

USO DO LEGÍTIMO INTERESSE NO TRATAMENTO DE DADOS SENSÍVEIS II

O tratamento de dados pessoais sensíveis com base exclusiva no legítimo interesse **não é admitido** pela LGPD, todavia, o **legítimo interesse pode ser utilizado como fundamento auxiliar e complementar**, especialmente nas hipóteses expressas do art. 11 (como prevenção à fraude e segurança, exercício regular de direitos, proteção da vida), desde que cumpridos alguns requisitos.

Este guia prático tem como objetivo fornecer subsídios técnicos e jurídicos para a aplicação do legítimo interesse como fundamento auxiliar no tratamento de dados sensíveis e visa analisar a possibilidade jurídica de fundamentar o tratamento de dados pessoais sensíveis com base no legítimo interesse do controlador, considerando o texto expresso da **LGPD**, a **Nota Técnica nº 175/2023 da ANPD**, as orientações do **Grupo de Trabalho Artigo 29** da União Europeia, **Comitê dos Direitos da Criança - Comentário geral n.º 14 (2013)** e o **Guia de Legítimo Interesse da ANPD**.

DOS FATOS

O tema é um dos mais complexos da LGPD, pois nem sempre é claro o limite do que são ou não dados sensíveis vejamos porque

INFERÊNCIA INDEVIDA

O RISCO INVISÍVEL NO TRATAMENTO DE DADOS

Dado pessoal¹: “*Qualquer* informação **relativa a** uma pessoa singular **identificada ou identificável** (“titular dos dados”); uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, em especial por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social”. – ***É toda declaração ou informação que possa estar ligada a um indivíduo, podendo ser “objetivas”, “subjetivas” e não necessariamente correta, verdadeira ou comprovada.***

Inferência Indevida: A Armadilha Oculta da LGPD. Quando o Simples se Torna Sensível e um Problema.

[...] ²é possível que dados pessoais sensíveis sejam revelados a partir do tratamento de dados que não possuem essa característica, mediante, por exemplo, procedimentos de inferência ou de cruzamento de bases de dados. A esse tipo de tratamento, em que há uma revelação ou identificação indireta de aspectos sensíveis relacionados a personalidade do titular, com potencial lesivo a seus direitos e interesses, também se aplica o regime jurídico especial previsto na LGPD para os dados sensíveis, conforme previsto no art. 11, § 1º, da Lei. É o que ocorreria no caso de identificação da

¹ 01248/07/PT WP 136 ARTIGO 29 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS

² Minuta - Guia Orientativo Tratamento de Dados Pessoais de Alto Risco p. 26

etnia ou da convicção religiosa de um titular a partir do tratamento de outros dados não sensíveis, tais como o nome, o endereço e o perfil de consumo. **ANPD - Minuta - Guia Orientativo Tratamento de Dados Pessoais de Alto Risco**

Um e-mail, apelido, número de casa, um GPS, roupa, compras, nomes ou dados financeiros podem assumir a posição de dados sensível dependendo do contexto do tratamento - Art. 5º II da LGPD

- Uma simples foto não é categorizada como dado sensível, porém se tirada dentro de uma organização religiosa, pode declarar sua religião, uma foto de perfil uma origem racial ou étnica.
- Uma foto de um fotografo, pode ser solicitada pela polícia para identificar um crime ou uma pessoa.
- Pelo GPS ou Localização, é possível **inferir padrões de comportamento**, o que pode levantar preocupações sérias de privacidade e discriminação.
 - ✓ **Frequência e horário de visita a locais religiosos**, como igrejas, mesquitas, sinagogas, templos etc.
 - ✓ Visitas regulares a determinados locais em dias e horários específicos (domingos às 9h na mesma igreja) podem ser **usados para inferir práticas religiosas**.
 - ✓ Combinando a localização com outros dados (buscas, redes sociais, consumo), **algoritmos podem rotular perfis com base em padrões religiosos**, que podem ser usados para **segmentação de anúncios** — por exemplo, campanhas eleitorais podem direcionar mensagens para grupos religiosos específicos.
 - ✓ **Frequentes visitas a locais ligados a grupos extremistas**, podem entrar em **monitoramento ou investigação**.
- Visitas frequentes a uma clínica oncológica, centro de tratamento de HIV ou templo religioso, pode revelar dados sobre Saúde, religião ou orientação sexual.

Coleta inicial mesmo com dados não sensíveis e sem intenção, podem levar o controlador a tratar dados sensíveis por consequência indireta sem base legal adequada.

Dado Pessoal Simples → Dado Sensível "Resultado"		
Dado Pessoal Simples	Contexto de Uso ou Análise	Dado Sensível Inferido
Localização via GPS	Presença frequente em templos, clínicas, partidos, sindicatos, casas de apoio LGBTQIA+	Religião, saúde, filiação política, orientação sexual
Nome completo	Nome revela origem (ex: nomes árabes, africanos, judaicos)	Origem racial/étnica, religião
E-mail corporativo	nome.sobrenome@partido.com, @igreja.org	Filiação política, religião
Histórico de compras	Compra de remédios controlados, suplementos hormonais, produtos religiosos	Saúde física/mental, identidade de gênero, religião, condições médicas, como intolerâncias, HIV, diabetes
Check-in em redes sociais	Participação em eventos religiosos, políticos ou terapêuticos	Religião, política, saúde
Imagem (foto ou vídeo)	Uso de turbante, quipá, cruz, deficiência visível	Religião, deficiência, origem étnica, PCD
Voz (áudio)	Fala com conteúdo emocional, religioso ou político	Saúde mental, religião, opinião política
Profissão	Profissões vinculadas a partidos, igrejas, causas sociais (ex: padre, pastor, ativista)	Religião, convicção filosófica, condição de saúde (acompanhante terapêutico), orientação política (militante)
Histórico de navegação	Acesso frequente a sites de grupos religiosos, terapias ou organizações políticas	Religião, saúde, filiação política
Horário de uso de aplicativos	Acesso a aplicativos de oração em horários religiosos específicos	Religião
Dados de mobilidade urbana	Visita recorrente a clínicas de reabilitação ou hospitais especializados	Saúde
Frequência em academias ou clínicas de estética	Relacionado a tratamentos hormonais ou cirurgias específicas	Identidade de gênero
Dispositivo ou sistema operacional	Uso de leitores de tela, modo de acessibilidade ativado	Deficiência visual ou física
Participação em grupos de WhatsApp ou Telegram	Grupos com temáticas religiosas, políticas ou de apoio à saúde mental ex-presidiários ou grupo de apoio	Religião, política, saúde mental, Círculo Espírita ou oração, Reunião do Partido, Nutricionista – Intolerância alimentar, Cozinha – Restrição,

		Católicos Progressistas ou Famílias com Autistas
Consultas em buscadores	Pesquisas sobre HIV, depressão, mudança de gênero, partidos políticos	Saúde, identidade de gênero, política
Filiação a clube ou associação	Associação em sindicato, igreja ou partido	Filiação política, religião
Assinaturas de revistas ou canais	Revista Espírita, Canal Cristão, Jornal de esquerda/direita	Religião, opinião política
Dados de vestuário (em fotos)	Uso constante de símbolos religiosos, roupas litúrgicas	Religião
Dados financeiros	Gastos com clínicas médicas, ONGs religiosas ou partidos	Saúde, religião, política
Agenda de Compromisso	Rotina e compromissos frequentes	Atividades religiosas, saúde, psicológicas ou psiquiátricas, hemodiálise, sessões espíritas, reuniões partidárias
Endereço	O endereço físico de clínicas, hospitais ou centro de reabilitação	Um abrigo, A.A, N.A, LGBTQIA+, Igreja, hospital psiquiátrico ou centro de reabilitação
Nome Social	Decreto Nº 8.727, de 28 de Abril De 2016	Identidade de gênero
Entrada em ambientes ou Horário de uso de aplicativos.	Uso ou visitas frequentes - rotinas	Pode indicar questões de saúde (ex: visitas frequentes a hospitais ou uso noturno de apps de apoio psicológico). Site de Igrejas.
Sites Acessados	Histórico de Acessos	Orientação sexual, religião, posicionamento político, doenças etc.
Participação em eventos	Filiação político ou religioso	Marcha para Jesus ou Parada LGBT
Observações em documentos e formulários	Tratamento, Restrições, Doenças, Encontros, Condições Físicas	Saúde, Religião, política, PCD
Acesso Físico	Rampa de acessibilidade, Braile(escrita e leitura tátil) Cadeirantes, Idosos, Pessoas com deficiência	Saúde, Condições Físicas , Idade
Assentos Preferenciais	Assento marcado como preferencial, cartão de passagem ou imagem ou a partir do comportamento - câmeras (CFTV)	Deficiência, gravidez, idade avançada ou condição de saúde.
Horário de transporte público	Uso constante a certas horas para trabalho especial, restrito ou agendamento médico	Saúde , religião
Tipo de escola	A escola ou curso frequentado. Escola especializada em TEA ou cegueira. Adventista ou Batista	Saúde – Deficiência , Religião
Cartão de benefícios ou isenções	Isenção em transporte por “tratamento contínuo” , baixa renda ou cotas	Deficiência, doença grave. Etnia
Idioma ou dialeto em formulários	Preenchimento de formulário com idioma pode indicar origem e crença.	Origem racial, étnica ou religiosa
Contato emergencial	Pessoa com acompanhante fixo pode estar sob tutela legal por incapacidade.- Dependência de cuidados especiais	Saúde, Condições físicas e psicológicas;
Escolha de plano de saúde	Planos podem ser escolhidos por acomodações, cobertura ou idade	Saúde, Doença,
Horário de check-in em aplicativos de controle de ponto	Jornada diferenciada por saúde, amparo legal ou licença de tratamento médico.	Saúde, Doença
Tipo de refeição	Titular com dieta “sem glúten e sem lactose” pode ter condição crônica. Doenças (ex: diabetes, intolerâncias, alergias graves)	Saúde
Participação em grupos internos	Filiação a sindicato, posicionamento político ou vulnerabilidades emocionais (comissão sindical, diversidade, apoio psicológico)	Religião, Política, Saúde, opção sexual
Insígnia ou símbolos	Símbolo de “comunicação alternativa”.	Saúde - Deficiência (insígnia para surdos ou autistas).
Reserva de espaços específicos	Registro de uso constante de sala pode indicar diagnóstico de ansiedade severa (sala silenciosa, sala de oração, sala sensorial) - Condições neurológicas (ex: autismo).	Saúde, Religião
I.A - Micro expressões ou voz coletados em sistemas de IA	Sistema que analisa tom de voz ou expressões em entrevistas. - Estado de saúde mental, histórico de depressão, burnout ou assédio.	Saúde. Etnia, Religião
Assinatura ou digitação (biometria comportamental)	Alterações na caligrafia digital ao longo do tempo podem revelar condição crônica. - Doenças degenerativas ou neuromotoras (ex: Parkinson, esclerose)	Saúde
Trocas de turnos ou afastamentos	Acompanhamento médico frequente, dependência de terceiros, ou condições cíclicas (ex: epilepsia, endometriose). - Padrão de afastamento sempre em períodos específicos do mês.	Doença, Saúde
Eventos internos com temas sensíveis	Funcionário inscrito em palestra sobre “vivência trans no ambiente corporativo”. Assédio moral	Orientações sexuais, crenças, saúde.
Iluminação diferenciada em ambientes de trabalho ou estudo	Requisição de luz indireta ou ausência de fluorescentes. - Epilepsia fotossensível, autismo ou enxaqueca crônica.	Doença – Saúde
Preferência por fila separada ou discreta em eventos	Pedido para evitar aglomeração pode revelar condição neurológica. - Transtorno de ansiedade social, TEA ou fobia.	Saúde – Doença

Atendimento com intérprete de Libras	O simples registro desse atendimento já pode configurar tratamento de dado sensível. Deficiência auditiva (dado sensível de saúde)	Saúde
Vagas específicas - Estacionamento	Um crachá que autoriza o uso frequente da vaga de gestante. Deficiência (vaga preferencial), idade avançada, ou gestação.	Deficiência, gravidez, idade avançada ou condição de saúde.
Recusa de datas comemorativas (ex: festas, aniversários, natal)	Convicção religiosa (ex: Testemunhas de Jeová, adventistas).	Religião
Tipo de papel usado	Pedido para usar Arial 16 preta sobre fundo amarelo. - Baixa visão ou dislexia.	Saúde – Doença
Emojis, figurinhas ou selos em plataforma	Uso recorrente de bandeira trans, arco-íris ou símbolos religiosos.	Identidade de gênero, orientação sexual, posicionamento ideológico.
Uniformes sob medida ou adaptações	Mesmo sem laudo médico, o pedido já revela informação sensível indiretamente. - Condições físicas específicas (nanismo, prótese, coluna, etc.).	Saúde, Condições físicas
Leitura em voz alta em sites ou aplicativos	O registro de uso frequente dessa função pode ser rastreável e inferido. - Baixa alfabetização, dislexia ou deficiência visual.	Saúde – Doença
Rejeição de alimentação	Requisição constante de comida alternativa por motivo de fé ou saúde. - Crença religiosa (adventista), ou condição médica (celíacos).	Religião, Saúde
Atividades físicas específicas	Atividades físicas específicas oferecidas por planos de saúde ou empresas - Inscrição em grupo de reabilitação pós-AVC ou ioga terapêutica monitorada.	Saúde – Doença
Avatar, nome de usuário ou nickname	Usuário que se identifica como "Ela/Delas" em plataforma interna. Identidade de gênero diferente do sexo registral, ou orientação sexual.	Religião, Opção Sexual
Horários alternativos	Prática de orações em horários definidos (ex: islâmicos), sabatistas, entre outros. Mesmo sem declarar a fé, os horários revelam o rito.	Religião
Cadeira ergonômica	Pode indicar hérnia, lesões de coluna ou outras condições ortopédica	Saúde
Tempo adicional para tarefas ou provas	Pode indicar deficiência intelectual, TDAH ou dislexia.	Saúde
Recusa de contato físico	Pode revelar crença religiosa, TEA ou trauma psicológico.	Religião, Saúde
Fone de ouvido	Seu uso pode indicar hipersensibilidade sensorial (ex: autismo)	Saúde
Agendamento de exames ginecológicos em adolescente	Pode indicar início precoce de atividade sexual, gravidez, abuso ou problemas hormonais.	Saúde – Doença
Cadastro em clínicas de fertilidade	Pode revelar infertilidade, casais homoafetivos ou tratamentos hormonais.	Opção Sexual, Saúde
Posts religiosos ou políticos	Uso de referências pessoais	Religião, Política, Sindicato
Teclado virtual ou ditado por voz	Pode indicar deficiência motora ou analfabetismo funcional.	Saúde
Embarque prioritário	Pode indicar deficiência, gestação de risco ou mobilidade reduzida.	Saúde
Aluguel social ou isenção de IPTU	Pode revelar vulnerabilidade social, doenças graves, HIV ou situações de violência doméstica.	Saúde
Doações frequentes	Pode revelar crenças, ideologia política ou religião.	Religião, Política
Grupos de apoio	Pode indicar condições de saúde, vida pregressa ou questões familiares delicadas.	A.A, N.A, LGBTQIA+, Igreja, hospital psiquiátrico ou centro de reabilitação
Retificação de nome	Pode revelar transição de gênero	Opção sexual
Troca de banheiro	Pode inferir identidade de gênero não cisnormativa ou condição médica.	Opção sexual, Saúde
Botão de pânico em aplicativo	Pode indicar histórico de violência doméstica ou perseguição. – Idoso debilitado	Saúde
Mudança de voz ao telefone	Pode permitir inferência sobre identidade de gênero, condição hormonal ou saúde.	Opção sexual, Saúde
Fraldas geriátricas ou dietas especiais via E-commerce	Pode indicar incontinência, doenças crônicas, Alzheimer, etc.	Saúde
Entrega com instruções como “não tocar a campainha”	Pode revelar condição psicológica, autismo, TEPT ou fobia.	Saúde
Processos que mencionam “violência doméstica”	Pode revelar condição de vulnerabilidade ou de gênero.	Saúde, Opção Sexual
Pseudônimo para audiências públicas	Pode indicar proteção contra represália por orientação sexual, religião ou saúde mental.	Religião, Saúde, Opção Sexual
Modo leitor fácil	Pode indicar deficiência intelectual ou baixa escolarização.	Saúde
Resposta por vibração” em apps médicos	Pode inferir surdez, distúrbios sensoriais ou motores.	Saúde
Objetos específicos	Pode revelar crença ou culto com normas de vestimenta (pulseiras, jalecos, distintivos)	Religião
Rejeição de transfusão	Pode indicar ser Testemunha de Jeová	Religião

Expressões, linguagem e comportamento	Pode indicar identidade de gênero não binária. Uso contínuo de pronomes neutros em formulários ou e-mails corporativos	Religião, Opção Sexual, Etnia
Avaliação Profissional	Entrevistas com RH com Avaliação comportamental, pontos positivos, pontos negativos ou HOBBY, podem revelar dados de Religião Opção Sexual e Doenças	Religião, Opção Sexual, Saúde
CadÚnico	Cadastro no CadÚnico com muita rotatividade de endereço, pode inferir situação de rua, violência doméstica ou abandono familiar.	Saúde,
Transferência Bancária	Transferências recorrentes para templos, igrejas ou centros religiosos	Religião
Cadastro em categorias específicas	Cadastro em categorias específicas de clientes como "servidor da segurança pública" ou "funcionário de presídio", pode expor riscos ligados à função, convicções políticas ou histórico de violência.	Opção política e sindicato
Cartão arco-íris	Pode indicar orientação sexual ou identidade de gênero.	Opção Sexual
Preferência por atendimento	Preferência por atendimento apenas por mulheres ou por pessoas religiosas - Pode revelar convicções religiosas, traumas ou gênero sensível.	Religião, Opção Sexual, Saúde

Nem todo dado sensível vem com um rótulo. Às vezes, o que parece ser apenas um dado comum — como localização ou nome — pode revelar informações pessoais delicadas. É nosso dever sempre avaliar o contexto."

Riscos:

1. Risco de Violação à LGPD
2. Discriminação e Prejuízos ao Titular
 - a. Discriminação indireta (ex: exclusão de crédito, planos de saúde mais caros, oferta restrita de serviços)
 - b. Estigmatização (ex: inferir que alguém tem HIV com base em geolocalização + horários de visita a clínicas)
 - c. Limitação de direitos (ex: decisões automatizadas baseadas em perfis)
3. Falhas em Avaliações de Riscos (RIPD)
4. Reputação da Empresa
5. Discriminação Algorítmica em Processos Seletivos
 - a. Universidade frequentada + geolocalização + redes sociais
6. Aumento Indevido de Plano de Saúde
 - a. Histórico de compras (ex: medicamentos para hipertensão)
 - b. Inferência sensível: Condição de saúde
7. Estigmatização por Suposta Orientação Sexual
 - a. Aplicativos utilizados + horários de acesso + locais frequentados
 - b. Preconceito, bullying ou até ser demitido com base em um perfil comportamental que sugira que ele pertence à comunidade LGBTQIA+.
8. Perseguição Religiosa
 - a. Geolocalização frequente (visitas regulares a templos específicos)
9. Decisões automatizadas injustas em crédito
 - a. Padrões de consumo e localização
 - b. Condição de saúde mental (ex: gastos impulsivos, medicamentos relacionados à ansiedade)
 - c. Negativa automática de crédito ou redução de limite sem justificativa plausível.
10. Danos morais e constrangimento público
 - a. Nome social, preferências de compra, histórico de navegação
 - b. Divulgação não autorizada pode gerar humilhação pública ou exposição indevida da intimidade.
11. Exclusão Educacional
 - a. Bairro de residência + padrão de consumo

1. FUNDAMENTAÇÃO NORMATIVA – INTERPRETAÇÃO DA LGPD

- **Art. 10 da LGPD** estabelece o legítimo interesse como base legal para tratamento de dados pessoais, desde que respeitados os direitos e liberdades fundamentais do titular e observada a necessidade e transparência do tratamento (incisos I e II, §§1º a 3º).
- **Art. 11 da LGPD** delimita hipóteses específicas para o tratamento de dados sensíveis, dentre as quais se destaca o inciso II, alínea “g”, que autoriza o tratamento para “garantia da prevenção à fraude e à segurança do titular”.

Nota-se, assim, que o legítimo interesse não figura diretamente como base exclusiva para dados sensíveis, mas pode ser considerado um ***fundamento auxiliar***, especialmente quando alinhado às hipóteses do art. 11.

A **Lei Geral de Proteção de Dados (LGPD)** estabelece no **Art. 11** hipóteses taxativas para o tratamento de **dados sensíveis**, como:

- **Inciso II, alínea “g”:** *“garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos”.*

Ocorre que o próprio **Art. 10 da LGPD** trata do **legítimo interesse do controlador** como hipótese legal para dados **não sensíveis**, mas:

- Reconhece o legítimo interesse como meio para proteger os direitos do titular (**art. 10, II**);
- Determina o uso de dados estritamente necessários (**art. 10, §1º**);
- E exige transparência e proporcionalidade (**art. 10, §2º**).

A partir dessa estrutura, é possível **integrar a leitura dos artigos Art. 10 e Art. 11**, especialmente quando o **legítimo interesse atua como reforço ou justificativa de finalidade legítima em hipóteses previstas no art. 11**, como:

- **Prevenção à fraude e segurança (art. 11, II, g);**
- **Exercício regular de direitos (art. 11, II, d);**
- **Cumprimento contratual e legítima expectativa do titular (art. 10, II + art. 11, II, d).**

Embora o legítimo interesse não se aplique de forma autônoma ao tratamento de dados sensíveis, ele pode ser invocado como elemento complementar de interpretação para justificar a necessidade, a proporcionalidade e a finalidade legítima do tratamento, desde que amparado por uma das hipóteses do art. 11 da LGPD.

Ele exige o alinhamento entre a proteção de dados e as finalidades operacionais legítimas do controlador, sobretudo em contextos onde a segurança da informação, a prevenção de fraudes e a identificação/autenticação segura do titular sejam indispensáveis para o funcionamento de sistemas eletrônicos e serviços digitais.

Portanto, o tratamento de dados sensíveis deve sempre observar a base legal prevista no art. 11, mas a análise da situação concreta pode ser enriquecida pela ponderação dos princípios da boa-fé, da finalidade, da necessidade e da transparência, conforme reforçado pelo art. 6º da LGPD. Nessa perspectiva, o legítimo interesse atua como fundamento interpretativo que auxilia na demonstração da adequação e da justificativa do tratamento, especialmente em situações de risco mitigável, reforçando a proteção dos direitos dos titulares

2. NOTA TÉCNICA Nº 175/2023/CGF/ANPD – RECONHECIMENTO DE FUNDAMENTO PRÓPRIO PELAS EPDS - MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP) - CONFEDERAÇÃO BRASILEIRA DE FUTEBOL (CBF).

A **Nota Técnica nº 175/2023/CGF/ANPD** admite expressamente que **Entidades de Prática Desportiva (EPDs)** realizem o tratamento de dados sensíveis com **fundamento próprio**, desde que:

- Reconhece que entidades podem realizar tratamento de dados sensíveis mediante fundamento próprio, desde que cumpram requisitos rigorosos de governança, transparência e proteção, incluindo elaboração do **RIPD (Relatório de Impacto à Proteção de Dados)**, **transparência**, **encarregado designado e ferramentas para exercício de direitos**;
- Abre espaço para entendimento mais flexível da base legal, desde que fundamentado em finalidades legítimas e estruturado em conformidade com a LGPD.
- O tratamento se dê com finalidade clara e legítima.

Essa Nota **não exclui** a possibilidade de o legítimo interesse ser **parte da estrutura de fundamentação**, desde que os requisitos formais da LGPD e do Guia da ANPD sejam atendidos.

Alternativamente, é possível que a coleta desses dados (inclusive os sensíveis) pelas Entidades de Prática Desportiva se dê com fundamento próprio (**finalidade e hipótese legal próprias**). É essencial que o MJSP só permita a adesão de EPD que, no mínimo: i) já houver preparado o RIPD (necessariamente abordando os mesmos riscos abordados no RIPD apresentado) e o Registro das Operações de Tratamento; ii) que já tenha encarregado designado; iii) disponha de ferramenta para exercício de direitos do titular; e iv) tenha disponibilizado informações sobre coleta e tratamento nos termos do art. 9º em lugar de franco e fácil acesso. - **175/2023/CGF/ANPD**

A Nota Técnica nº 175/2023/CGF/ANPD representa um avanço significativo na interpretação e aplicação da LGPD, ao reconhecer a possibilidade de as Entidades de Prática Desportiva (EPDs) operarem com maior autonomia jurídica, desde que respeitados os parâmetros legais e técnicos estabelecidos pela legislação e pela própria ANPD.

Esse reconhecimento reforça a necessidade de que o tratamento de dados — especialmente sensíveis — esteja sempre embasado em uma estrutura de governança robusta, com mecanismos claros de responsabilização, prestação de contas e garantia dos direitos dos titulares. A adoção de medidas como a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), a designação formal de encarregado, a

implementação de canais efetivos para o exercício de direitos e a comunicação transparente com os titulares são elementos indispensáveis para validar esse fundamento próprio.

Além disso, o entendimento da ANPD permite que, em determinados contextos, o legítimo interesse atue como elemento complementar de análise, desde que não se sobreponha às hipóteses taxativas do art. 11 da LGPD e que sua utilização esteja devidamente justificada e documentada, conforme as diretrizes do Guia de Bases Legais da ANPD.

Portanto, a admissibilidade de um fundamento próprio para o tratamento de dados sensíveis por parte das EPDs não implica em flexibilização dos direitos dos titulares, mas sim em uma adaptação responsável e contextualizada da LGPD à realidade específica, sempre condicionada ao cumprimento rigoroso dos princípios da lei e ao compromisso com a proteção dos dados pessoais.

3. ARTIGO 29 – GRUPO DE TRABALHO EUROPEU DE PROTEÇÃO DE DADOS (REFERÊNCIA INTERNACIONAL) 844/14/PT WP 217

O **Artigo 29 Working**, referência da União Europeia (cuja GDPR inspirou a LGPD), afirma que:

“O tratamento pode se basear em interesses legítimos do controlador, desde que haja ponderação com os direitos e liberdades do titular”.

E ainda:

- Estabelece que o legítimo interesse deve ser ponderado e avaliado frente aos direitos do titular, sendo um critério válido para justificar o tratamento de dados, desde que haja necessidade, proporcionalidade e inexistam meios menos invasivos.
- Suporta a interpretação de que o legítimo interesse pode atuar como base complementar ou elemento justificatório em tratamentos que envolvam dados sensíveis.

“O tratamento de dados deve ser necessário e proporcional, considerando se existem meios menos invasivos.”

Isso valida o uso do legítimo interesse como critério de ponderação e equilíbrio, inclusive quando combinado com bases legais mais restritivas, como é o caso do tratamento de dados sensíveis para segurança, antifraude e exercício de direitos.

O **Parecer 06/2014 do Grupo de Trabalho do Artigo 29 (WP217)** contribui de maneira significativa para o entendimento de como o legítimo interesse pode ser operacionalizado no tratamento de dados pessoais, inclusive em cenários mais complexos, como aqueles que envolvem dados sensíveis. Embora a GDPR — assim como a LGPD — imponha limites claros ao tratamento desses dados, o documento reconhece que o

legítimo interesse pode atuar como elemento de reforço argumentativo, desde que amparado por uma base legal principal prevista na legislação e submetido a uma rigorosa análise de impacto e proporcionalidade.

Nesse sentido, o parecer europeu reforça a ideia de que a simples invocação do legítimo interesse não basta. É indispensável que o controlador demonstre, de forma documentada, que:

- A finalidade do tratamento é legítima e claramente definida;
- O tratamento é necessário para alcançar tal finalidade;
- Não existem alternativas menos intrusivas que ofereçam o mesmo resultado;
- Os direitos, liberdades e garantias do titular foram devidamente ponderados e resguardados;
- Medidas técnicas e organizacionais foram implementadas para mitigar riscos e assegurar a transparência.

Portanto, o legítimo interesse pode ser considerado uma ferramenta jurídica relevante no contexto da proteção de dados, desde que interpretado com cautela e utilizado de forma subsidiária, respeitando os princípios fundamentais da proteção à privacidade. No caso da LGPD, essa referência internacional reforça a necessidade de avaliações de impacto, registros de tratamento e políticas de governança bem estruturadas para que o uso do legítimo interesse, ainda que complementar, seja legítimo, seguro e conforme o direito fundamental à proteção de dados.

4. GUIA DE LEGÍTIMO INTERESSE – ANPD

O Guia da ANPD destaca que:

“O teste de balanceamento do legítimo interesse **também se aplica à hipótese legal prevista no art. 11, II, g da LGPD**”.

E complementa:

- Aponta que o teste de balanceamento do legítimo interesse também se aplica ao art. 11, II, “g”, da LGPD.
- Destaca que o interesse legítimo deve estar baseado em situações concretas e reais, com finalidades claras, específicas e compatíveis com as expectativas do titular.

“O interesse deve ter **lastro em situações reais e concretas**, com objetivo legítimo, específico e alinhado às expectativas do titular”.

Isso significa que, embora o **legítimo interesse não seja uma base legal direta para dados sensíveis, pode ser usado como suporte normativo** para demonstrar: **Finalidade legítima do tratamento; Necessidade da operação de dados; Não violação de direitos fundamentais do titular; Justificativa ética e técnica da escolha da base do art. 11.**

O Guia da ANPD deixa claro que o legítimo interesse, embora não configure base legal autônoma para o tratamento de dados sensíveis, pode ser utilizado como elemento auxiliar no processo de análise e justificativa do tratamento com fundamento no art. 11, II, “g” da LGPD — especialmente em contextos como prevenção à fraude, segurança da informação e autenticação do titular.

Nesse contexto, o teste de balanceamento passa a desempenhar papel fundamental na validação da escolha pela hipótese legal do art. 11. Trata-se de um exercício de ponderação (equilíbrio) que exige do controlador uma avaliação estruturada, baseada em três eixos principais:

1. **Finalidade legítima:** o tratamento deve estar vinculado a uma necessidade real e justificada, que respeite os princípios da finalidade e da adequação;
2. **Necessidade:** a operação deve ser imprescindível para alcançar a finalidade proposta, sem que existam alternativas menos invasivas;
3. **Equilíbrio:** os direitos e liberdades do titular não podem ser sobrepostos ou prejudicados de forma desproporcional, devendo haver medidas de mitigação de riscos e salvaguardas adequadas.

Dessa forma, o legítimo interesse atua como uma ferramenta de **reforço argumentativo** e de conformidade, permitindo que o controlador demonstre de forma transparente, ética e técnica que o tratamento é legítimo, proporcional e alinhado às expectativas razoáveis dos titulares de dados. Essa abordagem fortalece a segurança jurídica da operação de tratamento e contribui para uma cultura de responsabilidade e respeito à proteção de dados pessoais.

5. CARTILHA SOBRE FINALIDADE E HIPÓTESES LEGAIS 2023 – Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos

A aplicação desta hipótese ao tratamento de dados pessoais sensíveis (artigo 11) não está prevista na LGPD. Para a adoção desta hipótese deve-se realizar uma avaliação de legítimo interesse - LIA (Legitimate Interests Assessment). Deve ser demonstrada a proporcionalidade entre os interesses do controlador e os direitos e expectativas do titular.

Caso o tratamento de dados pessoais baseado nesta hipótese descumpra a LGPD, o titular poderá se opor.

6. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 2020

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados. Pg 24

A **Lei Geral de Proteção de Dados (LGPD)** exige que todo tratamento de dados pessoais siga a **boa-fé** e **10 princípios fundamentais**. Esses princípios são **obrigatórios, independem da base legal escolhida**, e visam garantir o respeito aos direitos dos titulares. Segui-los evita riscos legais, reputacionais e operacionais.

Seguir os princípios da LGPD **não é opcional**. Mesmo que a empresa tenha uma base legal válida (como consentimento ou interesse legítimo), **deve sempre observar os princípios**, ou o tratamento será considerado irregular

- | | |
|------------------------|---|
| 1. Finalidade | 6. Transparência |
| 2. Adequação | 7. Segurança |
| 3. Necessidade | 8. Prevenção |
| 4. Livre acesso | 9. Não discriminação |
| 5. Qualidade dos dados | 10. Responsabilização e prestação de contas |

Cumprir uma base legal (como o legítimo interesse) não é suficiente. É obrigatório **respeitar todos os princípios** da LGPD para o tratamento ser considerado legítimo.

Mesmo quando o tratamento se baseia no **legítimo interesse**, ele **só é válido se todos os princípios da LGPD forem respeitados**. Ou seja, **não basta ter uma justificativa**, é preciso **agir com transparência, responsabilidade e segurança**.

A LGPD não autoriza explicitamente o uso de "legítimo interesse" para tratamento de dados sensíveis (art. 11). Portanto, está justificativa deve ser usada com cautela e acompanhada de avaliação de risco, Relatório de Impacto à Proteção de Dados (RIPD) e, preferencialmente, parecer jurídico.

Apesar de o legítimo interesse não constar entre as bases legais previstas para dados sensíveis no art. 11, entende-se que, em situações concretas onde o tratamento biométrico seja essencial para garantir a segurança e prevenir fraudes, o legítimo interesse pode ser usado de forma análoga, com base no:

- Art. 10 da LGPD: que permite tratamento com base em legítimo interesse, desde que a finalidade seja legítima, concreta e observados os direitos e liberdades fundamentais do titular;
- Art. 11, II, "g": que permite tratamento de dados sensíveis para prevenção à fraude e segurança do titular, o que possui afinidade funcional com o legítimo interesse
- Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Legítimo interesse com reforço no art. 37 e 11, II, "g" (segurança do titular)

“Cumpre destacar que os exemplos de finalidades apresentados na LGPD não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.”

7. INTERESSE DA CRIANÇA – COMITÊ DOS DIREITOS DA CRIANÇA, COMENTÁRIO GERAL Nº 14 (2013)

A avaliação do **interesse da criança** deve ser feita **caso a caso**, considerando as **características individuais** (como idade, maturidade, deficiência, cultura, etc.) e o **contexto familiar e social** da criança.

Esse processo envolve:

- A escuta e consideração das **opiniões da criança**;
- A proteção da **identidade, saúde, educação e segurança**;
- A preservação de **relações familiares**, sempre que possível;
- A atenção à **vulnerabilidade específica** da criança.

*Em situações em que esses elementos **entram em conflito** (ex.: manter vínculo familiar vs. risco de abuso), deve-se fazer uma **ponderação cuidadosa** para alcançar a **solução que melhor atenda aos interesses da criança**.*

👤 A avaliação do melhor interesse **não é fixa**, devendo ser adaptada ao contexto e às necessidades específicas de cada criança ou grupo de crianças.

Tratar dados pessoais de crianças, com o uso do **legítimo interesse** pode ser **justificado** desde que:

- O tratamento **respeite e priorize o interesse superior da criança**;
- Haja **avaliação individualizada do contexto e das necessidades da criança**;
- O tratamento busque finalidades como **educação, proteção e segurança**.

Logo, o L.I exige que sejam aplicadas salvaguardas reforçadas, como a limitação da finalidade, minimização dos dados, transparência e controle parental, quando aplicável;

O tratamento seja claramente necessário, proporcional e não represente risco significativo aos direitos e liberdades da criança.

Nessa perspectiva, o legítimo interesse só poderá ser considerado em situações excepcionais e com base em uma análise profunda de impacto, sempre subordinado à primazia do **interesse da criança**, conforme orienta o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU.

Além disso, é essencial que o controlador demonstre, de forma documentada, que o tratamento:

- Não expõe a criança a riscos desnecessários ou indevidos;

- Está alinhado com as expectativas razoáveis de proteção e cuidado próprias da infância;
- Foi precedido de mecanismos adequados de consulta, consentimento ou informação aos responsáveis legais, quando exigido.

Portanto, o uso do legítimo interesse no tratamento de dados pessoais de crianças deve ser cuidadosamente fundamentado, sempre pautado pela ética, legalidade e pelas diretrizes internacionais de proteção integral à criança. O foco deve estar não na conveniência do controlador, mas na efetiva proteção e promoção dos direitos da criança em seu contexto individual e social.

CONCLUSÃO:

A análise combinada da legislação brasileira, das orientações da ANPD e das referências internacionais permite concluir que:

É juridicamente defensável, sob uma **interpretação sistemática e finalística da LGPD**, com base nos **princípios de necessidade, adequação, transparência e responsabilidade**, que o **legítimo interesse do controlador** funcione como **fundamento auxiliar** no tratamento de **dados sensíveis**.

O tratamento de dados pessoais sensíveis com base exclusiva no legítimo interesse **não é admitido** pela LGPD, todavia, o **legítimo interesse pode ser utilizado como fundamento auxiliar e complementar**, especialmente nas hipóteses expressas do art. 11 (como prevenção à fraude e segurança, exercício regular de direitos, proteção da vida), desde que cumpridos os requisitos de:

1. A base legal principal esteja prevista no **art. 11 da LGPD** (como exercício regular de direitos, proteção à vida, prevenção à fraude etc.);
2. O tratamento seja **estritamente necessário e proporcional**;
3. Seja realizado um **teste de balanceamento de interesses** do controlador e os direitos do titular.;
4. Haja **RIPD e mecanismos de transparência** adequados;
5. O **titular seja beneficiado direta ou indiretamente** com a operação de tratamento;
6. Não haja violação de direitos fundamentais nem abuso de finalidade.
7. Necessidade e proporcionalidade;
8. Transparência e responsabilização;
9. Garantia dos direitos dos titulares;

Aplicações Práticas:

- Controle de acesso por biometria em hospitais, academias e outras;
- Monitoramento antifraude em sistemas eletrônicos de atletas e pacientes;
- Compartilhamento de dados clínicos para defesa judicial ou contratual;
- Acompanhamento de performance esportiva com dados de saúde: plano de treino;
 - ✓ Condição médica de atletas;
 - ✓ Dados de performance física;

- Proteger a integridade física e segurança;
- Cumprir exigências regulatórias da Anvisa;
- Pacientes voluntários em cooperação científica - Contrato;
 - ✓ Dados genéticos, biométricos e de saúde;
 - ✓ Informações psicossociais;
 - ✓ Histórico de doenças crônicas;
- Dados de saúde de pacientes atendidos (diagnóstico, CID, procedimentos);
- Informações de reembolso e cobertura;
- Exames médicos compartilhados para auditoria;
- Exames admissionais (aptidão, vacinação, doenças pré-existentes) Art. 11, II, “a”;
- Laudos ocupacionais Art. 11, II, “a”;
- Registro ou atendimento de PCD, se aplicável;
- Dados sobre uso de medicamentos controlados;
- Registro eletrônico de acesso ao prontuário (log de acessos por profissionais autorizados);
- Registros de ponto.

Essas aplicações demonstram que, embora o **legítimo interesse não possa fundamentar isoladamente** o tratamento de dados sensíveis, ele desempenha papel relevante **como elemento integrador de uma base legal válida**, reforçando a análise de proporcionalidade, finalidade legítima e alinhamento com as expectativas do titular.

A sua utilização deve ser sempre acompanhada de **medidas técnicas e administrativas eficazes**, como:

- Elaboração de **Relatórios de Impacto à Proteção de Dados (RIPD)** que analisem os riscos e benefícios do tratamento;
- Implementação de políticas de **governança e segurança da informação**;
- Estabelecimento de **canais acessíveis para o exercício dos direitos dos titulares**;
- Garantia de **transparência ativa**, inclusive mediante a disponibilização de informações claras nos termos do art. 9º e art. 18º da LGPD;
- Nomeação de **encarregado pelo tratamento de dados (DPO)**, com capacitação adequada.

Além disso, o tratamento deve ser periodicamente reavaliado à luz dos princípios do art. 6º da LGPD — especialmente os da **finalidade, necessidade, não discriminação e responsabilização** — assegurando que os dados sejam utilizados de forma ética, proporcional e respeitosa aos direitos fundamentais.

Portanto, o legítimo interesse, **quando usado de forma subsidiária e responsável**, pode ser compatibilizado com o tratamento de dados sensíveis, desde que atenda a todos os critérios legais e seja orientado pela máxima proteção ao titular, especialmente em contextos de vulnerabilidade, como saúde, infância, deficiência ou exposição a riscos. Essa abordagem promove segurança jurídica, efetividade no tratamento e respeito à dignidade da pessoa humana — fundamento maior da LGPD.

A análise integrada da LGPD, das orientações da ANPD, dos referenciais internacionais e dos princípios constitucionais aplicáveis evidencia que o **legítimo interesse do controlador pode atuar como fundamento jurídico complementar**, especialmente no tratamento de **dados sensíveis**.

A **Lei Geral de Proteção de Dados (LGPD)** veda o uso do legítimo interesse como **base legal autônoma para dados sensíveis**, conforme o art. 11, mas permite sua **utilização como suporte** em hipóteses expressamente previstas, como a prevenção à fraude, a segurança do titular, o exercício regular de direitos e a proteção da vida. Essa compatibilização está amparada pelos princípios da **necessidade, adequação, proporcionalidade, responsabilidade e transparência** (art. 6º), e encontra eco nas diretrizes da ANPD e em referências internacionais.

O **Guia de Legítimo Interesse da ANPD** reforça que o **teste de balanceamento** deve ser aplicado inclusive no contexto do art. 11, II, “g”, exigindo que o tratamento tenha base em finalidades legítimas, específicas e alinhadas às **expectativas do titular**, com **salvaguardas efetivas**, como Relatório de Impacto (RIPD), mecanismos de transparência e controle.

O **Artigo 29 Working (WP 217)** sustenta que o legítimo interesse pode ser **ponderado com os direitos do titular**, inclusive em cenários que envolvam dados sensíveis, desde que não existam meios menos invasivos e o tratamento seja necessário para atingir uma finalidade legítima e concreta. Essa perspectiva reforça uma **interpretação da LGPD**, permitindo o uso responsável do legítimo interesse como elemento de **justificação ética, técnica e jurídica**.

Em contextos de maior vulnerabilidade, como o tratamento de **dados pessoais de crianças**, aplica-se o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que estabelece o **interesse da criança como critério máximo de decisão**. Nesses casos, o legítimo interesse só poderá ser considerado se compatível com o melhor interesse da criança, com **análise individualizada** e **proteções reforçadas**, incluindo a escuta da criança, a transparência e a mitigação de riscos.

A **Nota Técnica nº 175/2023/CGF/ANPD** também valida a possibilidade de **fundamento próprio para entidades específicas**, desde que cumpridos rigorosamente os requisitos da LGPD, como RIPD, designação de encarregado, registro das operações e disponibilização clara de informações ao titular, não se afastando da exigência de proporcionalidade, necessidade e respeito aos direitos fundamentais.

Portanto, conclui-se que o **legítimo interesse**, embora não seja base legal autônoma para dados sensíveis, **pode e deve ser considerado como instrumento jurídico complementar e legítimo**, desde que:

1. Haja **base legal principal válida no art. 11 da LGPD**;
2. **Teste de balanceamento** com documentação clara dos riscos e medidas mitigadoras;
3. O tratamento seja **necessário, proporcional e transparente**;
4. Os direitos e a dignidade do titular sejam plenamente **respeitados**;
5. O tratamento resulte em **benefício direto ou indireto** para o titular;
6. Haja estrutura robusta de **governança, responsabilização e prestação de contas**.

Essa abordagem promove segurança jurídica, viabiliza operações essenciais em setores como **saúde, educação, Religião, segurança, esporte e pesquisa**, e fortalece a cultura de **proteção de dados pessoais como direito fundamental** no Brasil.

APLICABILIDADE (PASSO A PASSO)

1. Identificar uma base legal principal válida no art. 11 (ex.: exercício regular de direitos, prevenção à fraude, proteção da vida);
2. Demonstrar a necessidade e proporcionalidade da operação;
3. Aplicar e documentar o Teste de Balanceamento (controlador x titular);
4. Elaborar o Relatório de Impacto à Proteção de Dados (RIPD);
5. Garantir mecanismos adequados de transparência e comunicação;
6. Nomear encarregado (DPO) e estruturar governança de dados;
7. Comprovar que o tratamento traz benefício direto ou indireto ao titular;
8. Implementar salvaguardas para crianças, idosos e pessoas com deficiência, quando aplicável.

Sobre o tratamento de dados pessoais **DANILO DONEDA, diz:**

[...] **a mera proibição da coleta e** tratamento de dados sensíveis recurso utilizado em algumas das leis sobre a matéria demonstra-se inviável, pois muitas vezes o uso de tais dados é legítimo e necessário além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações deste gênero, como diversas entidades de pesquisa ou do setor de saúde, caráter político, religioso ou filosófico.

Segundo a ANPD, o legítimo interesse:

Interesse será considerado legítimo quando atender a três condições: (i) compatibilidade com o ordenamento jurídico; (ii) lastro em situações concretas; e (iii) vinculação a finalidades legítimas, específicas e explícitas. ANPD. HIPÓTESES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS LEGÍTIMO INTERESSE. p.16

Ainda diz:

Cumpram-se destacar que os exemplos de finalidades não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados. ANPD. HIPÓTESES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS LEGÍTIMO INTERESSE. p.37

TESTE DE BALANCEAMENTO

VANTAGENS BIOMETRIA			
Critério	Reconhecimento Facial	Impressão Digital	Código de Entrada - Senha / Código de Acesso / Token
Segurança	Alta (mas vulnerável a fotos/3D bem feitos)	Alta (biometria é única e difícil de falsificar)	Média (pode ser adivinhado, compartilhamento ou vazado)
Conveniência	Muito alta (mãos livres)	Alta (rápido, mas exige contato)	Média (exige digitação)
Velocidade de Acesso	Muito rápida	Rápida	Moderada (digitação leva mais tempo)
Custo de Implementação	Alto (câmeras + software avançado)	Médio (leitor biométrico)	Baixo (teclado ou app)
Privacidade	Sensível (dados faciais)	Sensível (biometria digital)	Alta (sem biometria, mais fácil de auditar)
Condições de Uso	Pode falhar com baixa luz, máscara, óculos	Pode falhar com dedo sujo/molhado/Cortes ou luvas	Pode ser usado sempre
Risco de Falsificação	Moderado (deepfakes, fotos 3D)	Baixo (dificuldade técnica - "requer presença física)	Alto (reutilização, engenharia social, compartilhada)
Manutenção e Suporte	Alta (ajustes em software e câmeras)	Média (limpeza e calibração)	Baixa (pouca manutenção)
Acessibilidade	Pode não funcionar com todos os rostos	Pode falhar com cicatrizes ou ausência	Totalmente acessível
Indicação Ideal	Ambientes de alto controle e conveniência	Acesso rápido e seguro	Ambientes simples e de baixo risco
Gerenciamento de Acesso	Alto controle via logs e integração de IA	Alto, com registros por usuário	Médio, logs mais simples e passíveis de uso indevido
Melhor uso corporativo	Acesso sem toque a áreas de alta segurança	Entrada em áreas restritas	Acesso a áreas comuns ou temporárias
Higiene	Excelente (Evita toque, mantém esterilidade - sem contato físico - ideal com EPIs)	Ruim (necessita contato — risco de contaminação)	Boa (mínimo contato com superfícies)
Funcionamento com EPIs	Pode falhar com máscaras, toucas, óculos	Frequentemente inutilizado com luvas	Funciona com EPIs
Custo de Implementação	Alto (câmeras, IA, integração)	Médio (leitores confiáveis)	Baixo (teclados e software simples)
Privacidade / LGPD	Sensível (reconhecimento facial = biometria)	Sensível (biometria digital)	Mais simples de gerenciar (sem biometria)
Acessibilidade	Pode não funcionar para todos (ex: deformidades)	Pode falhar com problemas físicos	Universal
Classificação LGPD	Dado pessoal sensível	Dado pessoal sensível	Dado pessoal comum (quando não vinculado ao nome diretamente)
Necessidade de Consentimento - LGPD	Sim ou Base legal específica como segurança	Sim ou Base legal específica como segurança	Pode ser dispensado se uso for legítimo e impessoal
Risco Legal (em caso de vazamento) - LGPD	Alto (imagem facial é sensível)	Alto (digital é irreversível)	Médio a baixo (senha pode ser trocada)
Conformidade com LGPD	Requer políticas, registro de tratamento e proteção rígida	Requer políticas, registro de tratamento e proteção rígida	Mais simples de adequar à LGPD
Segurança Técnica - LGPD	Alta (com liveness detection)	Alta	Média (PIN pode ser compartilhado)
Facilidade de Revogação - LGPD	Baixa (não se pode "trocar" o rosto)	Baixa (não se pode "trocar" a digital)	Alta (senha pode ser alterada facilmente)

IMPACTO BIOMETRIA			
Aspecto	Descrição	Avaliação / Impacto	Justificativa e Considerações
Interesse do Controlador - LGPD	Garantir a segurança física e patrimonial no ambiente	Alto	Segurança do hospital e proteção de pacientes, colaboradores e visitantes é fundamental - Mais higiênico em ambiente hospitalar
Direitos e Liberdades do Titular - LGPD	Proteção da privacidade e dados pessoais sensíveis	Alto	Dados biométricos são sensíveis e demandam cuidados rigorosos na coleta, armazenamento e uso
Finalidade Específica e Transparente - LGPD	Dados coletados apenas para controle de acesso e segurança	Essencial	Transparência e comunicação clara para titulares são obrigatórias
Minimização de Dados	Coleta limitada ao necessário para atingir o objetivo	Adequada	Apenas dados faciais biométricos, sem coleta de dados adicionais irrelevantes
Segurança Técnica	Proteção dos dados contra acessos não autorizados, vazamentos	Rigorosa	Uso de criptografia, autenticação forte, monitoramento e auditorias regulares
Segurança Organizacional	Políticas internas, treinamentos e controles de acesso	Rigorosa	Garantia de uso ético e responsável da tecnologia
Avaliação de Riscos	Identificação e mitigação de riscos à privacidade e segurança	Obrigatória	DPIA (Análise de Impacto à Proteção de Dados) recomendada para mapear riscos e definir controles
Direitos do Titular	Garantia de acesso, correção, exclusão e revogação do consentimento	Fundamental	Procedimentos claros para atendimento a solicitações dos titulares
Alternativas para Titulares	Disponibilização de outros métodos para quem não deseja biometria	Necessário	Alternativas como senha, cartão ou outros métodos de autenticação devem ser oferecidas

Proporcionalidade e Necessidade	Uso da biometria é proporcional ao objetivo e imprescindível para segurança	Deve ser justificado	Justificar que métodos tradicionais não oferecem o mesmo nível de segurança ou praticidade
Transparência e Comunicação	Informação clara e acessível sobre o tratamento de dados	Obrigatória	Política de privacidade atualizada e canais de comunicação eficientes
Retenção e Exclusão de Dados	Tempo limitado para armazenamento e procedimentos para exclusão	Essencial	Dados mantidos pelo tempo necessário e removidos ao término da necessidade ou pedido do titular - Usar Picotadora
Impacto em Caso de Violação	Consequências para titulares em eventual vazamento ou uso indevido	Elevado	Dados biométricos comprometidos podem causar danos graves à privacidade e segurança pessoal / Possível exposição e discriminação se dados vazarem
Conformidade Legal e Regulamentar	Atendimento às disposições da LGPD e demais normas aplicáveis	Obrigatório	Auditorias periódicas e revisões para garantir conformidade contínua
Natureza dos Dados	Tipo de dado tratado (biometria facial, considerado sensível)	Sensível	Biometria tem alto risco se vazada ou mal utilizada
Riscos Potenciais	Vazamento, uso indevido, discriminação, falhas técnicas	Moderado a Alto	Risco elevado devido à sensibilidade do dado
Medidas Mitigadoras	Procedimentos para minimizar riscos	Implementadas	Controles técnicos e organizacionais robustos
Alternativas Disponíveis	Opções para titulares que não desejam usar biometria	Sim	Senha, cartão, reconhecimento manual
Necessidade e Proporcionalidade	Uso da biometria é necessário e proporcional ao fim	Adequada	Tecnologia justificada pela criticidade da segurança hospitalar

ITEM	VANTAGEM
Segurança Reforçada	Reduz fraudes de identidade (não pode ser facilmente replicado como crachás ou senhas).
	Controla rigorosamente o acesso a áreas restritas e sensíveis.
	Permite auditoria e rastreamento de acessos com precisão.
	Pode ser combinado com alertas em tempo real (ex: tentativa de acesso por pessoa não autorizada).
Eficiência Operacional	Automatiza processos de identificação e autenticação.
	Aumenta a velocidade do controle de entrada/saída (sem contato físico).
	Reduz filas e necessidade de pessoal para checagem manual.
	Evita a necessidade de portar crachá, senha ou chave física.
Experiência do Usuário	Facilita o acesso de forma fluida e rápida.
	Gera menos atrito no dia a dia de colaboradores e visitantes.
	Elimina o contato físico com superfícies (comparado a digitais, cartões ou teclados).
	Ideal para ambientes sensíveis como hospitais, laboratórios e cozinhas industriais.
Monitoramento e Análise Inteligente	Permite integração com sistemas de vigilância, registro de ponto e BI (business intelligence).
	Gera relatórios de acesso, horários de entrada e saída, e padrões de comportamento.
	Possibilita cruzamento com outras bases (ex: listas de bloqueio, visitantes agendados).
	Diminui despesas com reposição de crachás, senhas e chaves.
Redução de Custos a Longo Prazo	Reduz necessidade de vigilância humana constante.
	Menor custo com fraudes ou acessos indevidos.
	Facilita a rastreabilidade de eventos e pessoas (quem entrou, quando e onde).
	Ajuda no cumprimento de normas regulatórias (ex: segurança do trabalho, ANVISA, LGPD com cuidados).
Conformidade e Auditoria	Suporta políticas de segurança corporativa com mais precisão.
	Pode ser combinado com sistemas de IA, machine learning e reconhecimento de comportamento.
	Integrável a CRMs, sistemas de RH, catracas eletrônicas e ERPs.
	Controla acesso a salas limpas, UTI, centros cirúrgicos, laboratórios.
Aplicações específicas para saúde	Restringe entrada de terceiros a ambientes de risco biológico.
	Garante que apenas profissionais autorizados tenham acesso a medicamentos controlados.

Base - Legítimo Interesse	
Critério	Descrição / Avaliação
Finalidade do tratamento	Controle de acesso seguro a áreas restritas do hospital (ex: UTI, farmácia, almoxarifado, centro cirúrgico, restaurante) com o objetivo de proteger pacientes, profissionais e visitantes.
	O objetivo é específico para o tratamento dos dados.
Tipo de dado tratado	Dado pessoal sensível – biometria facial (Art. 5º, II da LGPD).
Base legal	Legítimo Interesse do controlador (Art. 7º, IX da LGPD) e exceção para dados sensíveis (Art. 11, II, “f”).
Interesse legítimo do controlador	Garantir a segurança física de pacientes, profissionais e instalações hospitalares. Prevenir acessos não autorizados.
	Existe relação prévia e direta com os titulares (funcionários, pacientes, prestadores, etc.)
	O tratamento garante a prevenção à fraude e à segurança do titular,
Necessidade do tratamento	O reconhecimento facial é mais seguro, higiênico (sem toque) e menos sujeito a fraudes do que senhas ou crachás.
	Profissionais, pacientes e terceiros compreendem que o hospital deve garantir um ambiente seguro.

Alternativas menos invasivas?	Sim (senhas, cartões), mas menos eficazes e mais suscetíveis a compartilhamento ou perda. O método biométrico é mais robusto.
Expectativa do titular	Alta: em hospitais, espera-se controle rígido de acesso. A visibilidade do sistema e avisos reforçam essa expectativa.
Proporcionalidade	O tratamento é proporcional à finalidade não sendo reutilizado para outras finalidade. Apenas dados necessários são tratados. O uso é restrito ao controle de acesso.
Riscos à privacidade	Vazamento, uso indevido, acesso não autorizado, ausência de controle sobre retenção e descarte.
Medidas de mitigação adotadas	- Criptografia dos dados
	- Acesso restrito
	- Registros de auditoria
	- Prazos claros de retenção e descarte
	- Alternativa para quem não aceitar biometria
Transparência com o titular	Política de privacidade acessível; avisos de uso; canal de atendimento para dúvidas e direitos.
Benefício para o Controlador	Prevenção de acessos não autorizados, redução de fraudes.
	Ambiente hospitalar mais seguro.
Conclusão do balanceamento	O tratamento é legítimo, necessário e proporcional. Os direitos dos titulares são respeitados e protegidos com medidas adequadas de segurança e transparência. / Ágil (evita filas e atrasos no atendimento); / Seguro (menos suscetível a fraudes do que cartões ou senhas); / Higiénico (sem contato físico, essencial em ambiente hospitalar). / Alternativas como crachás e senhas apresentam riscos maiores de uso indevido, perda ou compartilhamento indevido.

REFERÊNCIA

BRASIL. Resolução CD/ANPD Nº 2 de janeiro de 2022, que Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial: Edição Nº 20 de 28/01/2022 - Pág. 6, Documento eletrônico. Disponível em < [**BRASIL Lei 8.069 – ECA** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências <\[**BRASIL. Lei 13.709 –** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 \\(Marco Civil da Internet\\). Diário Oficial da União: Seção 1, Brasília, DF, 15 de agosto de 2018. Documento eletrônico. Disponível em \\[http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm\\]\\(http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm\\) Acesso em 05 jun. 2025\]\(https://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=Art.%203%C2%BA%20crian%C3%A7a%20e,f%C3%ADsico%2C%20mental%2C%20moral%2C%20esp%C3%ADritual> Acesso em 05 jun. 2025</p>
</div>
<div data-bbox=\)](https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022#:~:text=Aprova%20o%20Regulamento%20de%20Comunica%C3%A7%C3%A3o%20de%20Incidente%20de%20Seguran%C3%A7a.&text=Aprova%20o%20Regulamento%20de%20aplica%C3%A7%C3%A3o,de%20tratamento%20de%20pequeno%20porte.> Acesso em 05 jun. 2025</p>
</div>
<div data-bbox=)

Declaração Universal dos Direitos Humanos. Disponível em <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>> Acesso em 18 mai 2023

DONEDA, Danilo. **A Proteção dos Dados Pessoais Como um Direito Fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Tratamento de dados pessoais pelo poder público. Brasília: anpd, versão 1.0., jan. 2022. Disponível em: < https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em 05 jun. 2025

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo Hipóteses legais de tratamento de dados pessoais legítimo interesse. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf Acesso em 05 jun. 2025

MATTIUZZO, Marcela; PONCE, Pula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. Em Revista InternetLab. Volume 1, nº 2, 2020.

GABRIADES de Souza, Felipe, MESTRADO PROFISSIONAL - O Uso do Legítimo Interesse como Ferramenta de Avaliação de Risco na Atividade de Tratamento de Dados Pessoais - Versão de 01.07.2022 < [instagram.com/reel/DBmQh8hpopT/?igsh=ZzgxbXA0cDZmYW52](https://www.instagram.com/reel/DBmQh8hpopT/?igsh=ZzgxbXA0cDZmYW52)> Acesso em 05 jun. 2025

Article 29 Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf Acesso em 05 jun. 2025

BRASIL. **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)**. Minuta - Guia Orientativo Tratamento de Dados Pessoais de Alto Risco. <https://www.gov.br/participamaisbrasil/blob/baixar/48651> Acesso em 05 jun. 2025