UNIVERSIDADE FEDERAL DE OURO PRETO

Escola de Direito, Turismo e Museologia

Departamento de Direito

Clara Fernandes Albuquerque Fadel

CONSENTIMENTO, BASES LEGAIS E TRATAMENTO DE DADOS DE SAÚDE NO SETOR PRIVADO: ESTUDO COMPARADO ENTRE O ART. 11 DA LGPD E O ART. 9 DO GDPR

Ouro Preto

2025

Clara Fernandes Albuquerque Fadel

Consentimento, Bases Legais e Tratamento de Dados de Saúde no Setor Privado: Estudo Comparado entre o Art. 11 da LGPD e o Art. 9 do GDPR

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientadora: Juliana Almeida Evangelista

Ouro Preto
2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Clara Fernandes Albuquerque Fadel

CONSENTIMENTO, BASES LEGAIS E TRATAMENTO DE DADOS DE SAÚDE NO SETOR PRIVADO: ESTUDO COMPARADO ENTRE O ART. 11 DA LGPD E O ART. 9 DO GDPR

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 03 de setembro de 2025

Membros da banca

Doutora - Juliana Evangelista de Almeida - Orientador(a) - Universidade Federal de Ouro Preto
Doutora - Beatriz Schettini - Universidade Federal de Ouro Preto
Mestrando - Vinicios Pereira Teixeira - Universidade Federal de Ouro Preto

Juliana Evangelista de Almeida, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 03/09/2025

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 04/09/2025, às 15:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0973387** e o código CRC **D7D688EE**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

RESUMO

O presente trabalho oferece uma análise comparativa das bases legais estabelecidas no Artigo 11 da Lei Geral de Proteção de Dados (LGPD) do Brasil e no Artigo 9 do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, com foco no tratamento de dados sensíveis de saúde por agentes do setor privado. A pesquisa, de abordagem qualitativa e natureza jurídico-dogmática, baseou-se na interpretação normativa, doutrinária e jurisprudencial, complementada por revisão bibliográfica abrangente e análise de casos práticos. A investigação revela que, embora ambas as legislações compartilhem o princípio fundamental de proteção reforçada para dados de saúde, existem diferenças estruturais e operacionais significativas. O trabalho destaca a abordagem mais abrangente e proativa do GDPR, especialmente no que tange à diversidade de hipóteses legais, à qualificação do consentimento e à obrigatoriedade da Avaliação de Impacto à Proteção de Dados (DPIA). A influência da jurisprudência europeia é examinada como um fator crucial na consolidação dos padrões de proteção. Conclui-se que, apesar dos avanços da LGPD, persistem lacunas que demandam aprimoramento regulatório e institucional no Brasil, com a experiência europeia servindo como um valioso referencial para a construção de um sistema mais robusto e eficaz.

Palavras-chave: LGPD. GDPR. Dados Sensíveis. Saúde. Consentimento. Direito Médico. Privacidade

ABSTRACT

This paper offers an in-depth comparative analysis of the legal bases established in Article 11 of Brazil's General Data Protection Law (LGPD) and Article 9 of the European Union's General Data Protection Regulation (GDPR), focusing on the processing of sensitive health data by private sector entities. The research, conducted through a qualitative approach and legal-dogmatic methodology, was based on normative, doctrinal, and case law interpretation, complemented by an extensive literature review and practical case analysis. The investigation reveals that while both legislations share the fundamental principle of enhanced protection for health data, significant structural and operational differences exist. The paper highlights the GDPR's more comprehensive and proactive approach, particularly concerning the diversity of legal bases, the qualification of consent, and the mandatory Data Protection Impact Assessment (DPIA). The influence of European jurisprudence is examined as a crucial factor in consolidating protection standards. It concludes that despite the advances of the LGPD, gaps persist, demanding regulatory and institutional improvements in Brazil, with the European experience serving as a valuable benchmark for building a more robust and effective system.

Keywords: LGPD. GDPR. Sensitive Data. Health. Consent. Data Protection. Comparative Law.

SUMÁRIO

INTRODUÇÃO

Em 2020, a Finlândia foi palco de um dos mais graves escândalos de violação de dados sensíveis da história europeia: o caso Vastaamo, clínica privada de psicoterapia que teve seu banco de dados exposto por hackers[1]. Milhares de registros contendo relatos íntimos de sessões terapêuticas foram vazados e utilizados para extorsão direta de pacientes. A gravidade do caso não apenas expôs falhas na segurança digital da instituição, mas também evidenciou o impacto devastador que o tratamento indevido de dados sensíveis de saúde pode causar na vida das pessoas.

O mesmo desafio tem sido percebido em outras partes do mundo. Entre 2009 e 2024, 6.759 violações de dados de saúde, envolvendo 500 ou mais registros, foram reportadas ao Escritório de Direitos Civis do Departamento de Saúde e Serviços Humanos dos Estados Unidos. Essas violações resultaram na exposição ou divulgação indevida de informações de saúde protegidas de 846.962.011 indivíduos – o equivalente a mais de 2,6 vezes a população dos EUA[2]. Situações como essa mostram que, em tempos de intensificação tecnológica, a proteção jurídica dos dados pessoais, sobretudo os sensíveis, tornou-se uma urgência ética, social e legal.

No ordenamento jurídico brasileiro, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) estabelece hipóteses legais específicas para o tratamento de dados pessoais sensíveis, incluindo aqueles relativos à saúde. De forma análoga, o Regulamento Geral sobre a Proteção de Dados da União Europeia (Regulamento UE nº 2016/679 – GDPR) disciplina com rigor ainda mais detalhado o tratamento dessas informações. Ambas as normas reconhecem a especial proteção que deve ser conferida a tais dados, mas apresentam diferenças significativas quanto à estrutura das bases legais, à amplitude conceitual e ao papel do consentimento nas relações privadas.

---

[1] AFP. 'Shocking' hack of psychotherapy records in Finland affects thousands. **The Guardian**, 26 out. 2020. Disponível em: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland. Acesso em: 21 jul. 2025.

[2] US DEPARTMENT OF HEALTH AND HUMAN SERhttps://www.google.com/search?q=VICES. Office for Civil Rights. **Breach Portal: Notice of Disclosures of Protected Health https://www.google.com/search?q=Information**. Disponível em: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Acesso em: 20 jul. 2025.

A presente pesquisa foi desenvolvida por meio de uma abordagem qualitativa, de natureza jurídico-dogmática, com foco na interpretação normativa, doutrinária e jurisprudencial sobre o tratamento de dados pessoais sensíveis no setor privado de saúde. Para tanto, foi realizada uma revisão bibliográfica abrangente sobre o tema, com ênfase em obras nacionais e estrangeiras que tratam da proteção de dados, especialmente no que se refere ao consentimento, às bases legais e à tutela dos dados de saúde.

O objetivo central deste trabalho é analisar, de forma comparativa, o artigo 11 da LGPD e o artigo 9 do GDPR, com especial atenção às hipóteses legais que autorizam o tratamento de dados sensíveis de saúde por agentes do setor privado. A pesquisa está delimitada ao tratamento de dados de pessoas maiores de idade, excluindo-se os aspectos próprios à proteção de dados de crianças e adolescentes, que envolvem requisitos adicionais e tratamento normativo diferenciado.

Além da análise normativa e doutrinária, este trabalho inclui o estudo de jurisprudências relevantes – como os casos *Lindqvist* e *Z v. Finlândia* – e a interpretação de documentos internacionais, a exemplo do relatório da Comissão Europeia *Assessment of the EU Member States' rules on health data in the light of GDPR*. Também foi realizada uma análise de caso prática, na qual se examinaram incidentes de vazamento de dados e suas repercussões jurídicas no setor privado da saúde.

Ao final, pretende-se verificar em que medida o modelo europeu contribuiu para a aplicação da LGPD no Brasil, especialmente no que diz respeito ao equilíbrio entre a proteção dos titulares e a viabilidade operacional das atividades médico-assistenciais no setor privado.

No Capítulo 1, apresentam-se os fundamentos jurídicos da proteção de dados pessoais, com destaque para o direito à privacidade, à autodeterminação informativa e à personalidade. Examina-se a evolução do reconhecimento da proteção de dados como direito fundamental autônomo, tanto no ordenamento jurídico brasileiro quanto no contexto europeu, além de delimitar os conceitos de dado pessoal, dado sensível e dado anonimizado.

O Capítulo 2 aborda especificamente os dados sensíveis de saúde, justificando sua proteção reforçada à luz dos riscos de discriminação, estigmatização e violação da dignidade da pessoa humana. São analisadas as definições legais previstas na LGPD e no

GDPR, bem como as implicações sociais, éticas e jurídicas do tratamento dessas informações.

No Capítulo 3, realiza-se uma análise comparativa entre as hipóteses legais previstas no artigo 11 da LGPD e no artigo 9 do GDPR para o tratamento de dados sensíveis de saúde no setor privado. Discutem-se as diferenças na estrutura normativa, no papel atribuído ao consentimento e nas exigências adicionais previstas em cada sistema, com base em doutrina, jurisprudência e documentos oficiais.

O Capítulo 4 é dedicado à investigação das variações na aplicação prática do GDPR entre os Estados-Membros da União Europeia, tomando por base o relatório oficial da Comissão Europeia mencionado. Examinam-se as combinações mais comuns de bases legais utilizadas por agentes privados de saúde, bem como as críticas e recomendações feitas por órgãos como o Comitê Europeu de Proteção de Dados (EDPB), possibilitando uma reflexão sobre os limites e avanços do modelo europeu.

Por fim, apresenta-se um estudo de caso visando ilustrar como as bases legais são aplicadas (ou descumpridas) no cotidiano de instituições privadas de saúde, tanto no contexto europeu quanto no brasileiro, contribuindo para uma avaliação crítica da eficácia normativa e para sugestões de aprimoramento da legislação brasileira.

Capítulo 1: Fundamentos da Proteção de Dados Pessoais

Este capítulo apresenta os elementos fundamentais que estruturam o direito à proteção de dados pessoais, diferenciando-o da noção clássica de privacidade. São discutidos os conceitos de autodeterminação informativa, privacidade, intimidade e identidade informacional, bem como a consolidação da proteção de dados como um direito fundamental autônomo. Além disso, o capítulo trata da definição jurídica de dados pessoais, dados sensíveis e dados anonimizados, destacando os critérios interpretativos adotados pelas legislações moderna, como a LGPD e o GDPR.

1.1 Direito à privacidade e autodeterminação informativa

Muito se fala sobre o direito à privacidade, mas há pouco consenso quanto ao seu conceito exato. Um dos marcos clássicos desse reconhecimento é o artigo seminal de

Samuel D. Warren e Louis D. Brandeis, publicado em 1890 na *Harvard Law Review*, que introduziu a ideia do direito de estar só (*"the right to be let alone"*) como a essência da privacidade individual de cada pessoa[3].

O jurista italiano Stefano Rodotà analisou as definições, ou melhor, os perfis de privacidade que mais se destacaram ao longo do tempo. Alan Westin, por exemplo, definiu privacidade como "o direito de controlar a maneira pela qual os outros utilizam as informações a nosso respeito". L. M. Friedman (2007) entendeu-a como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social". Já J. Rosen (2001) viu a privacidade como "a reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetificado e avaliado fora de contexto".[4]

A partir dessas perspectivas, Rodotà constrói sua própria definição do direito à privacidade como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir a sua própria esfera particular" – acrescentando que essas visões não se excluem mutuamente, mas, ao contrário, vão incorporando progressivamente novos aspectos de liberdade dentro de um conceito mais abrangente de privacidade. Ou seja, trata-se de uma evolução do conteúdo tutelado por esse direito, ampliando-se gradativamente o escopo da liberdade protegida[5].

Na Constituição Federal de 1988, o direito à privacidade e à intimidade é consagrado como direito fundamental (art. 5º, X). No âmbito infraconstitucional, o art. 21 do Código Civil brasileiro também garante a proteção da vida privada, permitindo inclusive que se busque amparo judicial contra intervenções que exponham indevidamente a esfera pessoal do indivíduo.

Ramon Daniel Pizarro explica que o direito à intimidade é mais amplo do que à primeira vista possa parecer, possuindo uma tríplice dimensão: **a)** direito de ser deixado em paz e tranquilidade; **b)** direito à autonomia nas decisões existenciais; e **c)** direito ao controle sobre as informações pessoais que dizem respeito ao indivíduo. Desse modo, essa última dimensão, relativa à proteção de dados pessoais, apresenta uma estrutura de direito

---

[3] WARREN, Samuel D.; BRANDEhttps://www.google.com/search?q=IS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 20 jul. 2016.

[4] RODOTÀ, Stefano. A vida na sociedade de vigilância – a privacidade hoje. Rio de Janeiro: Renovar, 2008.

[5] RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

fundamental que é consequência de uma série de outros direitos relacionados – dignidade, privacidade, inviolabilidade de comunicações e dados, habeas data, entre outros – formando um arcabouço de salvaguardas interligadas, evidenciando a interconexão entre esses direitos fundamentais[6].

No entanto, apesar da relação entre os termos, a distinção entre os conceitos de privacidade, autodeterminação informativa e proteção de dados pessoais é essencial para a compreensão do regime jurídico atual. A privacidade, em sentido clássico, está relacionada ao direito de manter uma esfera íntima livre de interferências, sendo compreendida como a proteção da vida privada, intimidade, honra e imagem, conforme previsto no art. 5º, X, da Constituição Federal. Trata-se de um direito fundamental que garante ao indivíduo o poder de excluir terceiros de aspectos íntimos de sua vida[7].

A autodeterminação informativa, por sua vez, representa um desdobramento contemporâneo da privacidade, surgido na jurisprudência constitucional alemã (Volkszählungsurteil, 1983), e assegura ao titular o controle sobre os seus próprios dados pessoais, ou seja, o poder de decidir sobre a coleta, o uso e a finalidade desses dados[8].

Já a proteção de dados pessoais se afirma como um direito fundamental autônomo, voltado à regulação do tratamento de informações relativas a pessoas identificadas ou identificáveis, independentemente da violação de sua intimidade. Nesse sentido, Bruno Bioni destaca que a proteção de dados "não se confunde com a privacidade", pois sua função precípua é limitar o poder de uso da informação, promovendo responsabilidade, transparência e proporcionalidade na atividade de tratamento[9]. Nessa mesma linha, Danilo Doneda reforça que a proteção de dados opera como ferramenta jurídica que regula as práticas informacionais na sociedade digital, mesmo quando os dados já são públicos[10].

1.2 Proteção de dados como direito fundamental autônomo

---

[6] PIZARRO, Ramon Daniel. **Datos personales y habeas data**. Buenos Aires: Astrea, 2006

[7] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

[8] GOMES, Joaquim Benedito Barbosa. Autodeterminação informativa e proteção de dados pessoais. In: PFEIFFER, Roberto; DONEDA, Danilo; GICO JUNIOR, Ivo Teixeira (orgs.). *Direitos da personalidade, proteção de dados e novas tecnologias*. São Paulo: Thomson Reuters Brasil, 2020

[9] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Forense, 2019.

[10] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Forense, 2021.

A distinção entre privacidade e proteção de dados pessoais tem sido objeto de importantes reflexões na doutrina contemporânea, assim como o debate sobre a autonomia da proteção de dados como um direito fundamental. Maria Tzanou defende que a proteção de dados deve ser compreendida como um direito fundamental autônomo, não se restringindo a uma subcategoria da privacidade[11]. Para a autora, enquanto o direito à privacidade visa resguardar a esfera íntima e pessoal do indivíduo; protegendo-o contra intromissões indevidas, o direito à proteção de dados está voltado à regulação do tratamento adequado das informações pessoais, assegurando ao titular o controle sobre seus próprios dados, ainda que o conteúdo dessas informações não esteja diretamente ligado à intimidade. A proteção de dados teria, assim, uma finalidade própria e intrínseca, independentemente do teor do dado específico que se busca resguardar[12].

Conforme sustenta Tzanou (2013), essa autonomia normativa é evidente na União Europeia, onde a Carta de Direitos Fundamentais dedica dispositivos distintos ao respeito pela vida privada (art. 7º) e à proteção de dados pessoais (art. 8º), conferindo a este último um conteúdo e uma função próprios.

No Brasil, embora a Constituição de 1988 já garantisse a inviolabilidade da intimidade e da vida privada (art. 5º, X), foi com a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que a proteção de dados pessoais foi expressamente reconhecida como direito fundamental autônomo, com a inclusão do inciso LXXIX ao artigo 5º. Essa positivação constitucional reforça a ideia de que a proteção de dados possui contornos próprios, exigindo uma abordagem jurídica distinta da mera tutela da privacidade. Sarlet (2020) ressalta que:

> O direito fundamental à proteção de dados pessoais, embora relacionado com a dignidade da pessoa humana e outros direitos fundamentais, como o direito à privacidade e à autodeterminação informativa, não se confunde com o objeto de proteção desses direitos. A terminologia escolhida para ‘proteção de dados pessoais’ reflete uma mudança conceitual, considerando que dados devem ser vistos de maneira ampla, com o entendimento de que seu tratamento pode violar direitos fundamentais[13]

---

[11] TZANOU, Maria. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. **https://www.google.com/search?q=International Data Privacy Law**, v. 3, n. 2, p. 88-99, 2013.
[12] TZANOU, Maria. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. **https://www.google.com/search?q=International Data Privacy Law**, v. 3, n. 2, p. 88-99, 2013.
[13] SARLET, Ingo Wolfgang**. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais e Justiça. Belo Horizonte, v.14, n.42, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/38102. Acesso em: 20 julho. 2025.

Dessa forma, a escolha do legislador brasileiro pela expressão “proteção de dados” não foi ao acaso. Ela reflete a necessidade de se atribuir uma tutela mais ampla, correspondendo à relação intrínseca entre a pessoa e os dados que a representam. Em outras palavras, esse direito garante não só que cada pessoa possa decidir sobre o uso de seus próprios dados (dimensão individual), mas também cumpre um papel importante para toda a coletividade (dimensão coletiva).

Quando respeitado em larga escala, o direito à proteção de dados contribui para uma comunicação mais transparente e para a prevenção de manipulações e abusos de poder informacional. Assim, ele fortalece uma ordem social mais democrática – em contraste com uma concepção de privacidade limitada apenas à ideia de estar “deixado em paz”.

Bruno Bioni observa, por sua vez, que a personalidade pode ser entendida como o conjunto de características que distinguem uma pessoa[14]. Nesse sentido, compreender a proteção de dados pessoais como um direito da personalidade implica reconhecer a necessidade de tutela jurídica sobre os atributos materiais e imateriais que representam a projeção da pessoa humana – isto é, os sinais, marcas e expressões que configuram sua identidade perante a sociedade. Trata-se de um *novo tipo de identidade*, uma “etiqueta” que identifica o indivíduo. No ambiente virtual, a pessoa deixa de se apresentar apenas por seu corpo físico, assumindo também uma identidade informacional – um conjunto de dados que compõe sua persona digital e influência como ela é percebida, avaliada e tratada por instituições, plataformas e algoritmos[15].

Essa discussão vai além da proteção da privacidade em seu sentido clássico. No caso dos dados pessoais, mesmo informações aparentemente públicas devem estar juridicamente protegidas quando dizem respeito a um indivíduo identificável. O ponto central é que os dados precisam refletir de forma fiel a realidade da pessoa. Quando essa correspondência não ocorre, surge inclusive o direito à retificação, como forma de preservar a integridade dessa exteriorização e projeção do sujeito no ambiente digital.

---

[14] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
[15] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

Outro ponto fundamental levantado por Bioni é a necessidade de estabelecer um marco conceitual claro do que sejam dados pessoais, a fim de definir os limites da própria tutela jurídica. Afinal, o que o direito visa proteger, em essência, é o *dado pessoal*: aquele que pode ser visto como um prolongamento da pessoa e imputado a um sujeito, seja de forma imediata ou mediata. Para tal verificação, é necessária uma análise contextual e circunstanciada do conjunto de dados em questão – avaliação essa que pode ser mais rígida ou mais flexível, a depender do referencial teórico adotado (mais reducionista ou mais expansionista).

Para o referencial reducionista, como o próprio nome indica, há uma delimitação mais estrita do que venha a ser "dado pessoal". Nesse entendimento, um dado é considerado pessoal apenas quando houver a individualização precisa do sujeito titular, abarcando, portanto, apenas situações de identificação direta e imediata. Já o referencial expansionista adota um conteúdo muito mais amplo, considerando como dado pessoal também aquele cujo titular seja *identificável*, ou seja, exista um potencial de individualização mesmo que de forma mediata ou remota.

1.3 Conceitos essenciais: dados pessoais, dados sensíveis e dados anonimizados

A ampliação crescente do conceito de dado pessoal nas legislações modernas, como a LGPD e o GDPR, trouxe avanços importantes para a proteção da privacidade. Essa abordagem expansionista busca garantir que qualquer informação que possa estar relacionada a uma pessoa natural – mesmo de forma indireta – esteja sob proteção jurídica. Contudo, tal amplitude gera um desafio: como distinguir, de modo prático e conceitual, os dados pessoais daqueles considerados dados anônimos?

Paul De Hert e Vagelis Papakonstantinou definem dados anônimos como aqueles que "não se relacionam com uma pessoa identificada ou identificável, ou que foram tornados anônimos de modo que a pessoa não é ou não possa mais ser identificada"[16]. Essa definição é especialmente relevante no cenário atual, em que a evolução das tecnologias de análise e cruzamento de grandes bases de dados pode, em certos casos, tornar possível a

[16] DE HERT, Paul; PAPAKONSTANTINOU, Vagelis. T**he new General Data Protection Regulation: Still a lot of smoke but no roast. Computer Law & Security Review**, v. 34, n. 4, p. 807-817, 2018.

reidentificação de dados inicialmente tratados como anônimos. Ou seja, sem critérios adequados, haveria uma redundância normativa: dados tidos como “anônimos” acabariam sendo, em última instância, considerados dados pessoais.

Para evitar esse problema e garantir coerência normativa, tanto a LGPD quanto o GDPR adotaram um filtro conceitual que limita a elasticidade da expressão “pessoa identificável”: o critério da razoabilidade. Essa razoabilidade deve ser avaliada considerando a tecnologia existente, o acesso a bases de dados correlatas e os recursos econômicos disponíveis – uma vez que a anonimização não é estática: um dado considerado anonimizado hoje pode deixar de sê-lo no futuro, à medida que novas ferramentas tornem possível sua reversão. Assim, parte da doutrina propõe uma abordagem baseada na análise de risco e no monitoramento contínuo do contexto tecnológico.

Mesmo quando utilizamos dados aparentemente anonimizados, essas informações podem continuar a impactar diretamente a vida das pessoas. Isso ocorre, por exemplo, quando algoritmos usam tais dados para criar perfis ou tomar decisões que afetam oportunidades – como em processos seletivos de emprego ou na oferta de crédito. Nesses casos, pouco importa se a pessoa é identificável ou não; o que importa são as consequências reais do tratamento dos dados. Logo, dados “anonimizados” frequentemente continuam sendo utilizados para inferências de perfis e comportamentos, o que pode comprometer a privacidade mesmo sem identificação direta.

Por isso, a proteção de dados deve ir além da simples distinção entre dados pessoais e dados anônimos. O foco precisa recair também sobre os efeitos que o uso desses dados pode ter sobre o desenvolvimento da personalidade de alguém. Esse é justamente o espírito da LGPD ao estabelecer, em seu art. 12, §2º, que dados anonimizados podem ser considerados dados pessoais caso sejam utilizados para formação de perfis comportamentais. A tutela legal, portanto, deve acompanhar o risco e o impacto envolvidos, não apenas a forma ou a categorização formal dos dados.

É nesse contexto que se reforça a ideia de que a proteção de dados deve ser compreendida como um novo direito da personalidade. Isso permite que a legislação alcance não apenas os dados que identificam diretamente alguém, mas também todo tipo de tratamento que possa afetar a liberdade, a dignidade ou o modo de vida de uma pessoa, mesmo que os dados utilizados não revelem sua identidade de forma imediata ou clara.

Capítulo 2: Dados de Saúde e o Risco de Discriminação

Neste capítulo, analisa-se o enquadramento jurídico dos dados de saúde como categoria sensível, com ênfase nos riscos sociais e jurídicos decorrentes de seu uso indevido. São discutidos os fundamentos que justificam a proteção reforçada dessas informações, as definições legais adotadas pela LGPD e pelo GDPR, e os impactos que o tratamento inadequado pode gerar na vida dos titulares, especialmente em relação à estigmatização, exclusão social e discriminação. O capítulo também aborda o papel da confidencialidade e da responsabilidade dos agentes privados no contexto da saúde.

2.1 A relevância jurídica dos dados sensíveis de saúde

Conforme mencionado, a legislação de proteção de dados objetiva resguardar direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural. Assim, entende-se a proteção de dados pessoais como uma extensão dos direitos da personalidade. Não obstante, o legislador reconhece que algumas categorias de dados possuem uma carga mais sensível que outras, em razão da natureza íntima das informações que contêm o que demanda um tratamento adicional, específico e cauteloso.

Jonathan Mann, especialista na abordagem da saúde sob a ótica dos direitos humanos, argumenta que o estigma relacionado a determinadas doenças não é apenas um problema de preconceito, mas constitui uma violação direta de direitos fundamentais. Para ele, a confidencialidade das informações de saúde é condição indispensável para proteger a dignidade dos pacientes[17].

Além disso, é importante pontuar que o sofrimento gerado pelas doenças vai além dos aspectos clínicos individuais: ele é também de natureza social. Isso significa que o impacto de uma condição de saúde não se limita à dor física ou ao transtorno psicológico, mas se estende à forma como a sociedade reage a esse corpo adoecido. Pessoas com enfermidades estigmatizadas como transtornos mentais, HIV, epilepsia ou obesidade

[17] MANN, Jonathan. Health and human rights. **British Medical Journal**, London, v. 313, n. 7056, p. 748, 1996

muitas vezes enfrentam exclusão social, desemprego e isolamento. Tais efeitos são ainda mais graves quando seus dados de saúde se tornam públicos, expondo informações sensíveis que dão margem a discriminações. A proteção legal aos dados sensíveis de saúde é, portanto, também uma forma de mitigar o sofrimento social e garantir igualdade material na vida em sociedade[18].[19]

Segundo Chiara Spadaccini De Teffé, a justificativa para esse cuidado redobrado com dados de saúde é que o tratamento ou vazamento indevido de informações dessa natureza pode gerar riscos ainda mais significativos à pessoa humana, tornando-se fonte de preconceitos e discriminações ilícitas ou abusivas contra o titular. Trata-se de conteúdo diretamente ligado à intimidade e à identidade do indivíduo, o que eleva significativamente o potencial de dano em caso de violação de seus direitos.[20] A própria LGPD prevê, em seu art. 6º, que as atividades de tratamento de dados pessoais devem observar a boa-fé e uma série de princípios, entre eles o princípio da não discriminação, que proíbe o tratamento de dados para fins discriminatórios, respeitando a igualdade e a proteção dos direitos fundamentais dos titulares.

No que se refere ao conceito de dado sensível, Stefano Rodotà, importante jurista e político italiano o define da seguinte forma:

> Chama-se sensível o dado que revela a origem racial e étnica, as convicções religiosas, filosóficas ou de outra natureza, as opiniões políticas, a adesão a partidos, sindicatos, associações ou organizações de caráter religioso, filosófico, político ou sindical, bem como os dados pessoais que revelem o estado de saúde e a vida sexual.[21]

Ainda segundo De Teffé, a forma como definimos o que são dados sensíveis pode mudar consideravelmente a depender da legislação e do contexto cultural em que estamos inseridos. Em geral, há um entendimento crescente de que várias informações pessoais que, à primeira vista, poderiam parecer triviais, passam a ter um peso diferente quando

---

[18] BONNA, Alexandre Pacheco. Profiling, stigmatization, and civil liability. **Brazilian Journal of Law, Technology and Innovation**, v. 2, n. 1, p. 25-49, 2024.
[19] BARBOSA, Carla et al. **Comentários à Lei Geral de Proteção de Dados: sob a perspectiva do direito médico e da saúde**. 1. ed. https://www.google.com/search?q=Indaiatuba, SP: Foco, 2023. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 17 jul. 2025.
[20] SPADACCINI de TEFFÉ, Chiara. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1. ed. Indaiatuba: Editora Foco, 2022.
[21] RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

utilizadas de determinadas maneiras[22]. Por isso, não basta olhar isoladamente para o dado em si: é preciso observar o que se faz com ele e quais as possíveis consequências desse uso. Para avaliar se um dado deve ser considerado sensível, é importante levar em conta, por exemplo, a natureza da informação, o contexto e a finalidade do tratamento, a possibilidade de combinação com outros conjuntos de dados e as capacidades tecnológicas presentes e futuras.[23]

Portanto, a compreensão do que constitui um dado sensível exige uma abordagem dinâmica, que leve em conta o contexto, os sujeitos envolvidos e a forma como os dados são tratados. Considerar um dado isoladamente, de maneira estática, pode ser insuficiente, especialmente diante da possibilidade de cruzamento com outras informações e da evolução constante das tecnologias de análise de dados. Essa perspectiva evita tanto uma concepção excessivamente limitada quanto o risco de banalização da categoria de dados sensíveis.

O Regulamento Geral de Proteção de Dados da União Europeia (Regulamento UE nº 2016/679 – GDPR) trouxe avanços importantes no tratamento dos dados sensíveis ao definir um rol específico de "*categorias especiais de dados pessoais*". Essa sistematização contribuiu para uma maior segurança jurídica, ao delimitar com mais precisão quais informações devem ser tratadas como sensíveis e ao fornecer definições claras sobre cada uma delas.

Entre os dados considerados sensíveis pelo regulamento europeu estão aqueles que revelam a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, além de dados genéticos, dados biométricos (quando usados com o objetivo de identificar uma pessoa natural), informações sobre a saúde, a vida sexual e a orientação sexual dos indivíduos.

O GDPR também introduziu regras específicas para o tratamento de dados sensíveis, estabelecendo não apenas bases legais próprias para esse tipo de dado, mas também restrições adicionais – especialmente no que diz respeito à tomada de decisões automatizadas envolvendo tais informações.

---

[22] SPADACCINI de TEFFÉ, Chiara. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1. ed. Indaiatuba: Editora Foco, 2022.

[23] SPADACCINI de TEFFÉ, Chiara. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1. ed. Indaiatuba: Editora Foco, 2022.

Por exemplo, quando há tratamento de dados sensíveis em grande escala, o regulamento impõe obrigações mais rígidas ao controlador, como a nomeação obrigatória de um Encarregado de Proteção de Dados (Data Protection Officer – DPO), nos termos do art. 37(1)(c) do GDPR, e a realização de uma Avaliação de Impacto à Proteção de Dados (Data Protection Impact Assessment – DPIA), conforme previsto no art. 35(3)(b). Assim, além de identificar a base legal adequada, o controlador deve cumprir exigências adicionais para garantir a conformidade e a proteção efetiva dos titulares.

O artigo 9º, §1º do GDPR define como dados sensíveis os "dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos tratados com o propósito de identificar de forma exclusiva uma pessoa natural, dados relativos à saúde, à vida sexual ou à orientação sexual de uma pessoa natural". De modo equivalente, a LGPD, em seu art. 5º, II, apresenta uma lista de dados pessoais sensíveis, incluindo informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dado genético ou biométrico quando vinculado a uma pessoa natural.

Discute-se na doutrina se esse rol legal de dados sensíveis é taxativo ou apenas exemplificativo. A maior parte dos autores tende a considerar o rol exemplificativo, dada a natureza aberta do conceito de dado sensível e a rápida evolução tecnológica.[24]

Caitlin Mulholland, por exemplo, destaca que a definição legal deve ser interpretada de forma funcional, considerando os efeitos concretos do tratamento de dados sobre os direitos fundamentais dos titulares. Segundo a autora, mesmo que um dado não esteja expressamente previsto na lista legal, ele poderá ser considerado sensível se, em determinado contexto, for capaz de revelar informações íntimas ou gerar discriminação.

[24] A doutrina majoritária interpreta o rol de dados pessoais sensíveis previsto no art. 5º, II da LGPD como exemplificativo, entendendo que a proteção de dados deve acompanhar os avanços tecnológicos e os contextos de risco, especialmente diante do uso crescente de técnicas de perfilização (profiling). Danilo Doneda e Laura Schertel Mendes destacam essa interpretação em diversos comentários à LGPD, afirmando expressamente que se trata de um "rol meramente exemplificativo". Pablo Malheiros, na obra Direito Civil e Tecnologia, também defende que a ampliação interpretativa é necessária para abarcar novas formas de violação de direitos fundamentais decorrentes do tratamento automatizado de dados. Leonardo Neves de Albuquerque, por sua vez, sustenta que a rigidez de um rol taxativo afronta o direito fundamental à proteção de dados em contextos discriminatórios não previstos expressamente pela lei, conforme exposto em sua análise sobre a influência dos padrões europeus na LGPD.

Kremer também defende a importância de se adotar uma abordagem que leve em conta a diversidade ao implementar a proteção dos dados pessoais sensíveis.[25]

2.2 Definições legais de dados sensíveis no GDPR e na LGPD

O GDPR, como visto, delineia categorias especiais de dados pessoais no seu art. 9º, enquanto a LGPD traz definição semelhante no art. 5º, II. Ambas as legislações enquadram dados de saúde no rol de dados sensíveis e estabelecem salvaguardas específicas para o seu tratamento. Apesar da intenção comum de reforçar a proteção, há diferenças na forma como cada regime concebe e operacionaliza essas definições.[26][27]

O regulamento europeu não apenas lista as categorias sensíveis, mas também impõe medidas adicionais de compliance: a obrigação de realizar DPIA ou Data Protection Impact Assessment (em português, Avaliação de Impacto à Proteção de Dados)[28] em certos casos de dados sensíveis (art. 35 do GDPR), a necessidade de um Encarregado (ou Data Protection Officer - DPO)[29] em organismos que tratem dados de saúde em larga escala (art. 37), além de prever, em considerandos como o 53 e o 54, a necessidade de maior proteção a esses dados devido aos riscos de discriminação e outros prejuízos aos titulares. A LGPD, embora liste os dados sensíveis de modo similar, não impõe de imediato a obrigatoriedade de instrumentos como o relatório de impacto (RIPD), deixando essa exigência a critério da autoridade nacional em situações específicas (art. 38). Isso indica, desde logo, uma

---

[25] MULHOLLAND,Caitlin;KREMER,Bianca.Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In Rodrigo da Guia Silva: Gustavo Tepedino.Org. O Direito Civil na era da inteligência Artificial. São Paulo: Revista dos Tribunais,2020, p.580.

[26] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 14 ago. 2018.

[27] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4.5.2016.

[28] O Relatório de Impacto à Proteção de Dados (RIPD), mais conhecido pela sigla em inglês "DPIA" (*Data Protection Impact Assessment*), é um documento concebido para descrever o tratamento de dados pessoais, avaliar a sua necessidade/proporcionalidade e ajudar a gerir os respectivos riscos aos direitos e liberdades, por meio da avaliação de tais riscos e da determinação de medidas para fazer frente a eles. Para mais informações, ver:<https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>.

[29] O tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o Controlador e o Operador. Além deles, há a figura do Encarregado (ou Data Protection Officer - DPO), que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os titulares dos dados e demais entidades de fiscalização. Para mais informações, ver:<https://ufdpar.edu.br/ufdpar/paginas/lei-geral-de-protecao-de-dados-lgpd-paginas/encarregado-dpo>.

diferença de rigidez normativa entre os dois sistemas na aplicação prática das definições sensíveis.

Outra distinção está na possibilidade de se ampliar a interpretação do rol de dados sensíveis. Conforme mencionado, a doutrina brasileira tende a interpretar o rol da LGPD de forma não exaustiva, considerando sensível qualquer dado que, pelo contexto, revele informações íntimas ou potencialmente discriminatórias, ainda que não explicitado na lei. Essa visão funcional acompanha a dinamicidade tecnológica e social, evitando lacunas de proteção. Já no contexto europeu, o art. 9(1) do GDPR estabelece um rol fechado de "categorias especiais de dados pessoais", que não pode ser ampliado pelos Estados-Membros, mas cujo alcance é estendido pela expressão "dados que revelem" tais características, ampliando sua aplicação sem alterar o rol formal[30]. Essa solução normativa busca garantir uniformidade na União Europeia, ao passo que o modelo brasileiro aposta em flexibilidade diante de cenários emergentes.

Embora o artigo 9(1) do GDPR apresente um rol fechado de categorias especiais de dados pessoais[31], sua aplicação prática admite expansão: dados que, por inferência, revelem características sensíveis também são abarcados. O Tribunal de Justiça da União Europeia já reconheceu que informações aparentemente neutras podem ser enquadradas como sensíveis quando permitem, por dedução ou cruzamento, identificar elementos protegidos.[32]

Há ainda críticas de que, com o aumento da capacidade tecnológica de análise e cruzamento de dados, cresce o risco de "inflação" do conceito de dado sensível, fazendo com que um número cada vez maior de informações, mesmo não listadas originalmente, passe a ser tratado como tal[33].

---

[30] QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework. German Law Journal, v. 22, p. 1583–1612, 2021. DOI: https://doi.org/10.1017/glj.2021.79.

[31] KUNER, Christopher; GKOTSOPOULOU, Olga. *Article 9. Processing of special categories of personal data*. In: The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. Oxford University Press, 2021

[32] INSIDEPRIVACY. *Special Category Data by Inference: CJEU significantly expands the scope of Article 9 GDPR*. 2022. Disponível em: https://www.insideprivacy.com/eu-data-protection/special-category-data-by-inference-cjeu-significantly-expands-the-scope-of-article-9-gdpr/. Acesso em: 8 ago. 2025.

[33] QUINN, Paul; MALGIERI, Gianclaudio. *The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework*. *German Law Journal*, Cambridge University Press, v. 22, p. 1583–1612, 2021. DOI: https://doi.org/10.1017/glj.2021.79.

2.3 Confidencialidade, estigmas sociais e impacto no titular

Na era da informação, o corpo humano não se resume ao aspecto físico e visível. Os dados e informações referentes à pessoa compõem o que Stefano Rodotà denominou de "corpo eletrônico",[34] cuja proteção deve ser integralmente assegurada pelas normas de proteção de dados especialmente pela LGPD, pela Constituição Federal e pela legislação infraconstitucional.[35]

O estado de saúde é considerado um dos dados mais sensíveis exatamente porque diz respeito àquilo que muitas vezes as pessoas escondem até de si mesmas: a sua vulnerabilidade. Diferentemente de outros dados, como endereço ou profissão, revelar informações de saúde envolve expor uma parte profundamente íntima da existência: o corpo, a dor, os limites físicos e mentais , condições que podem gerar medo, estigma ou até exclusão social se divulgadas sem controle.

Saber que alguém tem uma doença crônica, um transtorno mental, é portador de HIV, faz terapia, ou já teve câncer ou infertilidade, por exemplo, pode alterar radicalmente a forma como essa pessoa é tratada e vista socialmente, interferindo em como ela se afirma no espaço público. Esse efeito pernicioso se manifesta em contextos diversos, como o mercado de trabalho, os seguros e planos de saúde, as interações em redes sociais ou qualquer outro ambiente de convivência.

Por isso, há grande preocupação em impedir a violação de direitos e o desenvolvimento de análises ou perfis discriminatórios a partir desses dados – que podem ser usados para segmentar e personalizar serviços de maneira potencialmente excludente.

Assim, ao proteger juridicamente essas informações, estamos na verdade protegendo a liberdade da pessoa de não ser definida exclusivamente pela sua doença, seu diagnóstico ou seu histórico médico. Em última instância, protege-se a liberdade de existir sem ser reduzido à própria fragilidade.

Shoshana Zuboff, professora emérita da Harvard Business School e estudiosa das relações entre tecnologia, dados e poder, argumenta em sua obra "*A Era do Capitalismo de*

---

[34] RODOTÀ, Stefano. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, pp. 91-107, 2004. p. 103-104.

[35] BARBOSA, Carla et al. **Comentários à Lei Geral de Proteção de Dados: sob a perspectiva do direito médico e da saúde**. Indaiatuba, SP: Foco, 2023, p. 88.

Vigilância" que as experiências humanas passaram a ser sistematicamente transformadas em dados, com o objetivo de prever e influenciar comportamentos para fins econômicos. Quando dados sensíveis de saúde são inseridos nesse circuito sendo coletados, analisados, classificados e até comercializados, a própria condição humana se converte em insumo para estratégias corporativas. Trata-se não apenas de uma invasão de privacidade, mas de uma forma de instrumentalização da vida, em que a pessoa deixa de ser sujeito para tornar-se um "perfil de risco" ou um consumidor parametrizado. Proteger esses dados, portanto, é também resistir à lógica que transforma vulnerabilidade em mercadoria.[36]

O cenário atual evidencia um crescimento exponencial de serviços e tecnologias voltados à área da saúde, com destaque para o uso de inteligência artificial em diagnósticos, softwares que monitoram tratamentos e aplicativos de saúde (por exemplo, apps de acompanhamento menstrual ou de gestão de exercícios). Esse avanço é acompanhado por estratégias cada vez mais agressivas de coleta de dados sensíveis, principalmente por parte de empresas de tecnologia, indústrias farmacêuticas, operadoras de planos de saúde, seguradoras e até setores de marketing especializados.

A coleta e o tratamento de dados de saúde ocorrem também em larga escala por instituições públicas (Ministério da Saúde, secretarias estaduais e municipais, hospitais públicos e profissionais ligados ao SUS), além de órgãos reguladores como a Agência Nacional de Saúde Suplementar (ANS).

Entretanto, focando-se no setor privado, é preciso observar que clínicas, hospitais e consultórios particulares também lidam com grandes volumes de dados sensíveis e estão submetidos às obrigações da LGPD. Nesses ambientes privados, o Prontuário Eletrônico do Paciente (PEP) tornou-se uma ferramenta central para registro, controle e armazenamento de informações de saúde – como histórico familiar, diagnósticos, prescrições, exames e outros dados essenciais ao atendimento. Seu uso, porém, exige atenção especial à segurança da informação.

É imprescindível que o PEP opere em sistemas protegidos por criptografia, armazenados em servidores seguros (como em nuvem) e com assinatura eletrônica dos profissionais de saúde (certificação digital), de modo a garantir a autenticidade e a

---

[36] ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1ª ed. Rio de Janeiro: Intrínseca, 2020.

integridade dos documentos. Mesmo em clínicas e consultórios particulares de menor porte, a manutenção dos dados deve observar normas rígidas de sigilo e confidencialidade, sob pena de responsabilização administrativa e judicial dos agentes por uso inadequado ou descumprimento da LGPD.

Capítulo 3: Tratamento de Dados Sensíveis de Saúde no Setor Privado na LGPD e no GDPR

Este capítulo analisa como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) regulam o tratamento de dados pessoais sensíveis relacionados à saúde no setor privado. O foco recai sobre os fundamentos legais que autorizam esse tratamento, as exigências específicas aplicáveis a esse tipo de dado e as salvaguardas que devem ser adotadas pelos agentes de tratamento. Além disso, são examinadas as diferenças e semelhanças entre as duas legislações no que diz respeito à definição, à base legal e às obrigações dos responsáveis pelo tratamento de dados de saúde.

3.1 Consentimento e outras bases legais previstas na LGPD para o setor privado

Inicialmente, cabe pontuar que, no tocante ao consentimento, há dois artigos específicos na LGPD: o art. 7º, I, que trata do consentimento para dados *não sensíveis*, e o art. 11, I, que diz respeito aos dados sensíveis. O artigo 7º da LGPD estabelece as bases legais gerais para o tratamento de dados pessoais, ou seja, as situações em que o tratamento de dados comuns (não sensíveis) é permitido listando diversas hipóteses, entre elas o consentimento do titular (inciso I). Já o artigo 11 da LGPD dispõe sobre as bases legais específicas para tratamento de dados sensíveis, mantendo várias das bases já previstas no art. 7º, mas excluindo duas hipóteses: a de tutela dos legítimos interesses do controlador ou de terceiro (prevista no art. 7º, IX) e a de proteção de crédito (art. 7º, X).

A razão dessa exclusão é clara: quando o tratamento de dados pessoais não sensíveis está vinculado aos propósitos legítimos do controlador ou de terceiro, admite-se a base do

legítimo interesse, que, no entanto, exige avaliação cuidadosa e criteriosa para assegurar equilíbrio com os direitos do titular. Porém, no caso de dados sensíveis, o legislador optou por não disponibilizar a hipótese do legítimo interesse, entendendo que se trata de uma base legal flexível demais frente ao nível de proteção exigido para dados que envolvem maior risco à dignidade e à privacidade dos titulares. Assim, para dados sensíveis, como os de saúde, a atividade de tratamento deve enquadrar-se nas demais bases legais dispostas no art. 11 da LGPD, entre as quais se destaca justamente o consentimento (foco central deste trabalho). O jurista Danilo Doneda reforça essa opção legislativa, argumentando que o legítimo interesse, por ser uma base aberta e de aplicação discricionária, não atenderia ao nível de proteção requerido para dados de natureza sensível; por envolver riscos superiores aos direitos dos titulares, esses tratamentos demandam fundamentos mais robustos e controlados[37].

Além do consentimento, o art. 11 da LGPD prevê outras bases legais que podem justificar o tratamento de dados sensíveis. Entre elas estão, por exemplo: a proteção da vida ou da incolumidade física do titular ou de terceiro; a tutela da saúde, exclusivamente, em procedimento realizado por profissionais da área médica, serviços de saúde ou autoridade sanitária; a prevenção à fraude e à segurança do titular, em processos de identificação e autenticação em sistemas eletrônicos; o exercício regular de direitos, inclusive em contrato ou em processo judicial, administrativo ou arbitral; e o cumprimento de obrigação legal ou regulatória pelo controlador – hipóteses que serão discutidas adiante no trabalho.

A LGPD também traz uma definição cuidadosa de consentimento, caracterizando-o como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII), em linha com o GDPR e com as normas mais atuais sobre o tema. Essa definição realça que o consentimento deve ser dado de forma voluntária, com pleno conhecimento e compreensão pelo titular, e sem ambiguidades quanto ao objetivo para o qual é fornecido.

Na perspectiva de Flaviana Rampazzo Soares, é essencial distinguir, de início, o consentimento na LGPD voltado ao tratamento de dados sensíveis do paciente (que ela denomina *CD*) do consentimento relacionado ao atendimento médico em si (*CA*). Embora

---

[37] DONEDA, Danilo. ***Da proteção de dados pessoais à tutela do consentimento: uma abordagem crítica***. Rio de Janeiro: Renovar, 2006.

ambos compartilhem o nome "consentimento", referem-se a dimensões distintas: o *CD* diz respeito à permissão para uso de dados pessoais (como histórico de saúde, exames, prontuário médico) para finalidades específicas de tratamento de dados, enquanto o *CA* refere-se à autorização do paciente para que o profissional de saúde realize determinados procedimentos médicos sobre seu corpo ou sua psique. Em outras palavras, o primeiro é um consentimento no âmbito da proteção de dados pessoais, e o segundo é um consentimento de natureza ética/biológica vinculado ao ato médico[38].

Soares esclarece ainda que o consentimento *para dados* (CD) é condição de licitude para o tratamento dos dados pessoais sensíveis do paciente – sua ausência pode acarretar a ilicitude do tratamento e responsabilidade civil do agente –, ao passo que o consentimento *para ato médico* (CA) é requisito de validade para a intervenção médica em si, sendo ambos manifestações da autodeterminação do paciente, porém com consequências jurídicas distintas em caso de vício ou ausência[39]. Note-se que, caso o titular não tenha capacidade para consentir (por exemplo, em situação de incapacidade civil ou impedimento médico), a autorização deve ser suprida por seu responsável legal, a qual igualmente precisa ser específica e destacada, tanto no âmbito do tratamento de dados quanto no da intervenção médica.

Além da base legal do consentimento, é possível reconhecer o tratamento de dados de saúde com fundamento no cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, "a" da LGPD). Nesse contexto, podem ser citadas, por exemplo, obrigações oriundas de Códigos de Ética Profissional, portarias do Ministério da Saúde ou resoluções de conselhos profissionais consolidados. A título ilustrativo, a Resolução CFM nº 1.605/2009 do Conselho Federal de Medicina determina que o médico não pode divulgar o conteúdo do prontuário ou da ficha médica do paciente sem o consentimento deste. Da mesma forma, a Resolução CFM nº 1.821/2007 estabelece normas técnicas sobre a digitalização e o uso de sistemas informatizados para armazenar e manusear prontuários, permitindo inclusive a substituição do papel pelo formato digital, desde que garantida a

---

[38] SOARES, Flaviana Rampazzo. ***Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade civil***. Revista IBERC (Responsabilidade Civil), Belo Horizonte, v. 5, n. 10, p. 75, 2021.

[39] SOARES, Flaviana Rampazzo. ***Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade civil***. Revista IBERC (Responsabilidade Civil), Belo Horizonte, v. 5, n. 10, p. 75, 2021.

identificação segura das informações de saúde. Tais regras de natureza profissional e administrativa, ao serem impostas aos controladores (médicos e estabelecimentos de saúde), acabam por configurar uma obrigação legal/regulatória que autoriza o tratamento de dados sensíveis independentemente do consentimento do paciente, inserindo-se na exceção do art. 11, II, "a".

Outra hipótese legal prevista no art. 11, II da LGPD é o exercício regular de direitos, inclusive em contrato, em processo judicial, administrativo ou arbitral (inciso II, "d"). Em determinadas relações contratuais – como em contratos de seguro saúde ou seguro de vida, o tratamento de dados sensíveis pode ser necessário para viabilizar a própria prestação do serviço pactuado. Isso ocorre, por exemplo, quando a seguradora precisa acessar informações médicas do segurado para efetuar o ressarcimento de despesas ou pagar uma indenização por invalidez decorrente de doença. Trata-se, portanto, do exercício regular de um direito decorrente da relação contratual, o que pode servir de base legal para o tratamento de dados sensíveis, desde que presentes certos requisitos: a existência de um direito legítimo em questão, o uso não abusivo desse direito e sua origem em vínculo contratual válido. Essa hipótese se distingue do legítimo interesse do controlador, exigindo uma análise mais rigorosa, justamente por envolver dados sensíveis.

Outra base legal presente no art. 11, II da LGPD, que pode ser aplicada no contexto da saúde, é a prevista na alínea "e": proteção da vida ou da incolumidade física do titular ou de terceiros. Essa base mostra-se especialmente relevante em situações de emergência nas quais não é possível obter o consentimento do paciente. A doutrina aponta que essa hipótese se aplica, por exemplo, quando um paciente é atendido em um hospital no qual nunca esteve antes, após um acidente grave, e o médico responsável precisa acessar seu histórico médico (exames, alergias, medicamentos em uso) para oferecer o cuidado adequado. Nesse tipo de situação, o compartilhamento de dados de saúde entre instituições, sem o consentimento prévio do titular, pode se justificar pela urgência e pela necessidade de preservar a integridade física e a vida da pessoa.

O art. 11, II, "f" da LGPD menciona ainda a base de tutela da saúde, exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária. A adequada aplicação dessa base legal exige cautela, especialmente porque seu uso não deve ocorrer de forma indiscriminada para qualquer tratamento de dados no setor

da saúde. Conforme o *Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde*, publicado em 2021 pela Confederação Nacional de Saúde (CNSaúde), essa base só é válida quando o tratamento for conduzido por profissionais ou instituições de saúde (ou autoridade sanitária) estritamente dentro de finalidades de cuidado à saúde, respeitando-se o princípio da confidencialidade profissional[40].

Nesse contexto, o referido Código recomenda que a interpretação da base de tutela da saúde seja feita à luz do conceito similar previsto no GDPR, especificamente nos artigos 9(2)(h) e 9(3). Esses dispositivos do regulamento europeu estabelecem que o tratamento de dados sensíveis é permitido quando necessário para fins de medicina preventiva ou do trabalho, diagnóstico médico, prestação de cuidados ou tratamentos de saúde, ou gestão de sistemas de saúde ou programas de assistência social, desde que realizado por profissional sujeito à obrigação legal de sigilo (ou sob sua responsabilidade).

Com base nessa diretriz, torna-se imprescindível verificar, em cada caso, se o tratamento de dados está vinculado às atividades-fim de prestadores de saúde (como exames médicos, diagnóstico clínico ou atendimento assistencial) e se os dados permanecem sob a responsabilidade de profissionais obrigados ao sigilo médico. O Código de Boas Práticas destaca, por exemplo, o manuseio de prontuários médicos por profissionais de saúde, o uso desses registros para gerar diagnósticos com apoio de softwares, ou o acesso a informações do paciente em ambientes clínicos – todas situações abarcadas pela tutela da saúde. Já nos casos em que o tratamento é feito por profissionais que não estão sujeitos à obrigação de sigilo (por exemplo, um analista de TI terceirizado sem vínculo de confidencialidade estrito), essa base legal não poderia ser invocada, devendo o tratamento encontrar fundamento em outra hipótese legal ou ser vedado.

Em relação a exames laboratoriais, o Código orienta igualmente que sejam observadas as bases legais do art. 11 da LGPD. A base de tutela da saúde será aplicável quando atividades como coleta de amostras, envio para análise clínica, emissão de laudos, divulgação de resultados ao paciente e armazenamento de informações forem realizadas por profissionais de saúde vinculados ao sigilo profissional. Nessas situações, entende-se que o

---

[40] CNSaúde (Confederação Nacional de Saúde). ***Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde***. Brasília: CNSaúde, 2021. Disponível em: http://cnsaude.org.br/codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-servicos-em-saude/. Acesso em: 20 jul. 2025.

compartilhamento de dados entre laboratório e médico, por exemplo, está abrangido pela tutela da saúde. Em contrapartida, se algum desses processos envolver agentes sem dever de sigilo (como um prestador logístico de TI que armazena os dados em nuvem, fora do controle do hospital), talvez essa base não seja adequada e deva-se recorrer, se possível, ao consentimento explícito do paciente ou outra hipótese.

Agora, voltemos o olhar para o cenário europeu: como o GDPR disciplina os dados relativos à saúde no setor privado, e quais bases legais dispõe para tanto?

3.2 Consentimento e outras bases legais previstas no GDPR e critérios europeus

As informações pessoais relacionadas ao estado de saúde de um indivíduo são classificadas como dados sensíveis tanto pelo art. 9(1) do GDPR quanto pelo art. 6º da Convenção 108 modernizada. Por isso, os dados de saúde estão sujeitos a regras de tratamento mais restritivas e rigorosas do que aquelas aplicáveis a dados pessoais comuns.

O GDPR, em seu art. 4º, traz diversas definições, incluindo a de **dados relativos à saúde**, entendidos como "informações pessoais vinculadas à saúde física ou mental de um indivíduo, incluindo aquelas geradas na prestação de serviços de saúde e que revelem aspectos sobre o seu estado de saúde".

O Considerando 35 do GDPR, parte de sua seção introdutória de fundamentos, esclarece o alcance do termo "dados relativos à saúde" nos seguintes termos:

> **(35)** Devem ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Isso inclui as informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, o risco de doença, histórico clínico, tratamento clínico ou estado fisiológico ou biomédico do titular dos dados, independentemente de sua fonte (por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro).[41]

[41] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. ***Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).*** Jornal Oficial da União Europeia, L 119, 4.5.2016.

O Manual da Legislação Europeia sobre Proteção de Dados é um guia interpretativo e educacional, elaborado pelo Conselho da Europa e pela FRA, que sintetiza e explica o conteúdo das principais normas europeias sobre privacidade e proteção de dados, como o GDPR e a Convenção 108, com base na jurisprudência e prática institucional. O documento utiliza o caso Z c. Finlândia como um exemplo prático para ilustrar a importância da proteção dos dados de saúde à luz do artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH), que assegura o direito ao respeito pela vida privada e familiar.

No caso em questão, o ex-marido da requerente, que era portador do vírus HIV, havia sido condenado por diversos crimes sexuais e por tentativa de homicídio, ao expor deliberadamente suas vítimas ao risco de infecção. A requerente, preocupada com sua privacidade e integridade, solicitou ao tribunal que os autos do processo e o acórdão permanecessem confidenciais por um período superior a 10 anos. No entanto, o pedido foi negado, e a decisão do tribunal de recurso manteve os nomes completos da requerente e de seu ex-marido no texto do acórdão.

O caso foi levado ao Tribunal Europeu dos Direitos Humanos (TEDH), que entendeu que a divulgação da identidade da requerente e de informações sobre seu estado de saúde, especialmente considerando a sensibilidade associada à infecção por HIV, configurava uma ingerência desproporcional e desnecessária à sua vida privada, violando assim o artigo 8.º da CEDH. O tribunal destacou que, em muitas sociedades, o estigma social relacionado ao HIV representa um grave risco à dignidade, à integridade e à inclusão da pessoa afetada, o que exige proteção especial dos dados médicos e maior rigor quanto ao acesso público a tais informações.

Embora o TEDH não seja responsável por aplicar o Regulamento Geral sobre a Proteção de Dados (GDPR), suas decisões têm forte valor interpretativo no contexto europeu, sob a ótica do tratamento de dados pessoais. Assim, a jurisprudência do TEDH funciona como base complementar para a aplicação do GDPR, especialmente quando se trata de dados sensíveis, como os de saúde, reforçando a compreensão de que a proteção desses dados está diretamente relacionada à preservação dos direitos fundamentais da pessoa.

Outro caso extremamente importante, que definiu as bases para esse conceito mais amplo de dados relativos à saúde, foi a decisão do Tribunal de Justiça da União Europeia (TJUE) no caso *Lindqvist* (Processo C-101/01), julgado em 2003, desempenhou um papel fundamental na consolidação da proteção dos dados relativos à saúde no contexto europeu, ainda sob a vigência da Diretiva 95/46/CE. Essa diretiva, aprovada em 1995 e vigente na época, antes do GDPR, tinha como objetivo harmonizar as legislações dos Estados-Membros em matéria de proteção de dados pessoais, assegurando tanto o respeito aos direitos fundamentais quanto a livre circulação desses dados no espaço europeu. Um de seus dispositivos centrais era o artigo 8.º, que proibia o tratamento de dados sensíveis, incluindo aqueles relacionados à saúde, salvo em hipóteses excepcionais.

No caso em questão, a ré, Sra. Bodil Lindqvist, uma catequista sueca, publicou em sua página pessoal na internet informações sobre colegas de trabalho, incluindo o fato de que uma delas havia machucado o pé e estava afastada por motivo médico. A controvérsia levou o TJUE a interpretar se essa menção constituía dado pessoal sensível à luz da Diretiva. O Tribunal adotou uma interpretação ampla (lato sensu) da expressão "dados relativos à saúde", entendendo que qualquer informação que revele, mesmo de forma indireta, aspectos do estado físico ou mental de um indivíduo se enquadra como dado sensível.

Isso incluiu não apenas diagnósticos ou prontuários médicos, mas também referências simples ao fato de que alguém está de licença por problemas de saúde. Essa abordagem foi decisiva para a evolução do conceito na legislação europeia e influenciou diretamente o Regulamento (UE) 2016/679, o GDPR, que substituiu a diretiva em 2018. Embora o RGPD traga inovações, ele não modifica a compreensão da União Europeia quanto à importância da proteção dos dados pessoais sensíveis, preservando o compromisso com a defesa significativa dos direitos fundamentais dos titulares dessas informações.

O artigo 4.º, inciso 15, do GDPR adota justamente essa noção ampliada, definindo como dado de saúde qualquer informação sobre o estado físico ou mental, passado, presente ou futuro de uma pessoa, inclusive inferências extraídas de dados que, isoladamente, poderiam parecer neutros. A jurisprudência do caso *Lindqvist*, portanto, serviu como base interpretativa sólida para a construção de um regime mais rigoroso e

protetivo no tratamento de dados sensíveis sob a nova regulação europeia. Observa-se a seguir, a conclusão do Grupo de Trabalho:

> Porém, o Grupo de Trabalho considera que os dados de saúde, ou todos os dados pertencentes ao status de saúde de um titular de dados, é um termo muito mais amplo que o termo 'médico'. Com base na Diretiva de proteção de dados, os legisladores, juízes e as Agências de Proteção de Dados nacionais concluíram que informações como o fato de uma mulher ter quebrado a perna (Lindqvist), que uma pessoa está usando óculos ou lentes de contato, dados sobre os aspectos intelectuais e emocionais da capacidade uma pessoa (como QI), informações sobre hábitos de fumar e beber, dados sobre alergias divulgadas a entidades privadas (como companhias aéreas) ou a órgãos públicos (como escolas); dados sobre condições de saúde a serem usadas em situações de emergência (por exemplo, informações de que uma criança que participa de um acampamento de verão ou evento semelhante sofre de asma); participação de um indivíduo em um grupo de apoio ao paciente (por exemplo, grupo de apoio ao câncer), Vigilantes do Peso, Alcoólicos Anônimos ou outros grupos de autoajuda e apoio com um objetivo relacionado à saúde; e a mera menção do fato de que alguém está doente em um contexto de emprego são todos dados relativos à saúde de indivíduos em questão (Eduardo Tomasevicius Filho, José Luiz de Moura Faleiros Júnior, Pedro Dalese, Pietra Daneluzzi Quinelato, Amanda Thereza Lenci Paccola, GDPR regulamento geral sobre a proteção...)[42]

Ao olhar especificamente para os Estados-Membros, pode-se encontrar na Lei portuguesa n.º 12/2005, em seu artigo 3.º, que a informação de saúde é propriedade da pessoa, e essas informações incluem os dados clínicos registados, resultados de análises e outros exames subsidiários, intervenções e diagnósticos, e obriga as unidades do sistema de saúde que no caso ao fazer o tratamento dos dados se tornam os depositários da informação. Ademais, essas informações não poderão ser utilizadas para outros fins que não os relacionados a prestação de cuidados e a investigação em saúde e outros por ventura estabelecidos pela lei.

O mesmo artigo assegura ao titular o direito de acesso integral ao seu processo clínico, diretamente ou por intermédio de uma pessoa por ele indicada. No entanto, esse acesso poderá ser restringido nos casos em que exista risco justificado de prejuízo à saúde do próprio titular, cabendo tal avaliação a um profissional habilitado. A legislação também determina que o acesso aos dados clínicos, seja pelo titular ou por terceiros com o seu

---

[42] TOMASEVICIUS FILHO, Eduardo et al. ***GDPR regulamento geral sobre a proteção de dados da União Europeia: análise de casos sobre a aplicação de sanções administrativas***. Indaiatuba, SP: Foco, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 19 jul. 2025.

consentimento, deve ocorrer por meio de um médico escolhido pelo próprio titular, com competência legal para interpretar e repassar a informação.

Já o artigo 4.º da Lei portuguesa n.º 12/2005 impõe ao responsável pelo tratamento da informação a adoção de medidas técnicas e organizativas adequadas para garantir a confidencialidade e a segurança desses dados. Isso inclui o controle de acesso, a proteção das instalações e equipamentos, o reforço do dever de sigilo profissional e a formação ética e deontológica dos profissionais de saúde, com base no compromisso ético da profissão em respeitar a privacidade e os direitos dos pacientes.

Na GDPR, contudo, o tratamento de dados sensíveis é proibido pelo art. 9º, 1, e é apenas lícito em algumas situações, presentes em seu art. 9º, 2, dentre as quais duas hipóteses não foram incluídas pela lei brasileira: “dados tornados públicos pelo titular” e “dados relativos a atuais ou ex-membros de fundações, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com medidas de segurança apropriadas”. Restringindo-se ao setor da saúde, seis dessas hipóteses são aplicáveis:

1. O titular dos dados deu consentimento explícito para o tratamento de seus dados de saúde para uma ou mais finalidades específicas.

2. O tratamento é necessário para cumprimento de obrigações trabalhistas, previdenciárias ou assistenciais, previstas em leis da União Europeia ou dos Estados-Membros.

3. O tratamento é necessário para proteger interesses vitais do titular dos dados ou de outra pessoa, quando o titular está incapaz física ou legalmente de consentir.

4. O tratamento é necessário por razões de interesse público substancial, com base em lei da UE ou do Estado-Membro, devendo respeitar os direitos fundamentais e prever medidas específicas de proteção.

5. O tratamento é necessário para fins de medicina preventiva ou ocupacional, avaliação da capacidade laboral, diagnóstico médico, prestação de cuidados de saúde ou sociais, ou gestão desses sistemas, com base em lei ou contrato com profissional de saúde.

   O tratamento é necessário por interesse público na área da saúde pública, como

controle de ameaças sanitárias, garantia da qualidade e segurança de medicamentos e dispositivos médicos.

6. O tratamento é necessário para pesquisa científica ou histórica, estatísticas ou arquivamento de interesse público, de acordo com o artigo 89(1) do GDPR, com garantias adequadas aos direitos do titular.

A alínea "a" do artigo 9º, §2º, prevê que o tratamento de dados sensíveis será lícito se o titular tiver dado consentimento explícito para uma ou mais finalidades específicas. Esse consentimento deve ser inequívoco, informado, e dado livremente, com linguagem clara e acessível. Portanto, enquanto na alínea "a" a proteção decorre da vontade informada do titular, na alínea "h" decorre da função e dever do profissional de saúde, que atua sob responsabilidade ética e legal.

Nos "considerandos" do GDPR, a explicação (51) estatui que "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".

Além disso, no comentário (71) do GDPR, fica consignado que "[...] o responsável pelo tratamento deverá (...) proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos".

Já o artigo 9, 2, alínea h), do Regulamento Geral sobre a Proteção de Dados permite o tratamento de dados médicos quando tal for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços de saúde. Porém, o tratamento só é admissível se for realizado por um profissional de saúde sujeito a uma obrigação de segredo profissional ou por outra pessoa sujeita a uma obrigação equivalente, com base em lei ou contrato com profissional de saúde. Logo, depois do consentimento, é uma das bases legais mais importantes no setor privado. É

relevante mencionar aqui que essa alínea é extremamente importante, uma vez que serve como base para a hipótese do Art. 11, II, f da LGPD.

O artigo 9 do GDPR, por outro lado, tem um sentido parecido com o Art 11, II, e, da LGPD, hipótese de utilizar-se da base legal da proteção da vida ou da incolumidade física do titular ou de terceiro, ou seja, aplica-se em casos de urgência em que o titular dos dados esteja inconsciente e incapaz de consentir.

Capítulo 4: Direito Comparado e Aplicação Prática na União Europeia

Considerando que este trabalho se limita à análise do tratamento de dados pessoais sensíveis no setor privado, optou-se por restringir a análise às bases legais aplicáveis a agentes privados que prestam cuidados diretos ao paciente, como clínicas, consultórios, laboratórios e hospitais particulares. Foram, portanto, excluídas hipóteses voltadas a políticas públicas de saúde e à atuação de autoridades públicas, ainda que previstas no GDPR.

4.1 Análise do relatório da Comissão Europeia

Um relatório intitulado *"Assessment of the EU Member States' rules on health data in the light of GDPR"*, publicado pela Comissão Europeia, revelou que, apesar de o GDPR buscar uma uniformização normativa, os Estados-Membros adotam combinações variadas de bases legais para legitimar o tratamento de dados de saúde. Entre essas bases, destaca-se o uso combinado do art. 6(1)(c) do GDPR que permite o tratamento quando necessário para o cumprimento de obrigação legal do controlador com o art. 9(2)(h) que autoriza o tratamento de categorias especiais de dados (como os de saúde) para finalidades de medicina preventiva, diagnóstico médico ou gestão de sistemas e serviços de saúde, desde que realizados por profissionais sujeitos ao sigilo legal.

No contexto do setor privado, especialmente quando não há lei nacional que imponha obrigações específicas a essas instituições, muitos países exigem o uso do consentimento explícito como base jurídica para o tratamento e o compartilhamento de

dados de saúde. Essa hipótese está prevista no art. 6(1)(a) do GDPR, segundo o qual o tratamento é lícito quando o titular "tiver dado o seu consentimento para o tratamento de seus dados pessoais para uma ou mais finalidades específicas". Tratando-se de dados sensíveis, como os de saúde, esse consentimento deve ser ainda mais qualificado, nos termos do art. 9(2)(a), que exige que o titular "tenha dado consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas".

Embora o consentimento seja amplamente utilizado no setor privado, o relatório europeu destaca que ele não é a base jurídica predominante, mas sim uma dentre as possíveis salvaguardas. Isso se deve ao fato de que, na relação médico-paciente, o consentimento pode não ser verdadeiramente livre, já que o titular pode sentir-se compelido a consentir para receber o tratamento necessário. Essa preocupação foi abordada pelo Comitê Europeu de Proteção de Dados (EDPB) nas suas Diretrizes 05/2020, que estabelecem que *"o consentimento só é válido quando o titular tiver uma escolha real e não sofrer nenhuma consequência negativa se optar por não consentir"*[43]. Ou seja, se o paciente não tiver como recusar sem colocar em risco o próprio atendimento médico, o consentimento obtido pode ser considerado inválido.

Na prática, isso significa que, em países onde não há base legal específica regulando a atuação de prestadores privados de saúde, o uso do consentimento é necessário, porém insuficiente por si só exigindo que os controladores demonstrem que houve efetiva liberdade de escolha por parte do titular. Além disso, o relatório indica que, mesmo em países que adotam o consentimento como base legal principal como Bélgica, Alemanha, França e Países Baixos, muitas vezes ele é utilizado em conjunto com outras bases legais, como obrigação contratual ou até legítimo interesse, quando cabível, para reforçar a licitude do tratamento.

4.2 Estudo de caso: fiscalização na Suécia e a exigência de DPIA

Em dezembro de 2020, a Autoridade Sueca de Proteção de Dados (IMY) concluiu uma auditoria conduzida em oito prestadores de serviços de saúde, a fim de verificar a

[43] EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 05/2020 on consent under Regulation 2016/679**. 4 May 2020. Disponível em: https://edpb.europa.eu/our-work-tools/documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. Acesso em: 21 jul. 2025.

conformidade com o GDPR no tocante à segurança no acesso a prontuários eletrônicos. A investigação revelou que sete das oito instituições não haviam realizado a análise prévia de riscos e necessidades (*Data Protection Impact Assessment* – DPIA) exigida antes de conceder autorizações de acesso a dados de saúde.[44]

Na prática, constatou-se que funcionários tinham acesso irrestrito a informações sensíveis de pacientes, sem qualquer justificativa baseada na função exercida. Essa omissão resultou em multas administrativas severas – variando entre 2,5 e 30 milhões de coroas suecas – fundamentadas na violação do art. 35 do GDPR, que torna obrigatória a realização de uma DPIA sempre que o tratamento de dados (especialmente sensíveis) puder representar alto risco aos direitos e liberdades fundamentais dos titulares.

A autoridade destacou ainda que o simples fato de não realizar a DPIA já constitui infração autônoma, mesmo que nenhuma violação concreta de dados tenha ocorrido, reforçando o caráter preventivo e proativo do modelo europeu de proteção de dados pessoais, centrado no princípio da responsabilização (accountability) e na adoção de medidas organizacionais ex ante[^21].

No Brasil, a Lei nº 13.709/2018 (LGPD) também prevê o instrumento do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), definido no art. 5º, XVII, como um documento que descreve os processos de tratamento de dados pessoais que podem gerar riscos aos direitos fundamentais dos titulares, bem como as medidas adotadas para mitigar esses riscos.

Contudo, diferentemente do GDPR, a LGPD não impõe a obrigatoriedade de elaboração do relatório em nenhuma situação concreta pré-definida – nem mesmo no tratamento de dados sensíveis no setor da saúde, que notoriamente envolve alto grau de risco e vulnerabilidade. O art. 38 da LGPD apenas faculta à Autoridade Nacional de Proteção de Dados (ANPD) a requisição do relatório em casos específicos, sem apresentar critérios objetivos ou automáticos.

Como apontam Margareth Zaganelli e Douglas Binda Filho, essa lacuna normativa compromete a efetividade da proteção e fragiliza a governança de dados nas instituições de

---

[44] EUROPEAN DATA PROTECTION BOARD. *Deficiencies in how healthcare providers control staff access to patient journal data*. 7 dez. 2020. Disponível em: https://www.edpb.europa.eu/news/national-news/2020/deficiencies-how-healthcare-providers-control-staff-access-patient-journal_en. Acesso em: 21 jul. 2025.

saúde, que muitas vezes operam sem parâmetros claros de conformidade. Além disso, enquanto o GDPR define expressamente os elementos mínimos que devem constar de uma avaliação de impacto (art. 35, §7º), a LGPD é omissa quanto ao conteúdo obrigatório do RIPD, delegando à ANPD a missão de futuramente regulamentar o tema. Esse cenário demonstra uma assimetria significativa entre os dois sistemas: o GDPR apresenta exigências normativas robustas, procedimentos claros e sanções proporcionais, enquanto a LGPD ainda caminha em direção a uma consolidação interpretativa, especialmente em setores de alta sensibilidade como a saúde[45].

4.3 Relatório de Impacto: diferenças de abordagem entre GDPR e LGPD

Como visto, o GDPR adota postura proativa em relação à avaliação de impacto (DPIA) exigindo-a de forma obrigatória em diversos cenários de alto risco, incluindo tratamentos em larga escala de dados sensíveis de saúde. Essa obrigação legal, combinada com a ameaça de sanções significativas, faz com que os agentes de tratamento na Europa incorporem a DPIA como parte integrante dos seus programas de compliance e gestão de riscos. Já a LGPD, embora conceitue o RIPD e o reconheça como ferramenta importante, não tornou sua elaboração mandatória em nenhum caso específico, colocando-o mais como um instrumento a ser eventualmente requisitado pela ANPD.

Na prática, essa diferença de abordagem implica que, no Brasil, muitos controladores do setor saúde podem acabar deixando de avaliar preventivamente os riscos de seus tratamentos de dados, por não haver uma imposição expressa na lei. Enquanto isso, na UE, mesmo hospitais e clínicas privadas precisam justificar formalmente, por meio de DPIAs, as medidas de segurança adotadas para proteger os dados sensíveis dos pacientes – sobretudo quando implementam novos sistemas eletrônicos de prontuário, telemedicina, aplicativos de saúde etc.

Ademais, a ausência, na LGPD, de parâmetros detalhados sobre o conteúdo do RIPD, transfere para a futura regulamentação infralegal (pela ANPD) a tarefa de preencher essas lacunas. Até que isso ocorra, permanece uma zona de incerteza quanto ao que

[45] ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis. ***A Lei Geral de Proteção de Dados e suas implicações na saúde: as Avaliações de Impacto no tratamento de dados no âmbito clínico-hospitalar.*** Revista de Bioética y Derecho, n. 54, p. 215–232, 2022. DOI: 10.1344/rbd2021.54.36005.

exatamente se espera de um relatório de impacto no contexto nacional. Em contraste, as orientações do EDPB na Europa e o próprio texto do GDPR já delineiam, com alguma precisão, os elementos que uma DPIA deve conter (descrição dos tratamentos e finalidades, avaliação da necessidade e proporcionalidade, gerenciamento dos riscos e medidas de mitigação, entre outros).

Em resumo, o modelo europeu enfatiza a prevenção e a prestação de contas antecipada (exigindo DPIA sempre que cabível), enquanto o modelo brasileiro, por ora, confia na atuação ex post da ANPD, requisitando relatórios caso a caso. Essa diferença reflete estágios distintos de maturidade regulatória e de cultura de proteção de dados entre os dois contextos.

4.4 Precedentes relevantes da Corte Europeia de Direitos Humanos no setor da saúde

A jurisprudência da Corte Europeia de Direitos Humanos (European Court of Human Rights – ECtHR), vinculada ao Conselho da Europa, tem desempenhado papel essencial na consolidação de padrões internacionais de proteção de dados sensíveis, especialmente no setor da saúde. A ECtHR atua como instância supranacional que julga Estados que, mesmo possuindo legislações próprias, falharam em garantir os direitos assegurados pela Convenção Europeia de Direitos Humanos – sobretudo o direito à vida privada (art. 8º). Abaixo, apresentam-se três precedentes paradigmáticos cujas decisões moldaram a interpretação contemporânea sobre confidencialidade médica, segurança da informação e dever estatal de prevenção e reparação:

Em I. v. Finlândia (2008): uma enfermeira soropositiva teve seu prontuário médico acessado indevidamente por diversos colegas de trabalho, sem consentimento e sem justificativa funcional. Mesmo após denúncia às autoridades locais, nenhuma medida efetiva foi tomada para sancionar ou impedir tal acesso. O TEDH entendeu que a mera falta de barreiras técnicas eficazes para impedir o acesso não autorizado a dados de saúde já configurava violação ao artigo 8º da Convenção Europeia, que protege a vida privada. Esse caso reforçou o entendimento de que os Estados têm a obrigação positiva de adotar medidas técnicas e organizacionais capazes de prevenir o acesso indevido a informações de saúde –

não bastando reagir após a violação, mas devendo impedir que ela ocorra. (I. v. Finland, App. no. 20511/03, ECtHR, 17 July 2008).

O precedente Mockutė v. Lituânia (2018): envolveu a divulgação, pela direção de um hospital psiquiátrico, de informações acerca do tratamento de uma paciente internada compulsoriamente, repassadas indevidamente à imprensa. As autoridades nacionais alegaram "interesse público" para justificar a exposição da paciente, cuja identidade e detalhes terapêuticos foram revelados sem consentimento. O TEDH condenou a Lituânia, afirmando que dados sobre saúde mental são extremamente sensíveis e que o Estado tem o dever de proteger a privacidade do paciente, inclusive contra divulgações não autorizadas por parte de agentes estatais. Reiterou-se que, além de punir ex post facto os responsáveis, o Estado deve estabelecer salvaguardas *ex ante* para evitar violações desse tipo. (Mockutė v. Lithuania, App. no. 66490/09, ECtHR, 27 February 2018).

No caso C.C. v. Espanha (2013): a questão aqui foi a publicação, em um acórdão judicial acessível ao público, do nome completo de um paciente vivendo com HIV, em um processo no qual figurava como parte. As instâncias espanholas não atenderam ao pedido do interessado para anonimizar sua identidade nos autos, resultando na revelação pública de sua condição de saúde. O TEDH entendeu que a Espanha violou o direito à vida privada do requerente, pois não ponderou adequadamente a necessidade de proteger sua identidade e saúde frente ao princípio da publicidade judicial. Destacou que, ao lidarem com dados sensíveis de saúde em decisões ou documentos públicos, os Estados devem aplicar técnicas de anonimização ou sigilo quando possível, para evitar danos irreparáveis à pessoa.

Os precedentes acima são vinculantes para os Estados condenados e servem de guia interpretativo para todos os membros do Conselho da Europa. Eles explicitam deveres como: assegurar confidencialidade efetiva em ambientes hospitalares (com controles de acesso); proteger identidades de pacientes em divulgações públicas (sejam midiáticas ou judiciais); e garantir recursos efetivos para vítimas de violações. Tais parâmetros influenciam diretamente o desenvolvimento legislativo e a atuação de autoridades de proteção de dados na Europa – e, por extensão, inspiram melhorias em outras jurisdições, inclusive no Brasil. Em última análise, a jurisprudência europeia evidencia que a responsabilidade pela proteção de dados de saúde é compartilhada entre agentes privados e

o Estado: cabe a este último fiscalizar, regulamentar e, se necessário, responder pelas omissões que permitam violações a direitos fundamentais dos pacientes.

CONCLUSÃO

Em síntese, os objetivos específicos delineados no início do trabalho foram integralmente alcançados, e os resultados confirmam a hipótese central da pesquisa. A análise comparativa demonstrou que não há completa uniformidade entre os Estados-Membros da União Europeia quanto às bases jurídicas predominantes para o tratamento e compartilhamento de dados de saúde no setor privado. As variações decorrem não apenas de diferenças legislativas nacionais, mas também da natureza dos prestadores, do tipo de dado tratado e das características de cada sistema de saúde.

No Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) também prevê bases legais específicas para o tratamento de dados sensíveis (art. 11). Contudo, não admite, no setor privado, hipóteses amplas baseadas em interesse público em saúde ou em obrigação legal ligada à organização dos serviços de saúde, possibilidades presentes em diversos países europeus. Assim, clínicas privadas brasileiras, via de regra, precisam obter consentimento expresso do titular ou enquadrar-se na hipótese restrita de tutela da saúde, prevista no art. 11, II, *f*, quando o tratamento é realizado por profissional ou serviço da área médica.

O objetivo geral de analisar, sob a perspectiva do direito comparado, a tutela jurídica dos dados pessoais sensíveis no setor privado da saúde, à luz da LGPD e do GDPR, foi atingido. Da mesma forma, os objetivos específicos foram atendidos: A) Mapear as bases legais previstas em cada legislação (Cap. 3 e 4); B) Identificar o papel do consentimento e suas limitações práticas (Cap. 3); C) Examinar a jurisprudência europeia, como os casos *Z. vs Finlândia*, *I. vs Finlândia*, *Mockutė v. Lituânia* e *C.C. v. Espanha*, que consolidam padrões protetivos (Cap. 4); D) Apontar desafios e lacunas da LGPD, como a ausência de obrigatoriedade de Relatórios de Impacto (RIPD) em atividades de alto risco (Cap. 4).

Apesar de representar um avanço expressivo, a LGPD ainda apresenta lacunas significativas em relação ao modelo europeu, especialmente pela falta de obrigatoriedade

de RIPD para operações de alto risco, pela imprecisão sobre algumas bases legais aplicáveis no setor privado de saúde e pela fragilidade na regulamentação do consentimento e do dever de confidencialidade. Ressalta-se que a proteção de dados pessoais foi reconhecida como direito fundamental com a inclusão do inciso LXXIX no art. 5º da Constituição Federal pela Emenda Constitucional nº 115/2022, reforçando a centralidade desse direito no ordenamento brasileiro.

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) é essencial para a consolidação do sistema. Sua transformação em autarquia especial pela Lei nº 14.460/2022 conferiu maior autonomia técnica e decisória. Nos últimos anos, a ANPD avançou na edição de normas, como a Resolução CD/ANPD nº 2/2023, que estabelece critérios de aplicação de sanções administrativas, e a Portaria nº 41/2024, que aprovou a Agenda Regulatória 2025-2026, prevendo a regulamentação específica para setores sensíveis, como saúde, uso de inteligência artificial e dados de crianças e adolescentes.

Além disso, em 2023, foram publicadas diretrizes preliminares para elaboração de Relatórios de Impacto à Proteção de Dados (RIPD), sinalizando evolução no alinhamento do Brasil às melhores práticas internacionais.

Diante desse cenário, conclui-se que o Brasil ainda se encontra em fase de consolidação normativa e institucional. É necessário fortalecer a atuação fiscalizatória da ANPD, desenvolver regulamentações específicas para o setor de saúde privado, estimular a obrigatoriedade de RIPD em operações de alto risco, além de promover capacitação contínua de agentes de tratamento para assegurar a efetividade da proteção de dados sensíveis.

A comparação com o GDPR e a análise da jurisprudência europeia forneceram modelos concretos de responsabilização e boas práticas, que podem servir de referência para o ordenamento brasileiro. Assim, o país pode evoluir rumo a um sistema equilibrado, capaz de proteger os titulares de dados e, ao mesmo tempo, garantir segurança jurídica e eficiência às atividades médico-assistenciais.

Por fim, reconhece-se que este trabalho possui limitações, por ter se concentrado exclusivamente no tratamento de dados de pessoas maiores de idade e nas normativas vigentes até 2024. Para pesquisas futuras, sugerem-se três frentes: A)Proteção de dados de crianças e adolescentes, tema que exige regulamentação e salvaguardas adicionais; B)

Impacto da inteligência artificial e do big data na coleta e uso de dados sensíveis, considerando riscos de perfilamento e decisões automatizadas; C) Interoperabilidade de dados de saúde entre sistemas públicos e privados, buscando o equilíbrio entre eficiência no atendimento médico e proteção efetiva da privacidade.

A efetivação dos direitos fundamentais à intimidade, dignidade e autodeterminação informativa depende de uma estrutura regulatória sólida e de agentes privados comprometidos com o cumprimento da LGPD. A experiência europeia, aliada à crescente atuação da ANPD, fornece parâmetros valiosos para que o Brasil avance na construção de um ambiente seguro, ético e eficiente para o tratamento de dados sensíveis de saúde no setor privado.

REFERÊNCIAS

ALBUQUERQUE, Leonardo Neves de. A evolução histórica, normativa e judicial da proteção de dados: um estudo sobre a influência dos padrões europeus sobre a LGPD. Rio de Janeiro: Lumen Juris, 2021.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Portaria nº 41, de 24 de janeiro de 2024. **Aprova a Agenda Regulatória da Autoridade Nacional de Proteção de Dados para o biênio 2025-2026**. *Diário Oficial da União*, Brasília, DF, 25 jan. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/portaria_41_2024_agenda_regulatoria_2025_2026. Acesso em: 25 mai. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 2, de 27 de janeiro de 2023. **Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas**. *Diário Oficial da União*, Brasília, DF, 27 jan. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/resolucao_cd_anpd_2_2023.pdf. Acesso em: 25 mai. 2024.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. [Constituição (1988)]. ***Constituição da República Federativa do Brasil de 1988***. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 mai. 2024.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para dispor sobre a competência da União para legislar sobre proteção e tratamento de dados pessoais**. *Diário Oficial da União*, Brasília, DF, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 25 mai. 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 25 mai. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 mai. 2024.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018 (**Lei Geral de Proteção de Dados Pessoais), para transformar a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de regime especial**. *Diário Oficial da União*, Brasília, DF, 26 out. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em: 25 mai. 2024.

CONFEDERAÇÃO NACIONAL DE SAÚDE (CNSaúde)**. *Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde***. Brasília, DF: CNSaúde, 2021.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.605, de 15 de setembro de 2009. **Dispõe sobre a confidencialidade das informações contidas nos prontuários médicos.** *Diário Oficial da União*, Brasília, DF, 15 set. 2009. Disponível em: https://portal.cfm.org.br/index.php?option=com_content&view=article&id=21453:resolucao-cfm-n-1605-2009&catid=3. Acesso em: 25 mai. 2024.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 1.821, de 23 de novembro de 2007. **Aprova as normas técnicas para a digitalização e o uso de sistemas informatizados para a guarda e manuseio dos prontuários de pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde**. *Diário Oficial da União*, Brasília, DF, 27 nov. 2007. Disponível em: https://portal.cfm.org.br/index.php?option=com_content&view=article&id=21469:resolucao-cfm-n-1821-2007&catid=3. Acesso em: 25 mai. 2024.

CONSELHO DA EUROPA. ***Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108)***. Estrasburgo, 28 jan. 1981. (Modernizada pelo Protocolo de Alteração de 2018).

CONSELHO DA EUROPA; AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (FRA). ***Manual da Legislação Europeia sobre Proteção de Dados.*** **Luxemburgo: Serviço das Publicações da União Europeia, 2018**. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-data-protection-law_pt.pdf. Acesso em: 25 mai. 2024.

COURT OF JUSTICE OF THE EUROPEAN UNION (TJUE). ***Judgment of the Court (Grand Chamber) of 6 November 2003. Bodil Lindqvist. Reference for a preliminary ruling: Kammarrätten i Jönköping - Sweden. Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Concepts of "personal data", "data relating to health", "processing of personal data", "file", "public file", "recipient" and "transfer of personal data to a third country" - Publication on the Internet of personal data concerning persons working in a parish***. Case C-101/01. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101. Acesso em: 25 mai. 2024.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis (Ed.). ***General Data Protection Regulation, Article-by-Article Commentary***. Baden-Baden: Nomos; Oxford: Hart, 2021.

DE TEFFÉ, Chiara Spadaccini. **Dati sensibili e privacy in sanità.** ***Chiarini.com***, [s.d.]. Disponível em: https://www.chiarini.com/privacy-sanita/. Acesso em: 25 mai. 2025.

DE TEFFÉ, Chiara Spadaccini. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. 1. ed. Indaiatuba: Editora Foco, 2022.

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados***. 3. ed. São Paulo: Revista dos Tribunais, 2021.
EUROPEAN COMMISSION. Directorate-General for Health and Food Safety. ***Assessment of the EU Member States' rules on health data in the light of GDPR.*** Brussels: European Commission, 2021. Disponível em: https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en. Acesso em: 25 julho. 2025.
EUROPEAN COURT OF HUMAN RIGHTS (ECtHR). ***Casado Coca v. Spain*****. Application no. 15450/89**. Judgment of 24 February 1994. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57866. Acesso em: 25 mai. 2025.

EUROPEAN COURT OF HUMAN RIGHTS (ECtHR). ***I. v. Finland***. Application no. 20511/03. Judgment of 17 July 2008. Disponível em: https://hudoc.echr.coe.int/eng?i=001-87614. Acesso em: 25 mai. 2025.

EUROPEAN COURT OF HUMAN RIGHTS (ECtHR). ***Mockutė v. Lithuania***. Application no. 66490/09. Judgment of 27 February 2018. Disponível em: https://hudoc.echr.coe.int/eng?i=001-180862. Acesso em: 25 mai. 2025.

EUROPEAN COURT OF HUMAN RIGHTS (ECtHR). ***Z v. Finland***. Application no. 22009/93. Judgment of 25 February 1997. Disponível em: https://hudoc.echr.coe.int/eng?i=002-9432. Acesso em: 25 mai. 2025.

EUROPEAN DATA PROTECTION BOARD (EDPB). ***Guidelines 05/2020 on consent under Regulation 2016/679***. Version 1.1. Adopted on 4 May 2020. Disponível em: https://edpb.europa.eu/our-work-tools/documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. Acesso em: 25 mai. 2025.

FRIEDMAN, Lawrence M. *The Republic of Choice: Law, Authority, and Culture*. Cambridge, MA: Harvard University Press, 1990.

GOMES, Joaquim Benedito Barbosa. Autodeterminação informativa e proteção de dados pessoais. In: PFEIFFER, Roberto; DONEDA, Danilo; GICO JUNIOR, Ivo Teixeira (orgs.). *Direitos da personalidade, proteção de dados e novas tecnologias*. São Paulo: Thomson Reuters Brasil, 2020.

INSIDEPRIVACY. *Special Category Data by Inference: CJEU significantly expands the scope of Article 9 GDPR*. 2022. Disponível em: https://www.insideprivacy.com/eu-data-protection/special-category-data-by-inference-cjeu-significantly-expands-the-scope-of-article-9-gdpr/. Acesso em: 8 ago. 2025.

KUNER, Christopher; GKOTSOPOULOUS, Olga. *Article 9. Processing of special categories of personal data*. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (ed.). *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*. Oxford: Oxford University Press, 2021

MALHEIROS, Pablo [et al].Direito Civil e Tecnologia. Belo Horizonte: Fórum, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. REVISTA DE DIREITO DO CONSUMIDOR, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. REVISTA DE DIREITO DO CONSUMIDOR, 2018.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor, linhas gerais de um novo direito fundamental. 1. ed. São Paulo, Saraiva, 2014.

MULHOLLAND, Caitlin Sampaio. Proteção de dados pessoais sensíveis: conceito e tratamento. *Revista Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

PIZARRO, Ramón Daniel. ***Derecho A La Intimidad*.** Buenos Aires: Rubinzal - Culzoni Editores, 2012.

PORTUGAL. Lei n.º 12/2005, de 26 de janeiro. **Lei da Proteção de Dados Pessoais.** ***Diário da República***, I Série-A, n.º 18, 26 jan. 2005. Disponível em: https://www.cnpd.pt/media/x4l2i01t/lei_12_2005.pdf. Acesso em: 25 mai. 2024.

QUINN, Paul; MALGIERI, Gianclaudio. *The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework*. German Law Journal, Cambridge University Press, v. 22, p. 1583–1612, 2021. DOI: https://doi.org/10.1017/glj.2021.79.

RODOTÀ, Stefano. *Il diritto di avere diritti*. Roma: Laterza, 2012.

ROSEN, Jeffrey. ***The Unwanted Gaze: The Destruction of Privacy in America.*** New York: Vintage Books, 2001.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. *Direitos Fundamentais e Justiça*, Belo Horizonte, v. 14, n. 42, jan./jun. 2020.

SOARES, Flaviana Rampazzo. **Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade**. *Revista IBERC*, v. 4, n. 2, p. 18-46, maio/ago. 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org. Acesso em: 25 mai. 2025.

TOMASEVICIUS FILHO, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura (coord.); DALESE, Pedro (colab.); QUINELATO, Pietra Daneluzzi; PACCOLA, Amanda Thereza Lenci. ***GDPR regulamento geral sobre a proteção de dados da União Europeia: análise de casos sobre a aplicação de sanções administrativas***. Indaiatuba, SP: Foco, 2023.

TZANOU, Maria. *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing, 2013.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. *Jornal Oficial da União Europeia*, L 281, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046. Acesso em: 25 mai. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que**

diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 25 mai. 2025.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy.** ***Harvard Law Revie****w*, Cambridge, MA, v. 4, n. 5, p. 193-220, 15 dez. 1890.

WESTIN, Alan F. ***Privacy and Freedom***. New York: Ig Publishing, 2015.

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder***. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2019.