suas implicacoes-no-direito-a-privacidade.pdf. Acesso em: 7 mar. 2025

CONSELHO DA EUROPA. **Convenção 108+**: Convenção para a Proteção das Pessoas com relação ao Tratamento Automatizado de Dados de Caráter Pessoal, emendada pelo Protocolo de 2018. Estrasburgo: Conselho da Europa, 2018. Disponível em: https://rm.coe.int/cm convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 7 mar. 2025.

CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael. **Lei Geral de Proteção de Dados e o poder público**. 2021. Disponível em: ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 8 mar. 2024

CRUZ, Giovana de Morais Figueiredo. **A Regulamentação da Inteligência Artificial no Âmbito da União Europeia: Implicações para os Direitos Humanos**. 2023. Dissertação. Universidade Lusófona do Porto.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

P.5. Disponível em: CRUZ, Giovana de Morais Figueiredo. A Regulamentação... - Google Acadêmico Acesso em 18 mar. 2025

DA SILVA, Guilherme Brito Araújo. **Aplicabilidade das tecnologias disruptivas de reconhecimento facial em sistemas de vigilância pública no brasil: implicações da efetividade do direito constitucional à privacidade**. 2025. Artigo Cientifico. Disponível em: Aplicabilidade das tecnologias disruptivas de reconhecimento facial em sistemas de vigilância pública no Brasil: implicações da efetividade do direito constitucional à privacidade. Acesso em 8 mar. 2025

DAGUER, Beatriz et al. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental**. 2023. Disponível em: RTDoc_15_08_2023_13_40_PM_-libre.pdf. Acesso em: 18 mar. 2025

DE CHAVES, Joel Ricardo Ribeiro; DE SÁ, Valdir Rodrigues; JANINI, Tiago Cappi. **O direito à privacidade na sociedade da informação**. 2024. Disponível em: Vista do O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO. Acesso em: 07 mai. 2025

DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO. **Ofício nº 020/2025** – DPE/SP. São Paulo, 2025. Disponível em: https://www.conjur.com.br/wp content/uploads/2025/02/OF_020_2025-Blocos-e-Carnaval-de-Rua_smart-sampa-a-uso-de teconologia-para-prisoes.pdf . Acesso em: 8 mar. 2025.

DE MACEDO, Caio Sperandeo. **O direito à revisão das decisões automatizadas de reconhecimento facial e o princípio antropocêntrico**. 2023. Disponível em: O DIREITO À REVISÃO DAS DECISÕES AUTOMATIZADAS DE RECONHECIMENTO FACIAL E O PRINCÍPIO ANTROPOCÊNTRICO | Revista de Direito Brasileira. Acesso em 8 mar. 2025

FERRAZ JR., Tércio Sampaio. **Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado**. 2021. Disponível em: https://www.terciosampaioferrazjr.com.br/publicacoes/sigilo-de-dados. Acesso em 8 abr. 2025

HARARI, Yuval Noah. **21 lições para o século 21**. 2018. Disponível em: 21 lições para o século 21 Acesso em: 18 dez. 2025

JÚNIOR, Janio Konno; JORGE, Derick Moura. **Inteligência Artificial no reconhecimento facial em Segurança Pública: dados sensíveis e seletividade penal**. Revista Eletrônica Direito & TI, v. 1, n. 15, p. 61-80, 2023. Disponível em: https://www.direitoeti.com.br/direitoeti/article/view/123/119. Acesso em: 18 dez. 2023

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. **Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos**. Revista de Direitos e Garantias Fundamentais, v. 24, n. 3, p. 43-71, 2023. Disponível em: Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos | Revista de Direitos e Garantias Fundamentais. Acesso em: 18 mar. 2025

LIMA, Dayana dos Santos. **Relação entre o reconhecimento facial e a sua responsabilidade Jurídica: A luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana?**. 2023. Disponível em: Relação entre o reconhecimento facial e a sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana?. Acesso em: 7 mar. 2025

MARINI, Bruno; COLVARA, Yasmin Zanuncio. **Da vigilância digital no contexto do direito à privacidade** .2024. Disponível em: Vista do DA VIGILÂNCIA DIGITAL NO CONTEXTO DOS DIREITOS HUMANOS E DO DIREITO À PRIVACIDADE. Acesso em 10 nov. 2024

MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**. Pensar Revista de Ciências Júridicas Universidade de Fortaleza (Unifor), Fortaleza, v. 25, n. 4, p. 1-18, 2020. Disponível em: MENDES, Laura Schertel Ferreira. Autodeterminação... - Google Acadêmico. Acesso em 8 mar 2025

MENDONÇA, Alice Godinho. **Reconhecimento facial em condomínios: desafios sob a ótica da LGPD**. 2024. Disponível em: https://www.conjur.com.br/2024-abr 07/reconhecimento-facial-em-condominios-desafios-sob-a-otica-da-lgpd/ Acesso em 8 mar. 2024

MENEZES, George Washington. **A ação do uso da inteligência artificial e microfeições faciais para mitigar os riscos de deepfakes para a autenticação por biometria facial no setor financeiro brasileiro**. 2024. Disponível em: GEORGE WASHINGTON MENEZES.pdf Acesso em: 07 mai. 2025

MIRANDA, Marina Ferraz de; SOUZA, Tayná Tomaz de. **Sobre inteligência artificial reconhecimento reconhecimento facial facial e LGPD**. Sobre inteligência artificial e LGPD [S. l.], 1 dez. 2021. Disponível em: https://www.conjur.com.br/2021-mai-05/miranda-souza-ia-reconhecimento-facial- lgpd/. Acesso em: 18 dez. 2023

MONÇÃO, Amanda Marques. **Da proteção aos dados pessoais sensíveis sob a luz dos direitos humanos e da Lei Geral de Proteção de Dados**. 2023. Artigo. Disponível em: https://repositorio.ufms.br/handle/123456789/5962. Acesso em: 18 dez. 2023

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

MONDAINI, Marco. Direitos Humanos. São Paulo: Edições 70, 2020. E-book. p.30. ISBN 9788562938368. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788562938368/. Acesso em: 07 mai. 2025

NEBESHIMA, Yuri. **Uso do reconhecimento facial na segurança pública**. 2024. Disponível em: https://www.conjur.com.br/2024-jan-06/uso-do-reconhecimento-facial-na seguranca-publica/ Acesso em 8 mar. 2024

NUNES, César Augusto R. **Anais de Artigos Completos do VII CIDHCoimbra** 2022 - Volume 4 / César Augusto R. Nunes et. al. (org.) [et al.] – Campinas / Jundiaí: Brasílica / Edições Brasil, 2023. 450 p. Série Simpósios do VII CIDHCoimbra 2022. Disponível em: Anais_de_Artigos_Completos_2022.pdf. Anais_de_Artigos_Completos_2022.pdf. Acesso em 8 abr. 2025

PEREIRA, Sara Matias Ferrari; OLIVEIRA, Tarsis Barreto. **O uso da inteligência artificial no direito penal e seus reflexos sobre os direitos fundamentais da não discriminação e da privacidade**.2024. Artigo cientifico. Disponível em: O uso da inteligência artificial no direito penal e seus reflexos sobre os direitos fundamentais da não discriminação e da privacidade | Revista do Instituto de Direito Constitucional e Cidadania. Acesso em 8 mar. 2025 ISBN

PINHEIRO, Patrícia P. **Direito Digital**. [Digite o Local da Editora]: Editora Saraiva, 2021. E book. 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 13 dez. 2024. p. 95

PINTO, Rodrigo Alexandre L.; NOGUEIRA, Jozelia**. Inteligência Artificial e Desafios Jurídicos: Limites Éticos e Legais**. São Paulo: Almedina, 2023. E-book. p.290. ISBN 9786556279268. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279268/. Acesso em: 09 mai. 2025

RABENHORT, Eduardo R.. **O que são direitos humanos?.** 1996. Disponível em: https://www.cchla.ufpb.br/redhbrasil/wp-content/uploads/2014/04/O-QUE-SÃO-DIREITOS HUMANOS.pdf. Acesso em: 7 mar. 2025

RAMOS, André de C. Teoria Geral dos Direitos Humanos. 8. ed. Rio de Janeiro: Saraiva Jur, 2024. E-book. p.I. ISBN 9786553628762. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553628762/. Acesso em: 07 mai. 2025

RUIZ, Jefferson Lee de S. **Direitos humanos e concepções contemporâneas**. São Paulo: Cortez Editora, 2015. E-book. p.Capa. ISBN 9788524923685. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788524923685/. Acesso em: 07 mai. 2025

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

SANTOS, Rafa. **Defensoria Pública questiona uso de reconhecimento facial no Carnaval de SP**. 2025. Disponível em: https://www.conjur.com.br/2025-fev-25/defensoria-publica questiona-uso-de-monitoramento-facial-no-carnaval-de-sp/. Acesso em: 8 mar. 2024

SÃO PAULO. 1ª Vara Cível Federal de São Paulo. **Processo nº 5028572-20.2022.4.03.6100**. Autor: Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação Sigilo. Réus: DATAPREV S.A, União Federal, Caixa e Autoridade Nacional de Proteção de Dados. Juiz: Marco Aurelio de Mello Castrianni, 06 de setembro de 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de imprensa/noticias-sp/justica-determina indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais vazados-em-2022. Acesso em 10 nov. 2024

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**.2020. Disponível em: *RBDFJ_42-MIOLO.indd Acesso em: 8 mar. 2025

SHARFI, Gabriela. **Do direito fundamental à proteção de dados pessoais: análise sobre os benefícios e malefícios da prática do reconhecimento facial e vigilância em massa**. 2023. Monografia. PUC –SP. P. 35. Disponível em: SHARFI, Gabriela. Do direito fundamental à proteção... - Google Acadêmico. Acesso em: 18 mar. 2025

SOUZA, Marco Antônio de. A Biometria e suas Aplicações. **Revista Brasileira de Ciências Policiais**, Brasília, DF, v. 11, n. 2, p. 79-102, maio/ago. 2020. Disponível em: giojr,+03+ +Artigo+03.pdf. Acesso em: 16 abr. 2025

SOUZA; Raquel; GONÇALVES, Marilia. CESeC. Centro de Estudos de Segurança e Cidadania. **Esporte, dados e direitos [livro eletrônico]: o uso de reconhecimento facial nos estádios brasileiros** / Raquel Sousa...[et al.] ; edição Marília Gonçalves. – Rio de Janeiro : CESeC, 2024. Disponível em: *OPANOPTICO_Pesquisa_Esporte_Dados_e_Direitos_O_Uso_de_Reconhecimento_Facial_ nos_Estadios_Brasileiros.pdf. Acesso em 8 mar. 2025

TAJRA, Alex. **Reconhecimento facial de crianças em estádios fere LGPD e ECA**. 2024. Disponível em: Reconhecimento facial de crianças em estádios fere LGPD e ECA, diz relatório. Acesso em: 7 mar. 2025

VIEIRA, Gabriel Braun. **A autodeterminação informativa na sociedade em rede e as perspectivas de responsabilidade civil à luz da LGPD: uma análise jurisprudencial do tribunal de justiça de São Paulo**. 2023. Monografia. Disponível em: A autodeterminação informativa na sociedade em rede e as perspectivas de responsabilidade civil à luz da LGPD: uma análise jurisprudencial do Tribunal de Justiça de São Paulo | Manancial - Repositório Digital da UFSM. Acesso em: 8 mar. 2025

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

YAROVENKO, Vasily; SHAPOVALOVA, Galina; ISMAGILOV, Rinat. **Some problems of using the facial recognition system in law enforcement activities. Правовое государство теория и практика**, [s. l.], v. 17, n. 1, p. 189-200, mar. 2021. Disponível em: (PDF) ALGUNS PROBLEMAS DO USO DO SISTEMA DE RECONHECIMENTO FACIAL EM ATIVIDADES DE APLICAÇÃO DA LEI. Acesso em: 7 mar. 2025

Artigo recebido: 01.07.2025

Artigo publicado em: 30.12.2025