Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i5.27168

A ÍRIS COMO IDENTIFICADOR BIOMÉTRICO E À PROTEÇÃO DE DADOS PESSOAIS NA ERA DIGITAL

THE IRIS AS A BIOMETRIC IDENTIFIER AND THE PROTECTION OF PERSONAL DATA

Rondinely Fonseca da Silveira[1]
Igor Câmara de Araújo[2]

RESUMO: Este artigo analisa a proteção de dados pessoais no contexto do uso da biometria da íris como mecanismo de identificação na era digital. O estudo aborda a relevância tecnológica desse método biométrico, suas principais vantagens técnicas e os desafios jurídicos relacionados à privacidade, à segurança da informação e ao tratamento de dados sensíveis. A biometria da íris destaca-se pela precisão, confiabilidade e crescente utilização em sistemas de autenticação e controle de acesso. Contudo, sua aplicação exige observância aos parâmetros legais de proteção de dados, especialmente aos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD) e no Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD). Nesse contexto, o artigo busca compreender os limites jurídicos do uso da biometria da íris, refletindo sobre o equilíbrio entre inovação tecnológica e proteção de direitos fundamentais, bem como sobre a atuação da Autoridade Nacional de Proteção de Dados (ANPD) na fiscalização e regulamentação da matéria.

Palavras-chave: Biometria 1. Íris 2. Proteção de dados 3. LGPD 4. RGPD 5. Legislação 6.

ABSTRACT: This article analyzes the protection of personal data in the context of the use of iris biometrics as an identification mechanism in the digital age. The study addresses the technological relevance of this biometric method, its main technical advantages, and the legal challenges related to privacy, information security, and the processing of sensitive data. Iris biometrics stands out for its accuracy, reliability, and growing use in authentication and access control systems. However, its application requires compliance with legal data protection standards, especially those established by the Brazilian General Data Protection Law (LGPD) and the European Union General Data Protection Regulation (GDPR). In this context, the article seeks to understand the legal limits of the use of iris biometrics, reflecting on the balance between technological innovation and the protection of fundamental rights, as well as on the role of the Brazilian National Data Protection Authority (ANPD) in overseeing and regulating this matter.

Keywords: Biometrics. Íris. Data protection. LGPD. GDPR. Legislation.

[1] Acadêmico, 10° Período de Direito - Faculdade Boas Novas.
[2] Orientador, Mestre, Doutor, Especialista em Direito. Professor do Curso de TCC II.

1 - INTRODUÇÃO

A intensificação da vida digital modificou profundamente as formas de identificação, autenticação e circulação de dados na sociedade contemporânea. Em um cenário marcado pela ampliação de serviços eletrônicos, pela automação de processos e pela crescente dependência de sistemas informacionais, as tecnologias biométricas passaram a ocupar papel central nos mecanismos de verificação de identidade. Segundo Malgheet, Manshor e Affendey (2021), os sistemas biométricos surgem como alternativa aos meios tradicionais de identificação, como senhas e chaves, especialmente em contextos que exigem maior confiabilidade e segurança. Nessa mesma direção, Almeida e Soares (2022) destacam que a era digital transformou os dados pessoais em ativos de elevado valor, o que tornou sua proteção uma preocupação normativa e institucional cada vez mais relevante.

Entre as diferentes modalidades biométricas, o reconhecimento da íris passou a receber atenção especial em razão de suas características fisiológicas. De acordo com Malgheet, Manshor e Affendey (2021), a íris é compreendida na literatura especializada como uma estrutura estável ao longo do tempo, dotada de singularidade e apta a oferecer elevada confiabilidade para fins de identificação e autenticação. Por isso, sua utilização tem sido associada a ambientes que exigem maior rigor na verificação identitária, como fronteiras, aeroportos, dispositivos móveis, instituições públicas e sistemas de segurança. A expansão desse tipo de tecnologia, entretanto, não deve ser observada apenas sob o prisma da inovação técnica, mas também à luz das implicações jurídicas decorrentes do tratamento de dados biométricos.

Nesse contexto, o debate sobre biometria se conecta diretamente à proteção de dados pessoais e à tutela da privacidade. Santana e Ansari (2023) observam que, em uma sociedade cada vez mais interconectada, a proteção de dados e a privacidade assumem posição de destaque como direitos fundamentais vinculados à autonomia, à dignidade e ao espaço pessoal do indivíduo. Na mesma linha, Almeida e Soares (2022) assinalam que o avanço das tecnologias digitais exigiu a formulação de instrumentos normativos voltados à regulamentação do tratamento, da acessibilidade e do uso de dados pessoais, especialmente diante de sua crescente circulação por instituições públicas e privadas. Assim, a discussão sobre biometria da íris insere-se em um ambiente jurídico mais amplo, no qual a proteção de dados deixa de ser mera cautela administrativa e passa a integrar o núcleo das garantias fundamentais na sociedade da informação.

A relevância do tema torna-se ainda mais evidente quando se considera que os dados biométricos estão diretamente vinculados ao corpo do titular e, por isso, demandam proteção reforçada. Nurhuda e Safitri (2026) ressaltam que a utilização de biometria em serviços públicos e sistemas eletrônicos se relaciona à busca por maior precisão identificatória, eficiência e segurança, mas também envolve riscos importantes à privacidade, sobretudo em situações de armazenamento massivo, acesso não autorizado e vulnerabilidade das bases de dados. Desse modo, a biometria da íris deve ser compreendida como fenômeno que reúne, ao mesmo tempo, inovação tecnológica, sensibilidade informacional e necessidade de regulação jurídica, o que justifica sua análise no âmbito da proteção de dados pessoais na era digital.

2 - A BIOMETRIA

A biometria consiste no uso de características físicas, fisiológicas ou comportamentais para fins de identificação e autenticação de indivíduos em sistemas automatizados. Seu desenvolvimento está relacionado à necessidade de superar limitações dos mecanismos tradicionais de verificação, como senhas, cartões e chaves, que podem ser esquecidos, perdidos, furtados ou compartilhados indevidamente. Conforme assinalam Malgheet, Manshor e Affendey (2021), os sistemas biométricos se consolidaram justamente como alternativa mais segura e eficiente aos métodos tradicionais de identificação, podendo operar a partir de modelos fisiológicos, como impressão digital, face, retina, geometria da mão e íris, ou comportamentais, como voz, assinatura e dinâmica de digitação.

Na sociedade digital, a biometria passou a ocupar espaço crescente em setores públicos e privados, especialmente em contextos que exigem maior precisão na autenticação da identidade. O uso dessas tecnologias tem se expandido em serviços bancários, controle de acesso, dispositivos móveis, sistemas administrativos e serviços públicos, em razão da busca por mais segurança, agilidade e confiabilidade. Nurhuda e Safitri (2026) observam que a biometria funciona como instrumento de identificação e autenticação baseado em características físicas e biológicas do indivíduo, sendo utilizada para aumentar a precisão da identificação, a eficiência dos serviços e a segurança dos sistemas. Na mesma direção, Almeida e Soares (2022) destacam que, na era digital, os dados pessoais passaram a assumir elevado valor econômico e institucional, o que reforçou a necessidade de regulamentar sua coleta, tratamento e proteção.

Embora a biometria seja frequentemente associada à ideia de maior segurança, seu emprego também levanta preocupações importantes no campo da proteção de dados pessoais.

Isso ocorre porque os dados biométricos são diretamente vinculados ao corpo do titular e, diferentemente de senhas ou códigos, não podem ser simplesmente substituídos em caso de comprometimento. Haasnoot, Spreeuwers e Veldhuis (2022) chamam atenção para esse aspecto ao destacar que aplicações biométricas dependem de um conjunto limitado e não revogável de características humanas, de modo que o vazamento dessas informações pode comprometer múltiplos sistemas de autenticação ao mesmo tempo. Por essa razão, a biometria deve ser compreendida não apenas como ferramenta tecnológica de identificação, mas também como categoria sensível de tratamento de dados, sujeita a riscos de vazamento, uso indevido, ataques de apresentação e fragilização da privacidade.

Entre as modalidades biométricas, a biometria da íris destaca-se pela singularidade de seus padrões, pela estabilidade ao longo do tempo e pela ampla utilização em contextos de alta segurança. Liu et al. (2021) observam que os padrões da íris são formados aleatoriamente durante o desenvolvimento fetal e permanecem invariáveis com a idade, o que faz dessa estrutura uma característica biométrica universalmente única, inclusive entre gêmeos. Já Malgheet, Manshor e Affendey (2021) ressaltam que o reconhecimento da íris alcançou grande relevância entre as técnicas biométricas por sua alta eficiência, confiabilidade e potencial de aplicação em sistemas automatizados. Desse modo, a compreensão geral da biometria constitui etapa necessária para, em seguida, examinar de forma mais específica a biometria da íris e seus reflexos no campo da proteção de dados pessoais.

2.1 - Tipos de biometria

Os sistemas biométricos podem ser classificados, de modo geral, em modalidades fisiológicas e comportamentais. As modalidades fisiológicas utilizam características corporais relativamente estáveis, como impressão digital, face, íris e geometria da mão, enquanto as comportamentais se baseiam em padrões de ação do indivíduo, como voz e dinâmica de digitação. Essa distinção é importante porque cada tipo de biometria apresenta diferentes níveis de precisão, custo, aplicabilidade e impacto sobre a privacidade. Conforme observam Malgheet, Manshor e Affendey (2021), os sistemas biométricos se desenvolveram justamente para oferecer métodos de autenticação mais seguros do que os modelos tradicionais baseados em senhas ou chaves, especialmente em ambientes que exigem maior confiabilidade.

A impressão digital constitui uma das modalidades biométricas mais difundidas, sendo amplamente utilizada em smartphones, sistemas de controle de acesso, registros

administrativos e ambientes corporativos. Seu uso decorre da relativa simplicidade técnica, do menor custo de implementação e da singularidade das minúcias presentes nas cristas papilares de cada indivíduo. Por essas características, a impressão digital continua sendo uma das formas mais conhecidas de autenticação biométrica, como pode ser observado na Figura 1.

Figura 01. Impressão digital

Fonte: pngegg.com

O reconhecimento facial baseia-se na análise das proporções, distâncias e características geométricas da face humana, sendo empregado em aeroportos, instituições financeiras, smartphones, vigilância pública e sistemas de identificação automatizada. Trata-se de uma modalidade que ganhou grande expansão em razão da facilidade de captura por câmeras e da integração com plataformas digitais de monitoramento e segurança. A aplicação desse mecanismo em diferentes contextos sociais e institucionais pode ser ilustrada na Figura 2.

Figura 02. Reconhecimento Facial

Fonte: Bio World Sistemas

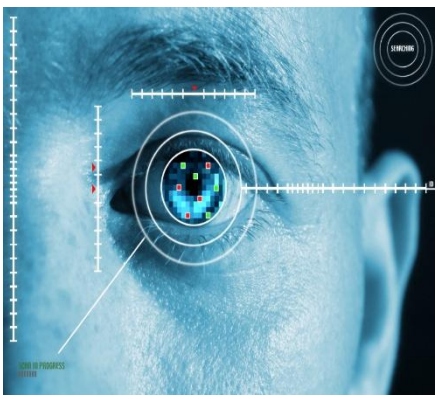
O reconhecimento de voz corresponde a uma biometria comportamental, pois se fundamenta em elementos como padrão vocal, frequência, timbre, entonação e ritmo da fala. Esse recurso é frequentemente utilizado em call centers, assistentes virtuais, autenticação remota e serviços bancários, sobretudo em situações nas quais o usuário precisa ser validado sem presença física. Como demonstra a Figura 3, a voz também passou a integrar o conjunto de tecnologias biométricas utilizadas em processos de autenticação contemporâneos.

Figura 03. Reconhecimento de Voz.

Fonte: Inforchannel

A biometria da íris destaca-se pela utilização dos padrões texturais presentes na íris, estrutura ocular distinta da retina e reconhecida por sua alta singularidade e estabilidade ao longo do tempo. Em razão dessas características, essa modalidade é frequentemente associada a contextos de alta segurança, como instituições financeiras, controle de acesso e sistemas avançados de identificação. Malgheet, Manshor e Affendey (2021) destacam que o reconhecimento da íris ocupa posição de destaque entre as técnicas biométricas em razão de sua confiabilidade e precisão. A representação dessa modalidade pode ser visualizada na Figura 4.

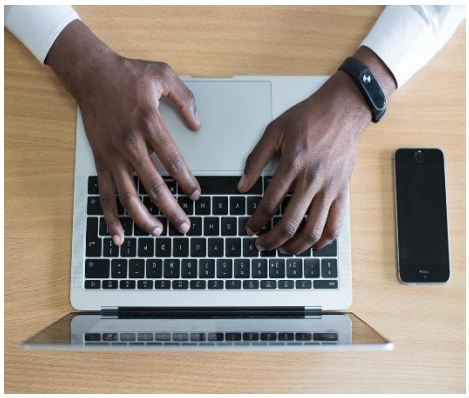
Figura 04. Reconhecimento da íris.



Fonte: Abióptica

A dinâmica de digitação constitui outra modalidade comportamental, baseada na forma como o indivíduo interage com teclados ou superfícies digitais. Nesse caso, o sistema analisa elementos como velocidade, intervalo entre toques, pressão e ritmo de digitação, criando um padrão de comportamento do usuário. Essa técnica é especialmente relevante em modelos de autenticação contínua, nos quais o sistema acompanha o comportamento do indivíduo ao longo da sessão. A aplicação dessa lógica biométrica pode ser observada na Figura 5.

Figura 05. Dinâmica de Digitação



Fonte: Assine Abril

A geometria da mão e dos dedos utiliza medidas estruturais, como comprimento, largura, espessura e curvatura da mão e dos dedos, com a finalidade de autenticação. Embora não seja atualmente a modalidade mais difundida, esse tipo de biometria já foi empregado em instituições bancárias, escolas, empresas e ambientes de controle físico de acesso. Seu diferencial está na leitura de proporções anatômicas gerais, e não em detalhes minuciosos como ocorre com a impressão digital. Essa modalidade pode ser identificada visualmente na Figura 6.

Figura 06. Geometria da mão e dedos

Fonte: AF.mil

Método de reconhecimento por meio da geometria da mão e dos dedos, cuja captura ocorre a partir da identificação do padrão da mão. Esse tipo de equipamento está presente em instituições bancárias, escolas, empresas e outros ambientes de controle de acesso. Sua especificidade está na leitura de características como comprimento, espessura, largura, curvatura e proporções da mão e dos dedos. Esse mecanismo, além de possuir menor custo em comparação com outras modalidades, contribui para a autenticação dos usuários, embora nem sempre tenha, de forma objetiva, a finalidade de identificá-los individualmente.

Esses sistemas biométricos apresentam aspectos positivos e limitações, mas, diante do avanço tecnológico, observa-se que a biometria vem ampliando continuamente suas possibilidades de aplicação. Nesse contexto, surgem novas formas de utilização dessas tecnologias, inclusive em setores que exigem elevado grau de segurança e precisão.

Essa realidade pode ser observada em diferentes áreas. Em algumas unidades hospitalares e em outros setores especializados, determinadas tecnologias biométricas já vêm sendo incorporadas aos seus procedimentos. Entre elas, destaca-se o DNA, considerado um dos mecanismos mais complexos de identificação, por permitir a análise de material genético para fins de comparação entre perfis biológicos. Também se destacam os sistemas biométricos presentes em passaportes e em mecanismos de inspeção utilizados em aeroportos e fronteiras, voltados à verificação de identidade e ao controle de circulação internacional.

No caso do DNA, sua aplicabilidade ocorre mediante procedimentos específicos, que envolvem a coleta do material genético, a realização de análise laboratorial para elaboração do perfil correspondente e, posteriormente, a comparação entre os perfis obtidos. Trata-se, portanto, de um método de identificação altamente especializado, utilizado em contextos que exigem elevado rigor técnico e científico.

De modo geral, esses mecanismos oferecem vantagens como segurança, praticidade, agilidade e maior precisão em diferentes ambientes de uso. À medida que a tecnologia avança, a biometria amplia sua presença e reforça sua importância nos processos de autenticação e identificação, especialmente em contextos que demandam maior confiabilidade na validação da identidade humana.

A presença da biometria não se limita às modalidades já consolidadas, mas continua em expansão, impulsionada também pelo desenvolvimento da inteligência artificial. Estudos recentes apontam para novas formas de aplicação que vêm se fortalecendo gradativamente, entre as quais se destacam:

- Biometria multimodal: técnica que combina diferentes modalidades biométricas, como impressão digital, reconhecimento facial, íris, voz e padrões comportamentais, com a finalidade de ampliar a precisão da autenticação e reduzir a possibilidade de fraudes.
- Autenticação contínua: mecanismo que permite a verificação constante do usuário durante a interação com o sistema, dispensando repetições frequentes de autenticação.
- Veículos com uso de biometria: aplicação que permite interação entre condutor e veículo por meio de abertura de portas, acionamento, ignição, reconhecimento de voz e outras funcionalidades automatizadas.
- Área da saúde: utilização da biometria para identificação de pacientes, autenticação de acesso e proteção de registros médicos.

Para que toda essa verificação seja possível, é necessário que os sistemas biométricos contem com estrutura tecnológica adequada, incluindo sensores capazes de detectar características específicas, equipamentos para leitura e armazenamento das informações, além de softwares responsáveis por processar, analisar e comparar os dados coletados. É por meio desse processamento que se torna possível gerar códigos ou padrões únicos para autenticação e identificação.

Assim, observa-se que os sistemas biométricos operam a partir da leitura de características humanas singulares, o que os torna instrumentos relevantes para a identificação de pessoas e para a redução de fraudes. Por essa razão, a biometria tem se consolidado como uma das ferramentas mais importantes da atualidade no campo da segurança e da validação de identidade.

2.2 - A íris

Para a compreensão da íris, é necessário recorrer à sua definição anatômica e funcional. A íris corresponde à parte colorida do olho humano, localizada entre a córnea e o cristalino, formando um anel ao redor da pupila. Sua função está relacionada ao controle da entrada de luz no olho, por meio da contração e da dilatação pupilar, desempenhando, assim, papel importante no processo da visão. Conforme destacam Bhatt, Sehrawat e Gupta (2025), a íris é a estrutura visível que circunda a pupila e apresenta características biológicas próprias, sendo composta por tecido vascularizado e pigmentado, cuja coloração varia conforme a quantidade de melanina presente.

Um aspecto que merece destaque é que a cor dos olhos — azul, verde, castanho, entre outras — está relacionada à distribuição e à quantidade de melanina na íris, sem que isso elimine a singularidade dos seus padrões internos. É justamente essa combinação de formas, texturas e marcas estruturais que torna a íris uma característica biométrica de grande relevância. Liu et al. (2021) observam que os padrões da íris são formados de maneira aleatória durante o desenvolvimento fetal e permanecem estáveis com o avanço da idade, razão pela qual são considerados universalmente únicos, inclusive entre gêmeos. No mesmo sentido, Malgheet, Manshor e Affendey (2021) ressaltam que a estabilidade e a singularidade da íris justificam seu amplo uso em sistemas de reconhecimento e autenticação.

No campo tecnológico, a leitura da íris permite a extração de informações que, após processamento computacional, são convertidas em um padrão matemático utilizado para autenticação. Esse processo não significa a reprodução integral da imagem ocular, mas a transformação de características específicas em códigos aptos à comparação automatizada em sistemas biométricos. Ben Chaabane, Harrabi e Seddik (2024) explicam que o reconhecimento da íris depende de etapas como segmentação, localização da região ocular, extração de características e classificação, o que demonstra o grau de sofisticação técnica envolvido nesse tipo de sistema. Em razão dessa capacidade de gerar um padrão biométrico singular, a íris passou a ser utilizada em contextos que exigem elevado grau de precisão e segurança, como controle de acesso, instituições financeiras e sistemas de identificação digital.

Além disso, a biometria da íris destaca-se por sua natureza não invasiva e por sua associação com mecanismos de autenticação considerados altamente confiáveis. Por essa razão, empresas e instituições que atuam no setor de segurança digital passaram a investir nessa tecnologia como forma de reforçar mecanismos de validação de identidade. Contudo, embora a íris apresente características que favoreçam sua utilização biométrica, seu emprego não se limita aos aspectos técnicos, uma vez que envolve também o tratamento de dados sensíveis e a necessidade de observância aos parâmetros jurídicos de proteção de dados pessoais. Nesse sentido, a análise da biometria da íris exige que se observem não apenas suas potencialidades, mas também as vantagens e desvantagens relacionadas ao seu uso, tema que será examinado nos tópicos seguintes.

2.3 - Biometria da íris e sua vantagem

A biometria da íris destaca-se entre os métodos de autenticação por apresentar elevado

grau de confiabilidade, sobretudo em contextos que exigem maior precisão na identificação de indivíduos. No cenário digital contemporâneo, sua utilização tem sido associada à busca por mais segurança, praticidade e eficiência nos processos de autenticação. Isso se deve ao fato de que a íris possui padrões altamente complexos e singulares, formados de maneira aleatória durante o desenvolvimento ocular, o que contribui para sua individualização biométrica, inclusive entre gêmeos. Liu et al. (2021) observam que os padrões da íris são universalmente únicos e relativamente estáveis ao longo da vida, enquanto Malgheet, Manshor e Affendey (2021) ressaltam que essa modalidade biométrica se destaca pela alta eficiência e confiabilidade no reconhecimento pessoal.

Outra vantagem relevante da biometria da íris está relacionada à estabilidade de seus padrões internos e ao fato de se tratar de uma característica menos exposta a desgastes físicos quando comparada a outras modalidades biométricas. Ben Chaabane, Harrabi e Seddik (2024) destacam que a íris é considerada um dos métodos biométricos mais seguros e precisos, justamente por se tratar de uma estrutura interna, protegida por elementos oculares externos e, por isso, menos suscetível a danos. Além disso, Rubio e Magnier (2024) observam que o reconhecimento da íris tem ampla aplicação em sistemas de segurança e identificação em razão de sua natureza não invasiva, de sua alta confiabilidade e de sua resistência relativamente maior a tentativas de fraude.

Também merece destaque a capacidade dos sistemas de reconhecimento da íris de operar de forma automatizada e com elevado grau de precisão em ambientes controlados. A leitura da íris, seguida da extração e comparação de características matematicamente codificadas, permite a autenticação do usuário com rapidez e consistência, favorecendo sua utilização em instituições financeiras, controle de acesso, aeroportos e outros ambientes que demandam identificação segura. Nesse sentido, os estudos de Ben Chaabane, Harrabi e Seddik (2024) demonstram que o desempenho do reconhecimento da íris depende de etapas técnicas bem definidas, como localização, segmentação, extração de características e classificação, o que reforça a robustez desse tipo de sistema quando implementado em condições adequadas. Assim, a biometria da íris apresenta vantagens relevantes quanto à precisão, à singularidade, à estabilidade e à segurança, fatores que explicam sua crescente utilização em sistemas digitais de autenticação.

2.4 - Biometria da íris e sua desvantagem

Apesar de suas vantagens, a biometria da íris também apresenta limitações e desafios

que precisam ser considerados. Um dos principais pontos diz respeito à necessidade de infraestrutura tecnológica adequada, com equipamentos específicos para captura da imagem ocular, softwares avançados de processamento e condições controladas de operação. Bhatt, Sehrawat e Gupta (2025) destacam que o reconhecimento confiável da íris depende de instrumentos apropriados, incluindo sistemas de imageamento em infravermelho próximo, além de requisitos mínimos de resolução para obtenção de imagens aptas à autenticação. Isso significa que a implementação dessa tecnologia pode demandar custos mais elevados e maior especialização técnica, o que limita sua adoção em determinados setores.

Outro aspecto importante refere-se às dificuldades de captura e processamento da imagem da íris em ambientes não ideais. Malgheet, Manshor e Affendey (2021) observam que, em contextos menos controlados, o reconhecimento da íris pode ser afetado por fatores como baixa resolução, posicionamento inadequado, rotação, distorções, interferência de cílios, reflexos, armações de óculos, borramentos e outras formas de ruído. No mesmo sentido, Rubio e Magnier (2024) apontam que a variação na qualidade da imagem, nas condições de iluminação e na posição do olho representa obstáculo importante ao desempenho dos sistemas de reconhecimento, exigindo técnicas sofisticadas de pré-processamento para lidar com oclusões, pigmentação variada e diversidade de texturas.

Há, ainda, limitações relacionadas a condições oculares específicas. Bhatt, Sehrawat e Gupta (2025) ressaltam que doenças oculares, cirurgias e alterações na estrutura do olho podem interferir na leitura da íris e comprometer a taxa de reconhecimento, sobretudo quando há mudanças relevantes na coloração, na forma pupilar ou na qualidade da imagem capturada. Além disso, o reconhecimento da íris pode exigir maior cooperação do usuário, especialmente nos sistemas convencionais, nos quais é necessário posicionar adequadamente o olhar diante do sensor para que a leitura seja realizada com precisão. Esses fatores demonstram que, embora se trate de tecnologia avançada, sua aplicação ainda depende de condições materiais e fisiológicas que nem sempre estão presentes em todos os contextos de uso.

Para além dos desafios técnicos, a biometria da íris também desperta preocupações no campo jurídico, principalmente em razão da coleta, do armazenamento e do tratamento de dados biométricos sensíveis. Como tais dados estão diretamente ligados ao corpo do titular, eventual comprometimento de bancos de dados ou uso indevido das informações pode gerar riscos significativos à privacidade e à segurança informacional. Nesse contexto, a expansão da biometria da íris exige não apenas aperfeiçoamento tecnológico, mas também mecanismos

normativos e institucionais capazes de assegurar a proteção dos direitos fundamentais, especialmente no que se refere à dignidade da pessoa humana, à privacidade e à proteção de dados pessoais. Por essa razão, a análise da biometria da íris não se encerra em suas características técnicas, mas precisa ser articulada ao debate jurídico mais amplo sobre regulação, limites de uso e tutela da pessoa natural, aspecto que será desenvolvido nos tópicos seguintes

3 - PESSOA NATURAL

Segundo o ordenamento jurídico brasileiro, a pessoa natural é o sujeito de direitos e deveres na ordem civil. O Código Civil de 2002 estabelece, em seu artigo 1º, que "toda pessoa é capaz de direitos e deveres na ordem civil", reconhecendo ao ser humano posição central nas relações jurídicas. A partir dessa compreensão, a pessoa natural passa a ser concebida como titular de direitos fundamentais e de prerrogativas inerentes à sua dignidade, cabendo à Constituição Federal e à legislação infraconstitucional assegurar sua proteção jurídica, especialmente no que se refere aos direitos da personalidade.

A personalidade civil tem início com o nascimento com vida, nos termos do artigo 2º do Código Civil, embora a lei resguarde, desde a concepção, os direitos do nascituro. Isso significa que, mesmo antes do nascimento, o ordenamento jurídico já reconhece determinados efeitos de proteção jurídica, como ocorre, por exemplo, em situações relacionadas à herança e aos alimentos. Dessa forma, a pessoa natural ocupa posição de relevância jurídica desde a concepção, consolidando-se, com o nascimento com vida, como sujeito pleno de relações jurídicas na esfera civil.

A capacidade de direito é inerente a toda pessoa natural, enquanto a capacidade de fato corresponde à aptidão para exercer pessoalmente os atos da vida civil. Nessa perspectiva, o Código Civil também disciplina os direitos da personalidade, especialmente entre os artigos 11 e 21, assegurando a tutela de atributos essenciais da pessoa humana, como nome, imagem, honra, integridade física, integridade psíquica e privacidade. Tais direitos possuem caráter personalíssimo e, em regra, são irrenunciáveis, intransmissíveis e imprescritíveis, o que reforça a proteção da dignidade da pessoa humana como valor central do sistema jurídico.

A extinção da personalidade civil ocorre com a morte, conforme dispõe o artigo 6º do Código Civil. Ainda assim, mesmo após o falecimento, o ordenamento preserva determinados aspectos ligados à memória, à imagem e ao respeito devido à pessoa falecida. Isso demonstra

que a proteção jurídica da pessoa natural não se restringe apenas à sua existência biológica, mas alcança também dimensões morais e existenciais que permanecem relevantes no campo do Direito.

Essa compreensão torna-se especialmente importante no contexto da proteção de dados pessoais. Quando uma informação se refere a uma pessoa natural identificada ou identificável, passa-se ao campo dos dados pessoais, conforme definição prevista no artigo 5º, inciso I, da Lei Geral de Proteção de Dados Pessoais. Por essa razão, a discussão sobre biometria da íris e proteção de dados pessoais exige, antes de tudo, a compreensão da pessoa natural como sujeito central da tutela jurídica. É justamente dessa condição que decorre a necessidade de proteção de suas informações, sobretudo quando se trata de dados sensíveis, capazes de afetar a privacidade, a dignidade e o exercício da cidadania.

4 - DADOS PESSOAIS

Nos termos da Lei Geral de Proteção de Dados Pessoais, dados pessoais são as informações relacionadas à pessoa natural identificada ou identificável. Essa definição abrange dados básicos, como nome, número de CPF, endereço e demais elementos que permitam identificar direta ou indiretamente o titular. Já os dados sensíveis constituem categoria específica dentro do regime jurídico da proteção de dados, incluindo informações sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos e biométricos. Por essa razão, ao tratar da biometria da íris, este artigo insere-se diretamente no campo da proteção de dados pessoais, com especial atenção à tutela reforçada conferida aos dados sensíveis.

O presente estudo relaciona-se à natureza dos dados pessoais, à sua relevância na sociedade da informação e aos desafios ligados à sua proteção e ao seu uso responsável na era digital. Nesse contexto, analisam-se a Lei Geral de Proteção de Dados Pessoais, no Brasil, e o Regulamento Geral de Proteção de Dados da União Europeia, além da atuação da Autoridade Nacional de Proteção de Dados, responsável por orientar e fiscalizar a aplicação da LGPD. A importância do tema se torna ainda maior quando se observa que o tratamento de dados biométricos, como a captura da íris, envolve não apenas inovação tecnológica, mas também questões diretamente ligadas à privacidade, à segurança da informação, à cidadania e à dignidade da pessoa humana.

O uso indiscriminado de informações pessoais expõe o titular a riscos de privacidade,

discriminação, vigilância indevida e comprometimento da segurança informacional. Por isso, a promulgação da Lei nº 13.709/2018 representou, no Brasil, a criação de um marco regulatório destinado a estabelecer princípios, fundamentos e diretrizes para o tratamento de dados pessoais, inclusive em meios digitais. A LGPD surgiu justamente para disciplinar a coleta, o armazenamento, o compartilhamento e as demais formas de tratamento de informações pessoais, buscando equilibrar a circulação de dados com a preservação dos direitos fundamentais do titular.

Essa finalidade está expressamente prevista no artigo 1º da LGPD, ao dispor que a lei trata do uso de dados pessoais, inclusive em meios digitais, por pessoas naturais ou jurídicas de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Dessa forma, o titular dos dados ocupa posição central no regime jurídico da proteção de dados, sendo definido pela própria LGPD como a pessoa natural a quem se referem os dados pessoais objeto de tratamento. Nesse sentido, a tutela legal não se limita ao reconhecimento abstrato do direito, mas busca assegurar garantias concretas diante dos riscos decorrentes do vazamento, do uso indevido, da circulação não autorizada e do tratamento incompatível com a finalidade informada.

Sob a perspectiva jurídica, o tratamento de dados pessoais também se relaciona à ideia de risco, uma vez que a circulação e o armazenamento de informações podem causar danos relevantes à esfera individual do titular. Nesse sentido, a doutrina da responsabilidade civil permite compreender que atividades que envolvem potencial de dano exigem cautela, segurança e mecanismos adequados de prevenção. Aplicada ao campo da proteção de dados, essa lógica reforça a necessidade de medidas eficazes de governança, controle e responsabilização, especialmente quando se trata de dados biométricos, cujo comprometimento pode gerar consequências mais graves e duradouras.

Por essa razão, a análise dos dados pessoais não pode ser dissociada da discussão sobre os dados sensíveis. Se os dados pessoais em geral já demandam proteção jurídica, os dados sensíveis exigem tutela ainda mais rigorosa, justamente por envolverem informações capazes de expor o titular a discriminação, violação da intimidade e restrições indevidas de direitos. É nesse ponto que se aprofunda a discussão seguinte, voltada à compreensão do que são dados sensíveis e de quais garantias jurídicas existem para proteger essas informações no contexto da biometria e da era digital.

5 - DADOS SENSÍVEIS

Nos termos do art. 5º, II, da Lei nº 13.709/2018, dados pessoais sensíveis são aqueles relacionados à 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 dado biométrico, quando vinculado a uma pessoa natural. Nessa perspectiva, os dados biométricos entre eles a biometria da íris inserem-se em categoria jurídica que exige tutela reforçada, justamente porque seu tratamento indevido pode comprometer direitos fundamentais da personalidade, como privacidade, liberdade, igualdade e dignidade da pessoa humana (art. 5º, II, da LGPD).

A centralidade dos dados sensíveis neste artigo decorre do fato de que a biometria da íris, objeto do estudo, é expressamente enquadrada pela LGPD como dado sensível. Por essa razão, sua coleta, armazenamento, compartilhamento e tratamento não podem ocorrer de forma indiscriminada. A própria LGPD estabelece regime mais rigoroso para esses dados, sobretudo no art. 11, ao exigir hipóteses legais específicas para seu tratamento, o que demonstra que não se trata de mera informação técnica, mas de conteúdo altamente protegido pelo ordenamento jurídico brasileiro.

5.1 - Desafios éticos

A proteção de dados sensíveis também envolve desafios éticos relevantes. Em uma sociedade marcada pela circulação massiva de informações, o tratamento de dados pessoais pode ser desvirtuado para práticas de vigilância excessiva, exploração econômica e perfilamento indevido. Por isso, a tutela ética desses dados exige que o titular seja informado, de forma clara, acessível e compreensível, acerca da finalidade da coleta, da possibilidade de compartilhamento, da base legal utilizada e dos riscos inerentes ao tratamento, em consonância com os princípios da finalidade, adequação, necessidade, transparência e segurança previstos na LGPD (art. 6º).

Quando se trata de dados sensíveis, o dever de transparência torna-se ainda mais importante, porque a deficiência informacional do titular pode comprometer o exercício efetivo de seus direitos. Assim, não basta que a organização possua base legal abstrata para o tratamento; é necessário que o uso da informação observe proporcionalidade, finalidade legítima e respeito à autodeterminação informativa. No campo da biometria, esse cuidado é ainda mais rigoroso, justamente porque a informação está ligada ao próprio corpo do titular e não pode ser simplesmente substituída como ocorre com uma senha ou código de acesso.

5.2 - Previsão legal no brasil

No Brasil, a proteção dos dados sensíveis está inserida em um sistema normativo composto pela Constituição Federal, pela LGPD e por regras de responsabilização civil, administrativa e, em situações específicas, penal. No plano administrativo, o art. 52 da LGPD prevê que os agentes de tratamento ficam sujeitos, entre outras medidas, a advertência, multa simples de até 2% do faturamento da pessoa jurídica de direito privado, limitada a R$ 50.000.000,00 por infração, multa diária, publicização da infração, bloqueio e eliminação dos dados pessoais, além de suspensão parcial do funcionamento do banco de dados e suspensão da atividade de tratamento por até seis meses, prorrogáveis por igual período.

Além da própria LGPD, a ANPD regulamentou a dosimetria e a aplicação dessas sanções por meio da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que detalha critérios e parâmetros para o cálculo das multas e disciplina medidas como bloqueio, eliminação e suspensão do banco de dados. Isso reforça que a proteção de dados sensíveis não depende apenas de comandos genéricos da lei, mas também de instrumentos regulatórios voltados à sua efetiva fiscalização e concretização.

No plano penal, determinadas condutas relacionadas ao uso indevido de informações podem configurar crimes específicos. No caso da fraude eletrônica, o art. 171, § 2º-A, do Código Penal, com redação dada pela Lei nº 14.155/2021, prevê pena de reclusão de 4 a 8 anos e multa. Já o art. 313-A do Código Penal prevê, para a inserção ou facilitação da inserção de dados falsos em sistema de informações por funcionário autorizado, pena de reclusão de 2 a 12 anos e multa. Quanto à falsidade ideológica, o art. 299 do Código Penal estabelece pena de reclusão de 1 a 5 anos e multa, se o documento for público, e de 1 a 3 anos e multa, se o documento for particular.

Desse modo, a tutela jurídica dos dados sensíveis não se limita ao campo administrativo da proteção de dados, mas alcança também a responsabilização civil e, em hipóteses específicas, a esfera penal. Isso é especialmente relevante quando se considera que o tratamento indevido de dados biométricos pode gerar discriminação, exposição indevida da intimidade, prejuízos econômicos e danos duradouros à esfera jurídica do titular.

5.3 - Regulação geral de proteção de dados (rgpd)

O Regulamento Geral sobre a Proteção de Dados da União Europeia foi proposto em 2012, adotado em 27 de abril de 2016, entrou em vigor em 24 de maio de 2016 e passou a ser aplicável em 25 de maio de 2018. Seu objetivo foi fortalecer a proteção da privacidade,

harmonizar as regras de tratamento de dados entre os Estados-membros e ampliar o controle do titular sobre suas informações pessoais. No âmbito europeu, a proteção de dados é tratada como direito fundamental, e o RGPD consolidou-se como uma das principais referências regulatórias contemporâneas sobre o tema.

O regulamento europeu também prevê mecanismos rigorosos de enforcement. Segundo a Comissão Europeia, em caso de infração, as autoridades de proteção de dados podem aplicar advertências, reprimendas, proibição temporária ou definitiva de tratamento e multas de até € 20 milhões ou 4% do faturamento anual global da organização, o que reforça a centralidade da responsabilização no modelo europeu.

5.4 - Impactos da rgpd no brasil

Os impactos do RGPD ultrapassaram o espaço territorial da União Europeia, alcançando empresas localizadas em outros países que tratam dados de pessoas residentes no bloco europeu. Isso significa que empresas brasileiras podem ser submetidas às exigências do regulamento quando oferecem bens ou serviços a residentes da União Europeia ou monitoram seu comportamento. Tal característica demonstra a dimensão extraterritorial do RGPD e ajuda a explicar sua influência no desenvolvimento da cultura regulatória da proteção de dados em diferentes países, inclusive no Brasil.

Além de seus efeitos diretos, o RGPD também exerceu influência relevante sobre a consolidação da LGPD, especialmente no que se refere à centralidade do titular, à proteção reforçada dos dados sensíveis, à necessidade de base legal para o tratamento e à responsabilização dos agentes de tratamento. Assim, embora os dois diplomas não sejam idênticos, é inegável que o modelo europeu serviu de importante referência para o amadurecimento normativo brasileiro.

5.5 - A lei geral de proteção de dados

Foi então que nestes moldes do RGPD, que nossa legislação brasileira passou a tratar biometria como dado sensível, sua origem está relacionada com a General Data Protection Regulation ou RGPD, que em português se traduz para: Regulamento Geral sobre a Proteção de Dados, com esta rigorosidade de privacidade e segurança de dados da União Européia (UE). Esta referida lei visa garantir aos cidadãos da União Europeia o controle sobre seus dados pessoais, o que inclui, tratamento de dados, coleta, armazenamento, uso e até mesmo o

compartilhamento de informações mediante autorização.

A origem para a realização da LGPD, teve início em 2018, mas sendo sancionada somente e entrando em vigor em setembro de 2020, pela Lei 13.709/2018. Seus objetivos foram elaborados para atender princípios fundamentais, dentre eles: Finalidade, adequação, livre acesso, qualidade dos dados, transparência, prevenção, segurança, não discriminação, além da responsabilização.

Mas até os dias atuais sua implementação enfrenta desafios, a baixa conscientização da população e das empresas sobre a importância da proteção de dados. No campo da tecnologia, há a necessidade de investimento em segurança da informação e uma amplitude em infraestrutura digital. Para que ocorra uma consonância da LGPD com outras normas, como o Marco Civil da Internet e legislações setoriais.

Outro importante fator está relacionado com o vazamento de dados, estes podendo gerar prejuízos financeiros e com gravíssimos danos à reputação, além da manipulação política. Para que o tema sobre dados pessoais e transferência internacional, e pudesse ter a amparo jurídico e garantisse meios mais eficazes, diremos, mais segurança jurídica, em Agosto de 2024, entrou em vigor, a Resolução CD/ANPD, N° 19. Aprovando o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art.2º, inciso XIII, do Anexo I, do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I, do Regimento Interno da ANPD, e tendo em vista a deliberação tomada no processo nº 00261.000968/2021-06, resolve:

Art. 1º Esta Resolução aprova, na forma dos Anexos I e II, o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais, nos termos do art. 33, incisos I e II, alíneas 'a', 'b' e 'c', art. 34, art. 35, caput e §§ 1º, 2º e 5º, e art. 36 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Parágrafo único. Os agentes de tratamento que utilizam cláusulas contratuais para realizar transferências internacionais de dados deverão incorporar as cláusulas-padrão contratuais aprovadas pela ANPD aos seus respectivos instrumentos contratuais, no prazo de até 12 (doze) meses, contados da data de publicação desta Resolução.

Por meio desta resolução, que regulamenta sobre a transferência internacional de dados,

sobre as regras e procedimentos aplicáveis que precisam estar em conformidade com as disposições da Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 2018), em paridade com o Regimento Interno da autoridade Nacional de Proteção de Dados (ANPD), visando a garantia na transferência internacionais de dados pessoais sendo mais seguras e transparentes, estreitando o alinhamento entre direitos fundamentais e à a segurança jurídica, e ampliando o desenvolvimento econômico e a proteção dos titulares de dados pessoais.

O que poderia se assemelhar ao RGPD, que proporciona ao próprio titular ou cidadão acessar para corrigir, apagar e até mesmo restringir o uso de seus dados. Para uma melhor compreensão é necessário haver autorização legal e válida por aquele é o titular destas informações.

5.6 - Autoridade nacional de proteção de dados

A ANPD, é responsável por realizar fiscalização e regulamentar a aplicação da LGPD, no Brasil, tem por finalidade ser guardiã da privacidade e da proteção de dados pessoais, mas ser o órgão fiscalizador, foi necessário haver uma alteração na LGPD, instituído pela Lei n°13.853/2029, estava vinculada à Presidência da República, mas somente em 2022, que passou a ter natureza de autarquia, em caráter especial, para que pudesse ter maior autonomia administrativa e técnica. Toda essa estrutura segue uma organização hierárquica, contando com o Conselho Diretor, Conselho Diretor Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) e unidades técnicas para a realização de fiscalização e orientação.

Alguns pontos importantes podem ser observados quando passamos a compreender melhor sobre a atuação da ANPD, dentre elas encontramos impactos sociais e econômicos como:

- O fortalecimento na confiança digital, o comércio eletrônico, serviços financeiros e inovação tecnológica, podem atrair mais investidores para o setor.
- Outro ponto importante é perceptível, se trata entre empresas que se adequam à LGPD, ganham vantagem competitiva, agora para aquelas que descumprem podem ser penalizadas e com multas de até R$50 milhões, por infração.
- Há ainda um incentivo no campo acadêmico, com o prêmio Danilo Doneda de Artigos Científicos, relacionado à produção de conhecimento sobre privacidade e proteção de dados.

Ferramentas estas que a ANPD estende para o público acadêmico e que de certa forma acaba produzindo material científico para alcançar a população que precisa ter conhecimento sobre a destinação de seus dados pessoais, o que é um grande desafio para os dias atuais.

A ANPD precisa consolidar a cultura da proteção de dados no Brasil, embora tenha encontrado muitos desafios, dentre eles, maior capilaridade, engajamento da sociedade, e o seu próprio fortalecimento institucional, além do alinhamento com as práticas globais que norteiam o mundo.

5.7 - Diferença entre lgpd e rgpd

Diante das análises feitas das referidas leis, encontramos pontos semelhantes e distintos. Todavia, essa divergência ocorre no escopo territorial, sanções, estrutura da fiscalização e maturidade regulatória. Porém, a RGPD, possui uma rigorosidade e é consolidada, por outro lado, a LGDP, enfrenta dificuldades para sua implementação e conscientização, mas que a mesma tem características próprias que repercutem sobre o contexto jurídico e social de nosso país.

ASPECTOS	LGPD	RGPD
Entrada em vigor	Setembro de 2020	Maio de 2018
Órgão fiscalizador	ANPD (Autoridade Nacional de Proteção de Dados)	CNPD (Comissão Nacional de Proteção de Dados) e autoridades nacionais em cada país
Multas	Até 2% do faturamento, limitadas a R$ 50 milhões por infração	Até € 20 milhões ou 4% do faturamento global
Escopo territorial	Empresas que tratam dados de pessoas no Brasil	Empresas que tratam dados de cidadãos da UE, mesmo fora da Europa
Dados sensíveis	Saúde, biometria, origem racial, religião, opinião política	Idêntico, mas com maior detalhamento e restrições.

Embora sejam legislações próximas, porém, não são idênticas. Entendemos que com uma fiscalização mais dura e com sanções mais pesadas se torna mais evidente sua aplicabilidade e avanços. Vale ressaltar que a LGPD amplia com hipóteses para justificar o tratamento de dados. Quanto o RGPD, é mais restrito e objetivo.

A LGPD coloca em vigor que somente é possível o tratamento de dados mediante consentimento claro e em hipóteses legais específicas, como segurança pública ou mesmo cumprimento de obrigação legal.

O RGPD fortalece a proteção de dados biométricos, requer bases legais resistentes, precisas e com medidas técnicas de segurança.

5.8 - Anonimização de dados sensíveis

A era digital é conhecida como período da informação ou era tecnológica. Isso significa que tudo está convergindo para o ambiente digital, processo que vem sendo impulsionado por constantes transformações históricas, inicialmente relacionadas às revoluções industriais e consolidado no final do século XX, com a expansão da internet e a popularização da informática. Essa transição dos processos físicos para o campo digital transformou profundamente as formas de comunicação, armazenamento e circulação de informações. Nesse sentido, Almeida e Soares (2022) destacam que os avanços tecnológicos trazidos pela era digital fizeram com que as informações coletadas por empresas e instituições se tornassem ativos de grande valor, o que elevou a proteção desses dados a uma posição de prioridade.

O tema da anonimização de dados pessoais tem recebido destaque em razão de sua relevância na atualidade e também por sua previsão na Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que define a anonimização como processo técnico destinado a eliminar a possibilidade de associação entre os dados e seu titular. Trata-se de mecanismo que busca reduzir riscos de utilização ilícita e evitar danos à privacidade do indivíduo. Nesse contexto, Santana e Ansari (2023) observam que a proteção de dados e a privacidade assumem posição central em um mundo cada vez mais interconectado, justamente por estarem ligadas à autonomia, à dignidade e ao espaço pessoal do indivíduo.

O alto fluxo de informações pessoais circulando em tempo real, a conectividade global proporcionada pela internet, a digitalização de processos físicos, a expansão das transações documentais e a utilização de dados por empresas e pelo poder público como insumo para decisões vêm redefinindo as dinâmicas sociais e institucionais. Nesse cenário, as plataformas

digitais assumem papel central nas relações de trabalho, na comunicação, no comércio e na própria organização da vida social. Almeida e Soares (2022) ressaltam que, na era digital, diversos países passaram a perceber a necessidade de regulamentar o tratamento, a disponibilização, a acessibilidade e o uso desses bens informacionais, precisamente porque os dados pessoais passaram a ocupar lugar de destaque nas transações contemporâneas.

Por isso, diante desse novo cenário digital, a LGPD estabelece diretrizes para o tratamento de dados anonimizados no país, além de diferenciar dados pessoais e dados sensíveis. A legislação brasileira busca assegurar a proteção da privacidade e fortalecer mecanismos de segurança jurídica no tratamento das informações, especialmente quando se considera o desafio de impedir a vinculação direta entre dados e indivíduos. Ainda nessa direção, Santana e Ansari (2023) destacam que a proteção de dados, na sociedade da informação, encontra fundamento justamente na necessidade de garantir a inviolabilidade da pessoa também em sua dimensão eletrônica.

Como a legislação brasileira foi influenciada por referências internacionais, especialmente pelo GDPR europeu, a anonimização passou a ser reconhecida como técnica relevante de proteção de dados, embora se distinga da pseudonimização, que admite a possibilidade de reidentificação mediante recomposição de elementos identificadores. Nesse cenário, medidas como substituição de identificadores diretos, generalização de dados e técnicas estatísticas são utilizadas para reduzir a exposição indevida do titular. Baig, Eskeland e Yang (2024) ressaltam que dados biométricos e outros atributos sensíveis devem ser armazenados e processados de forma orientada à preservação da privacidade, justamente porque seu tratamento inadequado pode expor o titular a riscos relevantes.

Além disso, embora técnicas de proteção e ocultação de dados sejam importantes, elas não eliminam completamente os riscos. Zhang, Zhang e Deng (2025) ressaltam que a disseminação indevida de informações biométricas, os vazamentos de dados e os usos não autorizados dessas informações evidenciam a necessidade de mecanismos robustos de supervisão, monitoramento e governança. Na prática, isso demonstra que a atualização constante das técnicas de proteção permanece necessária para reduzir o risco de reidentificação e equilibrar, ao mesmo tempo, privacidade, pesquisa, inovação e utilidade social dos dados.

Na prática, é necessário que as organizações adotem técnicas adequadas de proteção de dados e atualizem continuamente seus mecanismos de segurança, especialmente quando tratam informações biométricas e outros dados sensíveis. Quando isso não ocorre, aumentam-se os

riscos de vazamento, uso indevido e comprometimento da privacidade do titular. Nesse sentido, Baig, Eskeland e Yang (2024) demonstram que o tratamento de dados biométricos e comportamentais exige soluções orientadas à preservação da privacidade, enquanto Zhang, Zhang e Deng (2025) reforçam a importância de estruturas de governança e monitoramento capazes de prevenir a exploração indevida dessas informações.

Vale ressaltar, por fim, que tanto a LGPD quanto o RGPD buscam equilibrar o desenvolvimento tecnológico com a proteção de direitos fundamentais. Santana e Ansari (2023) destacam que a proteção de dados e a privacidade se afirmam como direitos fundamentais justamente em razão do crescimento da circulação, do armazenamento e da análise de informações pessoais em ambientes digitais, o que exige constante aperfeiçoamento dos instrumentos normativos e institucionais de proteção.

6 - CONSIDERAÇÕES FINAIS

Este artigo baseou-se em revisão bibliográfica e analisou na busca em compreender possíveis impactos sociais e jurídicos do uso da biometria ocular, tanto na comparação com outros mecanismos biométricos e suas aplicações.

Além disso, realizamos uma vasta leitura bibliográfica fundamentada nas legislações internacionais e nacionais, como a LGPD e GDPR, bem como a revisão de literaturas que serviram de base para a pesquisa, e passando a observar os possíveis conflitos com as referidas normas, bem como os dados e consequências jurídicas. Analisou-se ainda o real esforço da Autoridade Nacional de Proteção de Dados (ANPD), em regulamentar o uso de técnicas de anonimização para que sejam mais robustas e atualizadas, assim como a fiscalização.

Tendo em vista que a anonimização é fundamental para haver equilíbrio diante de tanta inovação tecnológica e à proteção de direitos, sem que haja qualquer comprometimento à privacidade.

Em uma análise qualitativa e exploratória de compreensão de todo este aparato tão presente nos dias atuais que é o caso da biometria e seus mecanismos pela qual passamos a entender sobre os prós e contras.

Tendo em vista que o estudo de caso foi apreciado com uma investigação detalhada na prática de suas aplicações no caso em bancos, aeroportos, smartphones, eletrônicos e outros mecanismos.

Destacamos ainda os reais desafios existentes, embora tenhamos acompanhado e visto mecanismos de alta definição e qualidade e de última geração, mas que apresentam possíveis possibilidades de erros no tratamento destes dados, pois envolve informações íntimas e potencialmente discriminatórias, tanto em processos seletivos quanto no acesso a serviços, além de uso indevido por empresas para obtenção de lucros. Mesmo havendo o trato jurídico conforme previsão estabelecida na Constituição Federal (1998), no artigo 5°, X, sobre as garantias ao direito à intimidade e à vida privada e sendo reforçada pela LGPD (2018), estabelecendo que o tratamento de dados sensíveis só pode ocorrer em hipóteses específicas, como consentimento explícito ou cumprimento de obrigação legal, como já mencionado, na construção deste artigo.

É óbvio que foram observados desafios, não pequenos, mas consideráveis na busca de soluções para se manter o bem em questão que é a dignidade da pessoa humana.

Nesta observação, os dados analisados resultaram que ambas as leis possuem equivalência para para garantir à proteção de dados pessoais para fins estatísticos, científicos ou de políticas públicas sem risco de exposição pessoal, o que por força de Lei como o Marco Civil da Internet (2014), se estende para a proteção real na preservação à proteção de dados pessoais no ambiente digital, podendo termos precisão no uso da anonimização.

Portanto, é sabido do valor social e econômico da internet e do seu alto potencial tecnológico, e a íris como identificador biométrico, deve ter seu uso equilibrado com a proteção de dados pessoais, por outro lado, quando tratamos da proteção de dados, bem como os meios tecnológicos, estes precisam ter um acompanhamento amplo e com um arcabouço jurídico consistente que assegure a proteção à privacidade e dos direitos fundamentais e evitando brechas que possam comprometer a privacidade.

É salutar que todo esse avanço tecnológico tenha sido significativo para nossa sociedade, mas que nada possa substituir o real valor que é a proteção de dados pessoais e que a utilização ao uso da biometria ocular ou outros mecanismos que já mencionados neste artigo, possam legitimizados pelas leis brasileiras, em sua proporcionalidade e garantindo a segurança para os indivíduos que a usam, mantendo-se assim um equilíbrio entre tecnologia e relações digitais futuras, evitando-se com que as possíveis brechas possam comprometer um direito fundamental que é a privacidade da pessoa, conforme previsto no artigo 5º da Constituição Federal do Brasil, que garante direitos fundamentais, assegurando a igualdade, liberdade, segurança e dignidade a todos os indivíduos.

7 - REFERÊNCIAS BIBLIOGRÁFICAS

AL-DEBEI, Mutaz M.; HUJRAN, Omar; AL-ADWAN, Ahmad Samed. Net valence analysis of iris recognition technology-based FinTech. **Financial Innovation**, v. 10, art. 59, 2024. DOI: 10.1186/s40854-023-00509-y.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, 2022. DOI: 10.1590/1981-5344/25905.

BAIG, Ahmed Fraz; ESKELAND, Sigurd; YANG, Bian. Novel and Efficient Privacy-Preserving Continuous Authentication. **Cryptography**, v. 8, art. 3, 2024. DOI: 10.3390/cryptography8010003.

BEN CHAABANE, Slim; HARRABI, Rafika; SEDDIK, Hassene. Iris Recognition System Using Advanced Segmentation Techniques and Fuzzy Clustering Methods for Robotic Control. **Journal of Imaging**, v. 10, art. 288, 2024. DOI: 10.3390/jimaging10110288.

BHATT, Sushil; SEHRAWAT, Jagmahender Singh; GUPTA, Vishali. A systematic review of iris biometrics in forensic science: applications and challenges. **Egyptian Journal of Forensic Sciences**, v. 15, art. 12, 2025. DOI: 10.1186/s41935-025-00431-7.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: **Presidência da República**, 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ: **Presidência da República**, 1940.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: **Presidência da República**, 2002.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: **Presidência da República**, 2018.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. Brasília, DF: **Presidência da República**, 2019.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: **Presidência da República**, 2021.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nº 13.709, de 14 de agosto de 2018, nº 13.853, de 8 de julho de 2019, e nº 7.689, de 15 de dezembro de 1988. Brasília, DF: **Presidência da República**, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: **ANPD**, 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Brasília, DF: **ANPD**, 2024.

HAASNOOT, Erwin; SPREEUWERS, Luuk J.; VELDHUIS, Raymond N. J. Presentation attack detection and biometric recognition in a challenge-response formalism. **EURASIP Journal on Information Security**, v. 2022, art. 5, 2022. DOI: 10.1186/s13635-022-00131-y.

KORDAS, Adrian; et al. Synthetic Iris Images: A Comparative Analysis between Cartesian and Polar Representation. **Sensors**, v. 24, n. 7, art. 2269, 2024. DOI: 10.3390/s24072269.

LIU, Guoyang; et al. An Efficient and Accurate Iris Recognition Algorithm Based on a Novel Condensed 2-ch Deep Convolutional Neural Network. **Sensors**, v. 21, n. 11, art. 3721, 2021. DOI: 10.3390/s21113721.

MALGHEET, Jasem Rahman; MANSHOR, Noridayu Bt; AFFENDEY, Lilly Suriani. Iris Recognition Development Techniques: A Comprehensive Review. **Complexity**, v. 2021, Article ID 6641247, 2021. DOI: 10.1155/2021/6641247.

NURHUDA, Abid; SAFITRI, Nuri. The Use of Biometrics in Public Services and the Risk of Privacy Violations. **Jurnal Hukum Siber dan Regulasi Teknologi**, v. 1, n. 1, 2026.

RUBIO, Arthur; MAGNIER, Baptiste. Preprocessing of Iris Images for BSIF-Based Biometric Systems: Binary Detected Edges and Iris Unwrapping. **Sensors**, v. 24, n. 15, art. 4805, 2024. DOI: 10.3390/s24154805.

SANTANA, Paulo Campanha; ANSARI, Faiz Ayat. Data protection and privacy as a fundamental right: a comparative study of Brazil and India. **Journal of Liberty and International Affairs**, v. 9, n. 3, p. 456-470, 2023. DOI: 10.47305/JLIA2393555cs.

SUMI, Mst Rumana; et al. A Comprehensive Evaluation of Iris Segmentation on Benchmarking Datasets. **Sensors**, v. 24, n. 21, art. 7079, 2024. DOI: 10.3390/s24217079.

ZHANG, Wenyi; ZHANG, Hengtian; DENG, Zhouyang. Public attitude and media governance of biometric information dissemination in the era of digital intelligence. **Scientific Reports**, v. 15, art. 2419, 2025. DOI: 10.1038/s41598-025-86603-w.