LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DA SAÚDE: PREVENÇÃO E PUNIÇÃO DE CONDUTAS ILÍCITAS

GENERAL DATA PROTECTION LAW IN THE HEALTHCARE SECTOR: PREVENTION AND PUNISHMENT OF UNLAWFUL CONDUCT

DOI: 10.19135/revista.consinter.00022.13
Recebido/Received 31/07/2025 – Aprovado/Approved 15/12/2025

Luiz Augusto Coutinho[1] *– https://orcid.org/0000-0002-1341-3838*
Leila Fraga Coutinho[2] *– https://orcid.org/0009-0005-9174-8210*

Resumo

O presente estudo analisa, sob o enfoque jurídico-penal, a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor da saúde, com especial atenção à proteção de dados sensíveis e à responsabilização por condutas ilícitas. Considerando a crescente digitalização dos serviços de saúde e o volume expressivo de dados pessoais tratados por hospitais, clínicas, operadoras de planos e plataformas digitais, destaca-se a relevância da LGPD como norma estruturante da proteção da intimidade e da privacidade na era da saúde digital. Com a constitucionalização da proteção de dados por meio da Emenda Constitucional 115/2022, o artigo investiga o papel da LGPD não apenas como instrumento regulatório, mas como parâmetro de ilicitude penal. Explora-se a responsabilidade de gestores e profissionais da saúde à luz do art. 13, § 2º do Código Penal e dos princípios da LGPD, relacionando-os a tipos penais já previstos, como violação de segredo, estelionato eletrônico e crimes contra a vida em contextos de falha de segurança. A metodologia utilizada é qualitativa, com base em pesquisa bibliográfica e documental, analisando contribuições doutrinárias, jurisprudência atualizada do STJ e normas da ANPD. O trabalho conclui que a LGPD opera como um mecanismo transversal de compliance e de imputação penal em ambientes de alto risco como o setor da saúde, exigindo a consolidação de uma cultura institucional de proteção de dados e responsabilização efetiva.

---

[1] Luiz Augusto Coutinho é advogado criminal, Conselheiro Federal da OAB, Pós-Doutor em Democracia e Direitos Humanos – Ius Gentium Coimbra (2021-2022). Doutor em Ciências Jurídico-Sociais – Universidad del Museo Social Argentino (2012-2015) e Professor na Universidade Católica do Salvador (UCSal) e na Academia da Polícia Militar da Bahia (APM), Salvador – Bahia – Brasil. E-mail: luizcoutinho@compos.com.br Orcid: https://orcid.org/0000-0002-1341-3838.

[2] Leila Fraga Coutinho é advogada sanitarista e médica veterinária. Especialista em Direito Sanitário pela UNICAMP e especialista em Saúde Coletiva, concentração em gestão pública municipal pela UFBA. Membro da Comissão Especial de Direito à Saúde do Conselho Federal da OAB. E-mail: leilafraga@gmail.com Orcid: https://orcid.org/0009-0005-9174-8210.

Declaração sobre o uso de IA: Os autores declaram que, durante a elaboração deste artigo, utilizaram ferramentas de Inteligência Artificial (ChatGPT da OpenAI e Gemini do Google) com o objetivo de aprimorar a clareza, a coesão e a qualidade linguística do manuscrito. Todo o conteúdo gerado por essa tecnologia foi cuidadosamente revisado e editado pelos autores, que assumem integralmente a responsabilidade pela precisão, integridade e confiabilidade das informações apresentadas..

Palavras-chave: LGPD. Saúde digital. Dado sensível. Direito penal. Responsabilidade. Privacidade.

Abstract

This study analyzes, from a criminal law perspective, the application of the General Personal Data Protection Law (LGPD) in the healthcare sector, with a special focus on the protection of sensitive data and accountability for unlawful conduct. Considering the increasing digitization of healthcare services and the significant volume of personal data processed by hospitals, clinics, health insurance providers, and digital platforms, the relevance of the LGPD as a structuring norm for the protection of privacy in the era of digital healthcare is highlighted. With the constitutionalization of data protection through Constitutional Amendment No. 115/2022, the article investigates the role of the LGPD not only as a regulatory instrument, but also as a parameter of criminal illegality. It explores the responsibility of healthcare managers and professionals in light of Article 13, § 2 of the Penal Code and the principles of the LGPD, relating them to existing criminal offenses, such as breach of confidentiality, electronic fraud, and crimes against life in contexts of security breaches. The methodology used is qualitative, based on bibliographic and documentary research, analyzing doctrinal contributions, updated jurisprudence of the STJ, and ANPD standards. The study concludes that the LGPD operates as a cross-cutting mechanism for compliance and criminal prosecution in high-risk environments such as the healthcare sector, requiring the consolidation of an institutional culture of data protection and effective accountability.

Keywords: LGPD. Digital health. Sensitive data. Criminal law. Accountability. Privacy.

1 INTRODUÇÃO

A revolução tecnológica no campo da saúde intensificou a utilização de ferramentas digitais para coleta, armazenamento e compartilhamento de dados clínicos, expondo pacientes a riscos complexos relacionados à violação da privacidade e à utilização indevida de informações sensíveis. Nesse cenário, a proteção de dados pessoais emerge como uma necessidade imperiosa, especialmente diante da assimetria informacional existente entre titulares e agentes de tratamento. A promulgação da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – e a elevação da proteção de dados pessoais à categoria de Direito Fundamental pela Emenda Constitucional 115/2022 revelam o reconhecimento estatal da urgência em tutelar a autodeterminação informativa no Brasil. Como destaca Doneda[3], "a proteção de dados pessoais não é apenas uma extensão da privacidade, mas um direito autônomo vinculado à dignidade da pessoa humana".

Nesse contexto, a proteção de dados sensíveis de saúde assume relevância constitucional acentuada. Trata-se de categoria especial de dados cujo tratamento se

[3] DONEDA, Danilo. "Da privacidade à proteção de dados pessoais: elementos da formação da autoridade nacional". *Revista de Direito Civil Contemporâneo*, São Paulo, v. 17, p. 13-35, jan./abr. 2018..

articula diretamente com a tutela dos direitos fundamentais à saúde e à vida. Como destaca Luigi Bonizzato[4], a Constituição Federal de 1988 confere a esses bens jurídicos o mais elevado grau de proteção, impondo ao intérprete a adoção de uma hermenêutica que lhes assegure a máxima efetividade. Assim, qualquer medida estatal ou privada envolvendo dados de saúde deve observar um padrão reforçado de legitimidade, proporcionalidade e garantias de autodeterminação informativa, sob pena de vulnerar o núcleo essencial desses direitos fundamentais.

Com a incorporação da proteção de dados à Constituição Federal, a LGPD passou a funcionar não apenas como instrumento regulador, mas também como parâmetro normativo de licitude penal. Isso significa que condutas relacionadas ao tratamento ilícito de dados podem ensejar responsabilização criminal com base em dispositivos já previstos no Código Penal, como violação de segredo profissional, invasão de dispositivo informático e estelionato eletrônico. Nesse sentido, o presente estudo tem por objetivo analisar os desdobramentos penais da LGPD no setor da saúde, com especial atenção à conduta de gestores e profissionais da área, à luz dos princípios da lei e das exigências constitucionais de proteção à intimidade, dignidade e autodeterminação informativa.

Desta feita, verificou-se a responsabilidade de gestores e profissionais da saúde à luz do art. 13, § 2º do Código Penal e dos princípios da LGPD, relacionando-os com tipos penais já existentes, como violação de segredo, estelionato eletrônico e crimes contra a vida, especialmente em situações de falha de segurança. A pesquisa tem caráter qualitativo, fundamentada em análise bibliográfica e documental, considerando contribuições doutrinárias, jurisprudência atual do STJ e normas da ANPD. Conclui-se que a LGPD atua como um mecanismo transversal de compliance e de responsabilização penal em ambientes de alto risco, como o setor de saúde, sendo essencial a promoção de uma cultura institucional de proteção de dados e responsabilização efetiva.

2 METODOLOGIA

O referido estudo caracteriza-se por uma abordagem qualitativa, com cunho exploratório e descritivo, focando na análise da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor da saúde sob a perspectiva jurídico-penal. A pesquisa empregou uma metodologia bibliográfica e documental, utilizando as seguintes fontes primárias e secundárias:

1. Legislação: Lei 13.709/2018 (LGPD), Código Penal Brasileiro (Dec.-Lei 2.848/1940) e Emenda Constitucional 115/2022.
2. Doutrina Especializada: Análise de obras e artigos científicos de autores renomados nos campos do Direito Digital, Direito Penal e Direito Sanitário que abordam a proteção de dados, a responsabilidade penal e a saúde.
3. Jurisprudência: Estudo de julgados relevantes do Superior Tribunal de Justiça (STJ) que tratam da proteção de dados e da responsabilidade em

[4] BONIZZATO, Luigi. *A Constituição da Saúde e da Vida: os Direitos Fundamentais à Saúde e à Vida e o Processo de Inconstitucionalização da Lei Brasileira do Plano de Saúde.* Rio de Janeiro: Renovar, 2008.

casos de violação, com destaque para a interpretação sobre o dano moral presumido.

4. Normas e Guias da Autoridade Nacional de Proteção de Dados (ANPD): Avaliação de notas técnicas, relatórios e processos administrativos sancionadores da ANPD, que fornecem diretrizes e exemplos práticos da aplicação da LGPD no setor da saúde e em outros contextos de tratamento de dados sensíveis.

A coleta de dados foi realizada mediante levantamento e seleção de material relevante que fundamentasse a discussão sobre a interface entre a LGPD e o Direito Penal na saúde. A análise dos dados ocorreu de forma interpretativa e crítica, buscando identificar as correlações entre as condutas de violação da LGPD e os tipos penais existentes, bem como as implicações da LGPD como parâmetro de ilicitude penal e de mecanismo de *compliance*. O objetivo foi construir um arcabouço argumentativo que evidencia a responsabilização penal de gestores e profissionais de saúde diante da omissão ou negligência na proteção de dados sensíveis.

3 DADOS PESSOAIS SENSÍVEIS NA SAÚDE

A LGPD reconhece como sensíveis os dados pessoais que, em razão de seu conteúdo, possam ensejar discriminação ou violação de direitos fundamentais. No setor da saúde, esses dados são inerentemente sensíveis, pois envolvem aspectos íntimos da vida do paciente, como diagnósticos, histórico clínico, doenças preexistentes, exames laboratoriais, dados genéticos e de saúde mental. A exposição indevida dessas informações pode gerar prejuízos graves à dignidade, à integridade moral e até física do titular.

A especificidade dos dados de saúde exige do agente de tratamento, especialmente no setor médico-hospitalar, um dever de cuidado qualificado. Como observam Sarlet e Dall'Agnol[5] "o direito à intimidade e à autodeterminação informativa, especialmente na saúde, é pressuposto para o exercício pleno da dignidade da pessoa humana". Trata-se de informações que transcendem a esfera privada e exigem, por força normativa, um regime jurídico protetivo reforçado.

A vulnerabilidade estrutural do paciente frente aos detentores de seus dados impõe a necessidade de regulação rígida sobre o ciclo de vida dessas informações. Não por acaso, a LGPD[6] impõe que o tratamento de dados sensíveis só seja lícito quando fundado em hipóteses legais específicas (art. 11), exigindo, na saúde, finalidades legítimas, como a tutela da saúde por profissionais ou instituições sanitárias. O desvio de finalidade pode configurar infrações éticas, administrativas e, em determinados casos, penais.

Embora a LGPD seja aplicável universalmente, as particularidades da saúde pública (com seus sistemas centralizados, integração com o SUS e regulamentação específica) e da saúde privada (com a concorrência, o papel das operadoras e a maior

---

5 SARLET, Ingo Wolfgang; DALL'AGNOL, Darlei. "Dignidade da pessoa humana e o direito à proteção de dados pessoais". *Revista Brasileira de Bioética*, v. 15, n. 3, p. 331-348, 2019.

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

diversidade de plataformas) impõem desafios e abordagens distintas para a conformidade e a mitigação de riscos penais, que serão explorados ao longo deste trabalho.

4 A LGPD COMO INSTRUMENTO DE PREVENÇÃO DE ILÍCITOS PENAIS

Embora concebida como norma de natureza predominantemente administrativa e civil, a LGPD cumpre relevante função preventiva no campo penal. O cumprimento diligente de seus princípios, deveres e obrigações constitui uma barreira normativa contra a ocorrência de ilícitos relacionados à segurança e ao sigilo dos dados sensíveis. A proteção de dados, nesse sentido, assume papel análogo ao do compliance nas estruturas organizacionais, contribuindo para a responsabilização e a mitigação de riscos penais nas instituições de saúde.

O art. 6º da LGPD estabelece princípios orientadores que devem guiar toda e qualquer atividade de tratamento de dados pessoais, incluindo os dados sensíveis. Dentre os mais relevantes no contexto penal estão: a finalidade, a necessidade, a segurança, a prevenção e a responsabilização. Segundo Opice Blum[7] os princípios da LGPD funcionam como elementos estruturantes da conduta dos agentes de tratamento e, quando ignorados, podem caracterizar imprudência, negligência ou até dolo na conduta do agente.

A governança de dados também ocupa papel central na prevenção de ilícitos. O art. 46 da LGPD[8] impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados. Entre essas medidas incluem-se a criptografia, a gestão de acessos, o treinamento contínuo de equipes, o plano de resposta a incidentes e o relatório de impacto à proteção de dados (RIPD), previsto no art. 38. A ausência de tais controles pode indicar despreparo institucional ou omissão relevante por parte dos gestores, o que é penalmente relevante nos termos do art. 13, § 2º do Código Penal.

No contexto da responsabilização penal, Barbagalo[9] defende que a LGPD deve ser interpretada como norma de tutela penal indireta, cuja violação serve como parâmetro de ilicitude para tipos penais já existentes. A inadequação das medidas de segurança ou a manipulação de dados com desvio de finalidade, pode configurar diversos crimes previstos na parte especial do Código Penal, se houver nexo com o resultado lesivo à saúde do titular.

Nesse sentido, a LGPD atua não apenas como arcabouço regulatório, mas também como um novo paradigma de diligência. Conforme aponta Guilherme Magalhães Martins[10], a Lei impõe um dever de cuidado qualificado no tratamento de

---

7 MÁLAGONDO, Viviane Nóbrega; Blum, Renato Opice (coord.). "Lei Geral de Proteção de Dados – comentada". *Revista dos Tribunais* .2ª ed. rev., atual. e ampl. São Paulo: 2019b.

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

9 BARBAGALo, Fernando Brandini. O novo crime de fraude eletrônica e o princípio da legalidade. TJDFT, Brasília, 3 jun. 2022. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade>. Acesso em: 31 jul. 2025.

10 MARTINS, Guilherme Magalhães. *LGPD comentada: a Lei Geral de Proteção de Dados e o Regulamento Europeu (GDPR)*. 3. ed. Rio de Janeiro: Forense, 2021.

dados, cuja inobservância pode caracterizar o elemento subjetivo da culpa em determinadas condutas penalmente relevantes.

5 A VIOLAÇÃO DA LGPD E OS TIPOS PENAIS EXISTENTES

A LGPD não inaugura um novo capítulo do Direito Penal em termos de tipificação autônoma, mas atua como parâmetro de interpretação para tipos penais já existentes. Isso ocorre porque sua violação pode representar o elemento normativo de tipos como a violação de segredo profissional, invasão de dispositivo informático, estelionato eletrônico, crimes contra a honra e, em situações extremas, lesão corporal ou homicídio por omissão. A LGPD, assim, configura-se como norma de tutela penal indireta, influenciando o juízo de tipicidade e culpabilidade.

O Código Penal brasileiro já contempla dispositivos que incidem diretamente sobre condutas ilícitas envolvendo dados. O art. 154 trata da violação de segredo profissional; o art. 154-A tipifica a invasão de dispositivo informático; o art. 266 prevê a interrupção ou perturbação de serviço de utilidade pública, como sistemas hospitalares; e o art. 171, § 2º-A, introduzido pela Lei 14.155/2021, trata do estelionato cometido por meio eletrônico. Em determinados contextos, a falha grave na proteção de dados pode ensejar crimes contra a vida (art. 121) ou integridade física (art. 129), quando houver nexo causal com os resultados que estejam diretamente relacionados através da teoria da "*conditio sine qua non*".

A jurisprudência do Superior Tribunal de Justiça tem reconhecido a gravidade das falhas na proteção de dados, inclusive admitindo o dano moral presumido em casos de vazamento de dados sensíveis, como decidido no REsp 2.121.904/SP[11]. Essa interpretação contribui como reforço argumentativo para a aferição da responsabilidade penal, especialmente nos casos em que a falha é reiterada ou previsível.

Para Nucci[12], "a culpa penal se evidencia pela inobservância do dever objetivo de cuidado, especialmente quando há previsibilidade objetiva do resultado e possibilidade concreta de evitação". No caso de gestores que negligenciam o cumprimento da LGPD[13], especialmente nos artigos que tratam da segurança (art. 46) e do dever de documentação (art. 37 e 38), a omissão pode ensejar responsabilização penal nos moldes do art. 13, § 2º, do CP.

Portanto, a violação da LGPD, embora não configure crime autônomo, opera como critério normativo de ilicitude penal e como agravante interpretativa em contextos nos quais a negligência com os dados de saúde resulta em prejuízos reais e juridicamente relevantes.

---

[11] STJ – REsp 2.121.904/SP. Rel. Min. Nancy Andrighi. Julgado em 11 fev. 2025.

[12] NUCCI, Guilherme de Souza. *Manual de Direito Penal: Parte Geral; Parte Especial*. 6. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2009.

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

Quadro 1: Correlação entre violações da LGPD no setor da saúde e tipos penais:

Conduta/Violação da LGPD no Setor da Saúde	Artigo Penal Correlacionado	Breve Explicação da Correlação
Violação de segredo profissional (ex: acesso indevido ou compartilhamento)	Art. 154 do Código Penal (Violação de segredo profissional)	Quebra do dever de sigilo imposto por lei ou função, especialmente grave no contexto de dados sensíveis de saúde, com potencial de dolo ou culpa grave.
Invasão de dispositivo informático (ex: hacking de sistemas hospitalares)	Art. 154-A do Código Penal (Invasão de dispositivo informático)	Acesso não autorizado a sistemas que contenham dados de saúde, com ou sem prejuízo, visando obter, adulterar ou destruir dados.
Estelionato eletrônico (ex: uso de dados de saúde para fraudes via internet)	Art. 171, § 2º-A do Código Penal (Estelionato mediante fraude eletrônica)	Obtenção de vantagem ilícita por meio de fraude eletrônica que se utiliza de dados pessoais de saúde obtidos indevidamente para enganar a vítima.
Interrupção/perturbação de sistemas de saúde (ex: ataques cibernéticos)	Art. 266 do Código Penal (Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informações de utilidade pública)	Ações que causem interrupção ou perturbação de serviços de saúde (como sistemas de prontuários, agendamento, etc.), considerados de utilidade pública, gerando risco à saúde ou vida dos pacientes.
Omissão/Negligência grave na proteção de dados com resultado lesivo à vida/integridade física (ex: falha de segurança que impede socorro imediato)	Art. 13, § 2º do Código Penal (Crime omissivo impróprio) c/c Arts. 121 (Homicídio) ou 129 (Lesão Corporal)	Gestores/profissionais com dever de garantidor que, por omissão ou negligência (não implementação de medidas de segurança, falta de treinamento), permitem falha que, com nexo causal, resulta em dano à vida ou integridade física do paciente.
Inobservância dos princípios da LGPD (finalidade, segurança, prevenção, etc.)	Parâmetro de Ilicitude Penal (indireta)	Embora não seja um crime autônomo, a violação desses princípios, especialmente por negligência ou dolo, pode fundamentar a culpabilidade em tipos penais já existentes, agravando a conduta.

6 RESPONSABILIDADE PENAL DE GESTORES E PROFISSIONAIS DE SAÚDE

Por se tratar de dados pessoais sensíveis, diretamente relacionados aos direitos fundamentais à vida e à saúde, o tratamento de informações de saúde impõe aos gestores e profissionais um dever reforçado de diligência e proteção[14]. A violação desse dever de cuidado, especialmente quando previsível, pode fundamentar a responsabilização penal por omissão, nos termos do art. 13, § 2º do Código Penal[15], ao caracterizar a negligência, imprudência ou imperícia aptas a integrar tipos penais já existentes.

Essa responsabilidade não se limita aos agentes que praticam diretamente a conduta ilícita, como aquele que vaza ou acessa indevidamente dados pessoais. Atinge também aqueles que, em virtude de suas funções institucionais, detêm o dever jurídico de impedir o resultado danoso – os chamados garantidores[16]. Nesse grupo inserem-se gestores de hospitais, diretores de unidades de saúde, administradores de clínicas e responsáveis por setores de tecnologia da informação, cuja atuação é indispensável para a implementação de políticas de segurança da informação, prevenção de incidentes e governança de dados.

No âmbito do tratamento de dados pessoais pelo Poder Público, a responsabilidade do gestor não pode ser analisada apenas sob a ótica administrativa. À luz do art. 13, §2º, do Código Penal, aquele que detém o dever jurídico de agir – especialmente em razão de funções de direção, vigilância ou proteção – assume posição de garante, respondendo pela omissão que contribui de modo relevante para o resultado lesivo. A LGPD, por sua vez, reforça esse dever, ao impor obrigações específicas de segurança, prevenção e governança aos agentes públicos responsáveis pelo tratamento de dados (arts. 42 a 45)[17/18]. Assim, a inobservância de medidas mínimas de proteção pode caracterizar culpa grave, e, em hipóteses excepcionais em que haja previsibilidade concreta do dano e assunção consciente do risco, poderá até configurar dolo eventual[19], a depender das circunstâncias do caso concreto. A responsabilização penal de diretores hospitalares, gestores de TI ou administradores de clínicas se torna plausível quando, mesmo diante de alertas, optam por negligenciar medidas básicas de proteção ou deixam de treinar equipes (responsabilidade por omissão) e revisar sistemas vulneráveis.

No tocante aos profissionais de saúde, o dever de sigilo é reforçado tanto pela LGPD quanto pelos respectivos códigos de ética profissional[20]. médicos, enfermei-

---

14 DONEDA, Danilo; MENDES, Laura Schertel; WIMMER, Miriam. Lei Geral de Proteção de Dados Pessoais Comentada. São Paulo: Thomson Reuters/Revista dos Tribunais, 2021. Comentários aos arts. 5º, 11 e 23 da LGPD.

15 MASSON, Cleber. *Código Penal Comentado*. 13. ed. Rio de Janeiro: Forense, 2023. Comentário ao art. 13, § 2º.

16 Id. Comentário aos crimes omissivos impróprios, quando analisa a posição de garante e o dever jurídico de agir.

17 BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Arts. 42 a 45.

18 TRIBUNAL DE CONTAS DA UNIÃO. Acórdão nº 1.841/2022 – Plenário. Rel. Min. Walton Alencar Rodrigues.

19 BRASIL. Secretaria de Governo Digital. *Guia de Privacidade desde a Concepção e por Padrão (Privacy by Design e Privacy by Default)*. Brasília, 2021.

20 CONSELHO FEDERAL DE MEDICINA. *Código de Ética Médica*. Resolução CFM nº 2.217/2018.

ros, psicólogos, fisioterapeutas e outros profissionais que acessam e tratam dados sensíveis têm obrigação de observar a finalidade legítima do tratamento e evitar qualquer exposição indevida. A quebra injustificada de sigilo, além de infração ética, pode configurar o crime de violação de segredo profissional (art. 154 do CP)[21].

Julgados recentes do STJ apontam para a ampliação da responsabilidade objetiva e subjetiva de controladores e operadores de dados, inclusive com implicações civis e administrativas. No âmbito da responsabilização por falhas na segurança da informação, especialmente quando envolvem dados sensíveis, como os bancários, o Superior Tribunal de Justiça tem adotado uma postura rigorosa. Em julgamento recente REsp 2.121.904/SP[22], o Tribunal da Cidadania reconheceu a responsabilidade da entidade por permitir, por meio de sua plataforma, o acesso indevido de terceiros a perfis de investidores. Ainda que a fraude tenha ocorrido fora do ambiente direto da corretora, entendeu-se que houve omissão no dever de segurança e prevenção, violando-se tanto a Lei Geral de Proteção de Dados quanto os deveres contratuais e consumeristas aplicáveis. A Ministra Nancy Andrighi, relatora do caso, ressaltou que o dever de cautela das instituições que tratam dados pessoais é reforçado pela LGPD, sendo possível a responsabilização mesmo na ausência de dano patrimonial concreto[23], quando configurada falha técnica institucional. Esse entendimento converge com a Nota Técnica 18/2022[24] da ANPD, que igualmente considera que a inobservância dos princípios da prevenção, da segurança e da boa-fé, no contexto de tratamento de dados, pode gerar responsabilização jurídica ainda que não se comprove, de imediato, a efetiva ocorrência de danos ao titular. Em outro momento, a ANPD, em Nota Técnica sobre o e-SUS Notifica[25], também afirma que a omissão institucional em proteger os dados pessoais pode acarretar consequências jurídicas relevantes, mesmo que o dano concreto não tenha sido comprovado.

6.1 Responsabilidade de Gestores na Saúde Pública

No âmbito da saúde pública, a responsabilidade dos gestores é informada pelos princípios constitucionais da administração pública, como legalidade, moralidade e eficiência. Conforme destaca Maria Sylvia Zanella Di Pietro[26], a atuação do administrador deve pautar-se pela busca do interesse público, disto infere incluir a proteção efetiva dos dados sensíveis dos cidadãos. A omissão na implementação de medidas de segurança adequadas para sistemas como o e-SUS Notifica, por exemplo,

---

21 BRASIL. Código Penal. Art. 154 – Violação de segredo profissional.

22 BRASIL. Superior Tribunal de Justiça. Recurso Especial n.º 2.121.904/SP. Rel. Min. Nancy Andrighi. 3ª Turma, julgado em 11 jun. 2024. Determinou-se a exclusão de dados cadastrais inseridos indevidamente por terceiros na plataforma da B3. Informações judiciais disponíveis em: Migalhas, Migalhas Quentes, 12 mar. 2024. Acesso em: 31 jul. 2025.

23 Id. Trecho do voto da Relatora: reforço do dever de cautela de instituições que tratam dados pessoais, mesmo sem dano patrimonial imediato.

24 BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica n.º 18/2022/CGF/ANPD sobre o sistema e-SUS Notifica. Brasília, DF, 14 dez. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/notas-tecnicas/nota-tecnica-no-18-2022-cgf-anpd.pdf. Acesso em: 31 jul. 2025.

25 BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica n.º 18/2022/CGF/ANPD sobre o sistema e-SUS Notifica. Brasília, DF, 14 dez. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/notas-tecnicas/nota-tecnica-no-18-2022-cgf-anpd.pdf. Acesso em: 31 jul. 2025.

26 DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 36. ed. Rio de Janeiro: Forense, 2023.

não apenas contraria os ditames da LGPD, mas pode configurar violação de dever funcional, sujeitando o agente à Lei de Improbidade Administrativa.

A escolha e contratação de soluções tecnológicas no setor público de saúde demandam um rigoroso processo de licitação. Conforme ensina Marçal Justen Filho[27], a Administração deve estruturar a contratação de forma a assegurar o atendimento ao interesse público e a efetividade das obrigações contratuais. No âmbito da proteção de dados pessoais, isso implica que o gestor público deve exigir e fiscalizar a conformidade com normas de segurança da informação desde a fase de planejamento e elaboração do edital, em alinhamento às diretrizes da LGPD e aos princípios da privacidade desde a concepção.

Nesse contexto, o gestor público assume o dever jurídico de exigir e fiscalizar a conformidade dos contratos e soluções tecnológicas com as normas de segurança da informação e de proteção de dados. A omissão grave em assegurar que os sistemas contratados estejam alinhados à LGPD, sobretudo diante de riscos previsíveis, pode ensejar a responsabilização civil do ente público, o controle sancionatório por Tribunais de Contas e, em hipóteses de violação dolosa de deveres funcionais, a configuração de ato de improbidade administrativa, sem prejuízo de eventual responsabilização penal com base em tipos já previstos no Código Penal.

A LGPD impõe ao Poder Público deveres específicos de transparência, governança e segurança, como desenvolvido na doutrina de Doneda, Mendes e Wimmer[28]. A notificação da ANPD ao Ministério da Saúde sobre falhas no sistema e-SUS Notifica, que permitiram o acesso indevido a dados sensíveis, exemplifica a materialização de uma conduta omissiva que, para além das sanções administrativas, pode configurar o cenário para a imputação penal de gestores, especialmente se for demonstrado dolo eventual ou culpa grave na inobservância do dever de garantidor.

6.2 Responsabilidade de Gestores e Profissionais na Saúde Privada

Na saúde privada, a responsabilidade pela proteção de dados sensíveis dos pacientes é amplificada pela natureza da relação, que muitas vezes configura uma relação de consumo, além das obrigações contratuais e extracontratuais. Conforme preleciona Sergio Cavalieri Filho, a falha na segurança de dados em instituições de saúde, que resultem em danos aos titulares, pode ensejar responsabilidade civil objetiva da instituição, independentemente da prova de culpa, devido ao risco da atividade. Essa responsabilidade civil, contudo, não exclui a possibilidade de imputação penal a gestores e profissionais, especialmente quando há dolo ou culpa grave na omissão de medidas de proteção".

Os dados de saúde, por serem intrinsecamente ligados aos direitos da personalidade, gozam de proteção especial. A utilização indevida desses dados em ambientes privados, como exemplificado no caso de uma empresa de telecomunicações, representa uma violação direta da privacidade do paciente, um bem jurídico tutelado

---

27 JUSTEN FILHO, Marçal. *Curso de Direito Administrativo*. 12. ed. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. No contexto da proteção de dados pessoais, ver também: BRASIL. Secretaria de Governo Digital. *Guia de Privacidade desde a Concepção e por Padrão*, 2021; TRIBUNAL DE CONTAS DA UNIÃO. Acórdão 1.841/2022-Plenário.

28 DONEDA, Danilo; MENDES, Laura Schertel; WIMMER, Miriam. *Lei Geral de Proteção de Dados Pessoais Comentada***.** São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

pelos direitos da personalidade. Como ensina Carlos Alberto Bittar[29], "os dados ligados à esfera íntima do indivíduo – especialmente aqueles relacionados à saúde – integram o núcleo dos direitos da personalidade e, por isso, merecem tutela jurídica reforçada". Nesse sentido, a utilização indevida de dados de saúde em ambientes privados constitui violação direta da privacidade e da intimidade do paciente, bens jurídicos protegidos pela ordem constitucional e civil.

A saúde privada, embora impulsionada pela produtividade, não pode negligenciar os pilares do compliance e da cultura de proteção de dados. A falha em implementar programas eficazes, que incluam o treinamento contínuo de equipes e a revisão de vulnerabilidades, pode refletir uma omissão gerencial. Além disso, a conduta de profissionais de saúde, regida por seus códigos de ética, reforça o dever de sigilo e cuidado com os dados dos pacientes. A quebra desse dever, por exemplo, através de acessos indevidos por pressão de metas ou falhas em plataformas de telemedicina mal configuradas, pode ter implicações éticas, administrativas e penais, revelando a complexidade da responsabilização nesse setor.

7 GARANTIAS DOS USUÁRIOS E O PAPEL DO DIREITO PENAL

A proteção de dados pessoais, sobretudo os dados sensíveis, deve ser compreendida como meio de salvaguarda da dignidade da pessoa humana e da autonomia individual. Esses direitos, alicerçados nos princípios constitucionais, encontram na LGPD uma concretização normativa e, no Direito Penal, uma instância de resposta estatal diante das ofensas mais graves à esfera privada do titular.

Como observa Rodotà[30], a proteção da privacidade evoluiu além do mero direito à intimidade, passando a abarcar a autodeterminação informativa – o poder do indivíduo de controlar suas informações pessoais. No campo da saúde digital, essa autodeterminação ganha contornos ainda mais relevantes, pois o desequilíbrio entre paciente e instituição pode resultar em graves violações da liberdade individual.

O art. 5º, X, da Constituição Federal consagra a inviolabilidade da intimidade, da vida privada e da imagem. A LGPD reforça esse dispositivo, ao exigir consentimento informado, livre e inequívoco para o tratamento de dados. A manipulação indevida de dados pode, portanto, constituir não apenas ilícito civil ou administrativo, mas violação penal, conforme os arts. 154 e 171 do Código Penal, vai depender do elemento subjetivo e do resultado.

O Superior Tribunal de Justiça, no julgamento do REsp 2.121.904/SP, reconheceu a existência de dano moral presumido em casos de exposição indevida de dados sensíveis, especialmente na área da saúde. Esse entendimento reforça a gravidade jurídica da violação, mesmo quando não há prova de prejuízo concreto, e abre margem para uma interpretação penal mais rigorosa em casos similares.

Como observa Sarlet[31], a dignidade da pessoa humana deve ser o núcleo axiológico do sistema de proteção de dados, conferindo ao titular o poder de decidir

---

29 BITTAR, Carlos Alberto. *Direitos da Personalidade*. 7. ed. São Paulo: Saraiva, 2015.

30 RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda. p. 24–27.

31 SARLEt, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (orgs.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 22-59.

sobre o uso e a finalidade de suas informações pessoais. A atuação do Direito Penal, nesse contexto, é legítima quando voltada à repressão de condutas que comprometam esse núcleo essencial de direitos fundamentais.

8 COMPLIANCE E CULTURA DE PROTEÇÃO DE DADOS NA SAÚDE

A consolidação de uma cultura organizacional voltada à proteção de dados é essencial para a efetividade da LGPD no setor da saúde. Diante do volume expressivo de dados sensíveis manipulados diariamente por clínicas, hospitais, laboratórios e operadoras de planos, a ausência de mecanismos estruturados de governança expõe as instituições a riscos jurídicos, financeiros e reputacionais consideráveis.

No setor público, a conformidade esbarra frequentemente em restrições orçamentárias e burocracia, enquanto no setor privado, a competitividade e a agilidade podem levar a soluções mais rápidas, mas nem sempre robustas, para a proteção de dados.

O compliance em proteção de dados deve incluir políticas internas claras, plano de resposta a incidentes, inventário de dados, controles de acesso, treinamento contínuo dos profissionais e auditorias regulares. Essas medidas encontram respaldo técnico nas diretrizes da ISO/IEC 27701, 2019 e na Recomendação da ANPD[32] sobre segurança da informação em ambientes hospitalares.

A figura do encarregado pelo tratamento de dados pessoais, conhecido como DPO (*Data Protection Officer*), prevista no art. 41 da LGPD, representa um elemento-chave dessa cultura de conformidade. Esse profissional atua como elo entre a instituição, os titulares e a ANPD, sendo responsável pela orientação, fiscalização e tratamento de eventuais reclamações.

A capacitação de profissionais da saúde e equipes administrativas é igualmente essencial. É preciso sensibilizar esses agentes para os riscos jurídicos do tratamento inadequado de dados, promovendo uma postura proativa de prevenção. Conforme destaca Juliana Abrusio[33], a proteção de dados deve ser compreendida como um valor institucional, a ser incorporado desde a concepção de qualquer projeto ou serviço, em conformidade com o princípio do *privacy by design*, previsto na LGPD.

A consolidação de uma cultura de proteção de dados não elimina a incidência penal, mas a mitiga significativamente. Instituições que adotam padrões rigorosos de governança demonstram boa-fé e diligência, elementos essenciais na análise da culpabilidade e na prevenção de ilícitos penais no setor da saúde.

---

[32] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Brasília, DF: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em: 20 jul. 2025.

[33] ABRUSIO, Juliana. Da relevância do privacy by design na governança dos dados pessoais. In: BLUM, Renato Opice (coord.). *LGPD – Lei Geral de Proteção de Dados Comentada*. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2019.

9 A ATUAÇÃO DA ANPD E A EFETIVIDADE DA FISCALIZAÇÃO

A Autoridade Nacional de Proteção de Dados (ANPD), instituída pela Lei 13.853/2019, exerce papel estratégico na fiscalização e implementação da LGPD, especialmente em setores de alto risco, como a saúde. Sua atuação combina funções normativas, fiscalizatórias e sancionatórias, além de promover a conscientização pública e o diálogo institucional com entidades públicas e privadas.

Entre as competências da ANPD destacam-se: zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções administrativas, elaborar diretrizes para a Política Nacional de Proteção de Dados e fomentar boas práticas. Nos termos do art. 55-J da LGPD, a ANPD pode expedir recomendações técnicas, aplicar advertências, multas e determinar bloqueio ou eliminação de dados.

Na área da saúde, a atuação da ANPD tem se mostrado crescente. Destacam-se, dentre outros casos, a notificação ao Ministério da Saúde relativa ao sistema eSUS Notifica[34], em que a ANPD apurou vulnerabilidade no Sistema de Cadastro e Permissão de Acesso (SCPA), permitindo a consulta indevida de dados sensíveis por meio de falha de autenticação do sistema, evidenciando riscos à privacidade mesmo sem comprovação de dano concreto. No caso de uma empresa de telecomunicações[35], a ANPD concluiu que a empresa comercializava listas de contatos telefônicos – inclusive de pacientes – sem o consentimento dos titulares, configurando tratamento ilegal conforme os arts. 7º e 41 da LGPD. A conduta ensejou a instauração de processo administrativo sancionador, resultando na lavratura de Auto de Infração e na aplicação de multa proporcional à gravidade da infração. Tal situação reforça que a omissão ou descumprimento dos deveres legais na proteção de dados pessoais pode gerar responsabilização, independentemente da ocorrência de dano concreto.

O cruzamento de bases de dados no contexto da pandemia de COVID-19 levou à articulação interinstitucional entre ANPD e o Ministério da Saúde, reforçando a necessidade de avaliações de impacto e segurança. Esse cenário ficou explícito no processo sancionador instaurado[36] pela ANPD em face do Ministério da Saúde, que cobrou a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) para sistemas críticos (como o e-SUS Notifica) e a adoção de medidas corretivas de segurança. No campo da saúde suplementar, a cooperação entre ANS e ANPD[37] também formalizou rotinas de compartilhamento de informações e ações educativas para aprimorar a proteção de dados.

---

[34] BRASIL. Autoridade Nacional de Proteção de Dados. Processo Administrativo de Fiscalização nº 00261.001963/2022-73 – Notificação ao Ministério da Saúde sobre falhas no sistema e-SUS Notifica (Sistema de Cadastro e Permissão de Acesso – SCPA). Brasília, DF: ANPD, 07 ago. 2024.

[35] BRASIL. Autoridade Nacional de Proteção de Dados. Processo Administrativo Sancionador nº 00261.000489/2022-62 – Auto de Infração contra empresa de telecomunicações. Brasília, DF, 10 mar. 2022. CGF/ANPD. Disponível em: https://www.gov.br/anpd. Acesso em: 31 jul. 2025.

[36] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Relatório de Instrução nº 5 – SEI 00261.000456/2022-12 (Ministério da Saúde). Brasília, 30 out. 2024. Disponível em: https://www.gov.br/anpd (acesso em: 31 jul. 2025).

[37] AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANS e ANPD firmam acordo para aprimorar proteção de dados na área de saúde suplementar. 27 dez. 2024. Disponível em: https://www.gov.br/ans (acesso em: 31 jul. 2025).

Apesar dos avanços, desafios persistem quanto à efetividade das sanções e à estrutura da ANPD. Os relatórios institucionais e o Plano de Ações Educativas[38] da própria ANPD confirmam a ênfase em iniciativas orientativas e corretivas[39] para consolidar a cultura de proteção de dados, com publicações, guias e fiscalizações pedagógicas. Em paralelo, análises públicas indicam restrição orçamentária e déficit de pessoal[40], fatores que impactam a velocidade e o alcance da fiscalização. Mesmo assim, casos recentes – como as advertências e determinações de medidas corretivas impostas ao Ministério da Saúde[41] – mostram a atuação sancionadora combinada a exigências de governança.

10 CONSIDERAÇÕES FINAIS

A proteção de dados sensíveis no setor da saúde configura-se como um dos maiores desafios contemporâneos do Direito, em especial diante da interseção entre tecnologia, dignidade humana e riscos penais. A LGPD, ao reconhecer a especial natureza dos dados de saúde, estabelece um marco regulatório que transcende o plano administrativo, projetando seus efeitos sobre a dogmática penal, especialmente no tocante à responsabilidade por omissão.

O presente estudo procura demonstrar que a atuação diligente de gestores e profissionais da saúde é fundamental para a prevenção de ilícitos penais relacionados à exposição indevida de dados. A posição de garantidor atribuída pelo art. 13, § 2º, do Código Penal, aliada aos princípios da LGPD, impõe um padrão de cuidado qualificado, cuja inobservância pode ensejar imputações de culpa ou dolo (direto ou eventual).

A análise doutrinária e jurisprudencial evidencia que a LGPD opera como instrumento transversal de compliance, cuja implementação eficaz depende da cultura organizacional, da atuação do DPO e da adoção de protocolos técnicos consistentes. A atuação da ANPD, embora incipiente, já representa um importante vetor de transformação institucional no setor da saúde.

Conclui-se que a prevenção de danos, a responsabilização proporcional e a promoção da autodeterminação informativa exigem um sistema jurídico-penal que dialogue com os direitos fundamentais da era digital. A consolidação dessa cultura passa por políticas públicas integradas, fiscalização efetiva e compromisso ético das instituições de saúde com a proteção da esfera íntima de seus pacientes.

---

38 BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Plano Institucional de Ações Educativas. Brasília: ANPD, 18 jan. 2024. Disponível em: https://www.gov.br/anpd (acesso em: 31 jul. 2025).

39 BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Relatório Anual de Gestão 2023. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd (acesso em: 31 jul. 2025).

40 Declaração concedida pelo presidente da Autoridade Nacional de Proteção de Dados (ANPD), *Aos Fatos*, em 23 ago. 2023, acerca da limitação orçamentária e de pessoal do órgão. A presente menção tem caráter ilustrativo e contextual, não constituindo fonte primária normativa, sendo complementada por dados oficiais constantes no Relatório Anual de Gestão 2023 e no Plano Institucional de Ações Educativas da ANPD.

41 Em 14 de agosto de 2024, a Autoridade Nacional de Proteção de Dados (ANPD) aplicou ao Ministério da Saúde duas advertências e determinou a adoção de medidas corretivas, em decorrência de falhas de segurança que permitiram a invasão de sistema e o acesso indevido a dados pessoais. A decisão decorreu de processo administrativo sancionador instaurado após incidente ocorrido em 2022.

11 REFERÊNCIAS

ABRUSIO, Juliana, “Da relevância do ‘privacy by design’ na governança dos dados pessoais”, in: Blum, Renato Opice (coord.), *LGPD – Lei Geral de Proteção de Dados Comentada*, 2. ed., rev., atual. e ampl., São Paulo, Revista dos Tribunais, 2019.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANS e ANPD firmam acordo para aprimorar proteção de dados na área de saúde suplementar. 27 dez. 2024. Disponível em: https://www.gov.br/ans (acesso em: 31 jul. 2025).

AOS FATOS. ANPD atua por orçamento maior em meio a PLs sobre economia digital e IA. 23 ago. 2023. Disponível em: https://www.aosfatos.org (acesso em: 30 jul. 2025).

BARBAGALO, Fernando Brandini, *O novo crime de fraude eletrônica e o princípio da legalidade*, TJDFT, Brasília, 3 jun. 2022, disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade>, acesso em: 31 jul. 2025.

BITTAR, Carlos Alberto. *Os Direitos da Personalidade*. 8. ed. Rio de Janeiro: Forense Universitária, 2015.

BONIZZATO, Luigi. *A Constituição da Saúde e da Vida: os Direitos Fundamentais à Saúde e à Vida e o Processo de Inconstitucionalização da Lei Brasileira do Plano de Saúde*. Rio de Janeiro: Renovar, 2008.

BRASIL, Autoridade Nacional de Proteção de Dados, *Nota Técnica n.º 18/2022/CGF/ANPD sobre o sistema e-SUS Notifica*, Brasília, 14 dez. 2022, disponível em: <https://www.gov.br/anpd/pt-br/assuntos/notas-tecnicas/nota-tecnica-no-18-2022-cgf-anpd.pdf>, acesso em: 31 jul. 2025.

BRASIL, Autoridade Nacional de Proteção de Dados, *Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte*, Brasília, ANPD, out. 2021, disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf>, acesso em: 20 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Plano Institucional de Ações Educativas. Brasília: ANPD, 18 jan. 2024. Disponível em: https://www.gov.br/anpd (acesso em: 31 jul. 2025).

BRASIL, Autoridade Nacional de Proteção de Dados, *Processo Administrativo de Fiscalização 00261.001963/2022-73 – Notificação ao Ministério da Saúde sobre falhas no sistema e-SUS Notifica*, Brasília, ANPD, 7 ago. 2024.

BRASIL, Autoridade Nacional de Proteção de Dados, *Processo Administrativo Sancionador 00261.000489/2022-62 – Auto de Infração contra Empresa de Telecomunicações*, Brasília, CGF/ANPD, 10 mar. 2022, disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_(xxxxxx).pdf>, acesso em: 31 jul. 2025.

BRASIL, Superior Tribunal de Justiça, *Recurso Especial n.º 2.121.904/SP*, Rel. Min. Nancy Andrighi, Brasília, julgado em 11 jun. 2024, disponível em: https://www.migalhas.com.br/quentes/398822/b3-deve-excluir-dados-inseridos-por-terceiros-em-perfil-de-investidor, acesso em: 31 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Relatório de Instrução 5 – SEI 00261.000456/2022-12* (Ministério da Saúde). Brasília, 30 out. 2024. Disponível em: <https://www.gov.br/anpd>. Acesso em: 31 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Relatório Anual de Gestão 2023*. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd (acesso em: 31 jul. 2025).

CAVALIERI FILHO, Sergio. Programa de Responsabilidade Civil. 16. ed. São Paulo: Atlas, 2023.

CONVERGÊNCIA DIGITAL. ANPD aplica sanção ao Ministério da Saúde por invasão de sistema. 14 ago. 2024. Disponível em: https://www.convergenciadigital.com.br (acesso em: 30 jul. 2025).

CONSELHO FEDERAL DE MEDICINA**.** *Código de Ética Médica*. Resolução CFM 2.217/2018. DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo, *Da privacidade à proteção de dados pessoais: elementos da formação da autoridade nacional*, Revista de Direito Civil Contemporâneo, São Paulo, vol. 17, pp. 13–35, jan.–abr. 2018.

DONEDA, Danilo; MENDES, Laura Schertel; WIMMER, Miriam. *Lei Geral de Proteção de Dados Pessoais Comentada.* São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

JUSTEN FILHO, Marçal. *Curso de Direito Administrativo*. 12. ed. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. Cf. ainda BRASIL. Secretaria de Governo Digital**.** *Guia de Privacidade desde a*

Concepção e por Padrão. Brasília, 2021; TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão 1.841/2022 – Plenário.*

MARTINS, Guilherme Magalhães. *LGPD comentada: a Lei Geral de Proteção de Dados e o Regulamento Europeu (GDPR). 3.* ed. Rio de Janeiro: Forense, 2021.

MASSON, Cleber. *Código Penal Comentado*.13ed. Rio de Janeiro: Forense, 2023.1816p.

NUCCI, Guilherme de Souza, *Manual de Direito Penal: Parte Geral; Parte Especial*, 6. ed., rev., atual. e ampl., São Paulo, Editora Revista dos Tribunais, 2009.

PEREIRA, Marina Pinhão Coelho; LIMA, Thiago (Coords.). *Compliance na Saúde: Aspectos Jurídicos e Práticos*. Belo Horizonte: D'Plácido, 2021.

RODOTÀ, Stefano, *A vida na sociedade da vigilância: a privacidade hoje*, tradução: Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro, Renovar.

SARLET, Ingo Wolfgang, "Fundamentos constitucionais: o direito fundamental à proteção de dados", in: Doneda, Danilo *et al.* (orgs.), *Tratado de proteção de dados pessoais*, Rio de Janeiro, Forense, 2021.

SARLET, Ingo Wolfgang; Dall'Agnol, Darlei, "Dignidade da pessoa humana e o direito à proteção de dados pessoais", *Revista Brasileira de Bioética*, Brasília, vol. 15, n.º 3, pp. 331–348.