VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS I

D597

Direitos e garantias fundamentais I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Daize Fernanda Wagner; Lucas Gonçalves da Silva; Marcos Leite Garcia. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-154-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos. 3. Garantias fundamentais. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS I

Apresentação

Apresentação

Nos dias 24 a 28 de junho de 2025 foi realizado o VIII Encontro Virtual do CONPEDI. A partir da temática geral do evento, “Direito, governança e políticas de inclusão”, pesquisadores, professores, estudantes de pós-graduação e graduação em Direito de todo o país puderam socializar suas pesquisas e participar de discussões avançadas em diferentes grupos de trabalho (GT).

O GT Direitos e Garantias Fundamentais I, coordenado pelos professores Marcos Leite Garcia (Universidade do Vale do Itajaí – UNIVALI), Lucas Gonçalves da Silva (Universidade Federal de Sergipe – UFS) e Daize Fernanda Wagner (Universidade Federal de Santa Catarina – UFSC/Universidade Federal do Amapá – UNIFAP) objetivou promover o debate acerca de pesquisas jurídicas desenvolvidas ou em desenvolvimento nos programas de pós-graduação e na graduação em Direito que abordam, sob diferentes enfoques, os mecanismos de proteção e defesa de direitos e garantias fundamentais, oferecendo uma perspectiva abrangente de debates.

Os dezessete trabalhos aqui reunidos propõem uma análise multifacetada dos direitos fundamentais no Brasil contemporâneo, mergulhando em suas bases teóricas e nos desafios práticos de sua efetivação, sobretudo para grupos vulnerabilizados. Além disso, demonstram agenda de pesquisa contemporânea, focada nos desafios impostos pelas novas tecnologias e pelo cenário de mudanças climáticas e ambientais profundas. Assim, representam um convite à reflexão sobre a complexidade e a constante demanda e luta por direitos, em um cenário de

Daize Fernanda Wagner, doutora em Direito. Professora no Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina (UFSC) e do Programa de Pós-Graduação stricto sensu em Direito da Universidade Federal do Amapá (UNIFAP).

PRIVACIDADE E PROTEÇÃO DE DADOS NA SAÚDE SUPLEMENTAR: UMA ANÁLISE CRÍTICA DO CASO KLARA CASTANHO À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO E DO COMPLIANCE

PRIVACY AND DATA PROTECTION IN SUPPLEMENTARY HEALTHCARE: A CRITICAL ANALYSIS OF THE KLARA CASTANHO CASE IN LIGHT OF THE BRAZILIAN LEGAL FRAMEWORK AND COMPLIANCE

Ana Carolina Couto Matheus [1]

Resumo

A presente pesquisa teve como objetivo geral analisar criticamente a proteção de dados pessoais na saúde suplementar brasileira, à luz do caso Klara Castanho, destacando o compliance como ferramenta estratégica de prevenção. Como objetivos específicos, buscou-se examinar o desenvolvimento normativo da proteção de dados no Brasil, identificar as legislações aplicáveis à saúde suplementar e avaliar a atuação institucional no episódio em questão. A metodologia adotada fundamentou-se em pesquisa bibliográfica, documental e jurisprudencial, com abordagem qualitativa e método dedutivo, a partir da análise de legislações como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet, a Constituição Federal, Resoluções Normativas da Agência Nacional de Saúde Suplementar (ANS) e normas dos Conselhos de Classe. Sustentou-se a hipótese de que a ausência de um compliance digital estruturado e de ações articuladas entre as esferas administrativa, judicial e ético-profissional contribuiu para a violação dos direitos fundamentais da atriz. Os resultados evidenciaram que programas de compliance, com ênfase em Data Mapping, Relatórios de Impacto à Proteção de Dados (RIPD) e capacitação continuada, mostraram-se indispensáveis à conformidade regulatória e à segurança informacional. Concluiu-se que a atuação insuficiente dos órgãos competentes no caso analisado revelou fragilidades na efetivação normativa e na proteção de dados sensíveis, reforçando a necessidade de políticas institucionais eficazes. Assim, verificou-se que a adoção de um compliance digital robusto configurou-se como medida essencial para a preservação da privacidade e dignidade dos titulares de dados no setor de saúde suplementar.

healthcare sector, and assess the institutional response to the episode in question. The methodology adopted was based on bibliographic, documental, and case law research, with a qualitative approach and deductive method, through the analysis of legislation such as the General Data Protection Law (LGPD), the Brazilian Civil Rights Framework for the Internet, the Federal Constitution, regulatory resolutions of the National Supplementary Health Agency (ANS), and professional councils' regulations. The hypothesis sustained was that the absence of a structured digital compliance program and coordinated actions among administrative, judicial, and ethical-professional spheres contributed to the violation of the actress's fundamental rights. The results demonstrated that compliance programs, with emphasis on Data Mapping, Data Protection Impact Assessments (DPIA), and continuous staff training, proved indispensable for regulatory compliance and informational security. It was concluded that the insufficient actions of competent bodies in the analyzed case revealed weaknesses in regulatory enforcement and in the protection of sensitive data, reinforcing the need for effective institutional policies. Thus, the adoption of a robust digital compliance framework emerged as an essential measure for preserving the privacy and dignity of data subjects in the supplementary healthcare sector.

Keywords/Palabras-claves/Mots-clés: Privacy, Data protection, Supplementary healthcare, Compliance, Klara castanho case

1 INTRODUÇÃO

Atualmente, a proteção de dados pessoais constitui-se um dos maiores desafios do ambiente jurídico e institucional, sobretudo diante do crescimento exponencial das tecnologias digitais e da circulação massiva de informações sensíveis.

No setor da saúde suplementar, essa realidade torna-se ainda mais complexa, uma vez que envolve dados extremamente sigilosos, relacionados à intimidade, integridade física e emocional dos indivíduos.

Nesse contexto, a privacidade e a proteção de informações de pacientes devem ser tratadas com rigor, considerando-se não apenas a confidencialidade médico-paciente, mas também o tratamento seguro e ético de dados pelos profissionais de saúde, instituições hospitalares e operadoras de planos de saúde.

Em 2022, o caso da atriz Klara Castanho trouxe à tona uma grave violação de direitos fundamentais, especialmente no que tange à proteção de dados pessoais no ambiente hospitalar e à exposição indevida de informações sensíveis por meio da mídia.

De acordo com as informações veiculadas, a atriz, após ser vítima de violência sexual, optou legalmente pela entrega voluntária de seu bebê para adoção, procedimento este que deveria ter permanecido resguardado pelo sigilo médico-hospitalar.

Entretanto, informações sigilosas sobre o caso foram divulgadas sem o consentimento da titular dos dados, possivelmente por meio do acesso indevido ao prontuário médico da paciente. Esse episódio expôs não apenas a fragilidade das instituições na proteção dos direitos de privacidade dos titulares de dados, mas também a insuficiência dos mecanismos de controle, prevenção e responsabilização disponíveis.

Diante disso, a pesquisa em tela tem como objetivo geral analisar a proteção de dados pessoais na saúde suplementar brasileira, à luz do caso Klara Castanho, destacando o *compliance* como ferramenta estratégica de prevenção. Para alcançar tal finalidade, definiram-se como objetivos específicos: examinar o desenvolvimento normativo da proteção de dados no Brasil; identificar as legislações aplicáveis ao setor de saúde suplementar; e avaliar a atuação institucional e as medidas adotadas no episódio em questão.

Pretende-se, assim, demonstrar de que forma a ausência de programas de *compliance* digital estruturados e a falta de ações articuladas entre as esferas administrativa, judicial e ético-profissional contribuem para a violação de direitos fundamentais, em especial no ambiente sensível da saúde.

A ideia central do estudo concentra-se na relevância do *compliance* digital no setor

de saúde suplementar, não apenas como uma exigência normativa, mas como uma estratégia preventiva eficaz na proteção de dados pessoais e sensíveis.

A partir da análise do caso Klara Castanho, evidencia-se a necessidade urgente de adoção de políticas institucionais mais robustas, capazes de coibir práticas ilícitas e de preservar a dignidade, intimidade e segurança dos titulares de dados.

O caso revela também a vulnerabilidade das estruturas institucionais brasileiras no enfrentamento a esse tipo de violação, demonstrando a urgência de se estabelecer diretrizes claras, articuladas e integradas entre os órgãos reguladores e fiscalizadores.

Nesse sentido, o problema de pesquisa está delineado na seguinte indagação: como o *compliance* pode ser utilizado para combater a disseminação e o vazamento de informações de pacientes no âmbito da saúde suplementar, prevenindo a repetição de episódios como o ocorrido com a atriz Klara Castanho?

A partir dessa problemática, formula-se a hipótese de que a ausência de um *compliance* digital estruturado, associado à ineficácia da atuação conjunta entre as esferas administrativa, judicial e ético-profissional, contribuiu significativamente para a violação dos direitos fundamentais da atriz, demonstrando a necessidade de reestruturação institucional e normativa nesse campo.

A justificativa para a realização desta pesquisa reside na importância social, jurídica e ética da proteção de dados pessoais na saúde suplementar, sobretudo diante do avanço das ferramentas digitais e do consequente aumento do risco de compartilhamento indevido de informações sensíveis.

A gravidade do caso Klara Castanho transcende os limites individuais, pois evidencia a falência de mecanismos institucionais em assegurar direitos básicos e previstos legalmente, além de ressaltar a importância da conformidade das operadoras de planos de saúde e instituições hospitalares às normas vigentes, de modo a evitar novas violações.

Para alcançar os objetivos propostos, a metodologia adotada consiste em uma pesquisa bibliográfica, documental e jurisprudencial, com abordagem qualitativa e método dedutivo. Serão analisadas legislações como a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), o Marco Civil da Internet (Lei n.º 12.965/2014), a Constituição Federal, as resoluções normativas da Agência Nacional de Saúde Suplementar (ANS) e normas dos Conselhos de Classe, como os Conselhos Federais de Medicina e de Enfermagem. Será feita a análise documental do caso Klara Castanho a partir das informações públicas disponíveis, avaliando as implicações jurídicas e institucionais da violação dos dados da atriz.

O desenvolvimento do trabalho está organizado da seguinte forma: será examinado o

desenvolvimento normativo do direito à proteção de dados pessoais na Constituição Federal, no Código Civil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Serão estudadas as normas relacionadas à proteção de dados na saúde suplementar, considerando as resoluções da ANS, as normas dos Conselhos de Classe e a Lei Anticorrupção, destacando o papel do *compliance* empresarial e digital na prevenção de violações.

Sob as perspectivas judicial e administrativa será analisado o caso Klara Castanho para identificar falhas, lacunas normativas e propor medidas preventivas baseadas na implementação de programas de integridade e *compliance*.

Dessa forma, esta pesquisa pretende contribuir para o aprimoramento do debate jurídico acerca da proteção de dados sensíveis na saúde suplementar brasileira, bem como para a construção de mecanismos institucionais mais eficientes de prevenção e controle, a partir da adoção de práticas de *compliance* digital e do fortalecimento da atuação integrada dos órgãos responsáveis pela fiscalização e aplicação das normas.

2 O DESENVOLVIMENTO DO DIREITO A PROTEÇÃO DOS DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Apesar da Constituição Federal de 1988 assegurar a privacidade como direito fundamental e o Código Civil de 2002 garantir a proteção dos direitos da personalidade, persistia uma lacuna legal no Brasil quanto à proteção de dados pessoais no ambiente digital e fora dele. Diante do avanço das normativas internacionais, especialmente na União Europeia, o Brasil passou a estruturar seu arcabouço normativo para acompanhar essa tendência.

Nesse sentido, destacam-se a Lei n.º 12.965/2014, o Marco Civil da Internet, que estabelece princípios e garantias para o uso da internet no país, e a Lei n.º 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que regulamenta a coleta, o tratamento, o compartilhamento e o descarte de dados pessoais, abrangendo o setor público e o privado.

Para Lenza (2016, p. 85) o Direito se estrutura de forma hierárquica, a Constituição Federal é norma suprema, fundamento de validade das demais normas, conforme preconiza a Teoria Pura do Direito de Kelsen (2000). No âmbito da proteção de dados, a Constituição de 1988, em seu art. 5º, X, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem, sem tratar expressamente dos dados pessoais (BRASIL, 1988).

A Emenda Constitucional n.º 115/2022 inseriu no art. 5º, LXXIX, a previsão específica do direito à proteção de dados pessoais, inclusive nos meios digitais (BRASIL, 2022). Enquanto o inciso X tutela aspectos amplos da privacidade e honra, como o sigilo

bancário ou a proteção contra revistas íntimas, o inciso LXXIX trata da proteção da coleta, tratamento e compartilhamento de dados pessoais, garantindo que tais operações sejam realizadas conforme princípios legais e éticos.

O Código Civil Brasileiro protege a personalidade, garantindo direitos essenciais à dignidade humana, como os direitos de imagem, nome e privacidade. Farias e Rosenvald (2006, p. 101-102) definem esses direitos como projeções fundamentais do indivíduo, essenciais ao seu desenvolvimento.

Venosa (2023, p. 306) afirma que esses direitos são irrenunciáveis, pois asseguram atributos indispensáveis à individualidade. O art. 17 do Código Civil estabelece que o nome não pode ser usado de forma a expor alguém ao desprezo público (BRASIL, 2002). O art. 21 garante que a vida privada é inviolável, permitindo que o juiz tome medidas para proteger a privacidade da pessoa (BRASIL, 2002). Na prática essa proteção nem sempre é respeitada, como exemplificado no caso da atriz Klara Castanho, cuja privacidade foi violada pela divulgação pública da sua decisão de entregar o filho para adoção, gerando julgamentos morais e uma repercussão nacional (FOLHA DE S.PAULO, 2022).

A violação da privacidade configura um dano moral, que deve ser reparado por meio da responsabilidade civil. Venosa (2023, p. 748) explica que a responsabilidade civil decorre da obrigação de reparar danos causados por atos ilícitos. Tartuce (2023) afirma que a responsabilidade civil exige quatro elementos: conduta humana (ação ou omissão), dolo ou culpa, nexo de causalidade e dano patrimonial ou extrapatrimonial. No caso da violação da privacidade de Klara Castanho está configurada a lesão ao bem jurídico da pessoa.

Portanto, o ordenamento jurídico brasileiro permite a proteção da privacidade e da personalidade por meio de normas constitucionais e civis, sendo imprescindível considerar a responsabilidade civil para reparar os danos decorrentes de violações à privacidade e à proteção de dados pessoais.

A Lei n.º 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, é um marco fundamental na regulamentação do uso da Internet no Brasil. Estabelece direitos e deveres para o ambiente digital, abordando a privacidade, a proteção de dados pessoais e a segurança das informações online (BRASIL, 2014). A principal inovação do Marco Civil foi alinhar direitos constitucionais, como liberdade de expressão, comunicação e manifestação de pensamento, com a proteção da privacidade e dos dados dos usuários, proibindo práticas que comprometam a segurança das informações e a intimidade no meio virtual (BRASIL, 2014).

Entretanto, a legislação tem uma natureza predominantemente principiológica, sem um caráter sancionatório amplo. Suas sanções são principalmente administrativas e

econômicas, como advertências, multas e suspensão de atividades, e são aplicáveis, sobretudo, a pessoas jurídicas, como provedores e empresas digitais (BRASIL, 2014). O Marco Civil, portanto, não responsabiliza diretamente indivíduos por infrações, limitando-se a estabelecer diretrizes para a atuação no ambiente digital.

Essa limitação evidenciou a necessidade de uma legislação mais detalhada sobre o tratamento de dados pessoais, o que levou à criação da Lei n.º 13.709, de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que preencheu as lacunas do Marco Civil, oferecendo um quadro legal mais robusto para a proteção de dados e privacidade (BRASIL, 2018).

A Lei n.º 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi sancionada como resposta à crescente preocupação com a privacidade e o uso de dados pessoais no Brasil, alinhando-se às exigências internacionais (BRASIL, 2018). Sua vigência plena, com sanções efetivas, iniciou-se em 1º de agosto de 2021, após o prazo de adaptação inicial e a prorrogação devido à pandemia de COVID-19 (BRASIL, 2020). O objetivo principal da LGPD é regulamentar o tratamento de dados pessoais, garantindo direitos fundamentais como liberdade e privacidade (BRASIL, 2018).

A LGPD estabelece princípios e controles técnicos para o tratamento de dados, incluindo os sensíveis, ao longo de seu ciclo de vida, com base em conceitos como finalidade, adequação e transparência (BRASIL, 2018). Embora similar ao Regulamento Geral sobre a Proteção de Dados (RGPD) europeu, a LGPD possui uma estrutura mais enxuta, com cerca de 60 artigos, o que gerou lacunas, como a indefinição dos prazos para comunicação de incidentes de segurança, que são vagos e dependem da interpretação judicial (Peck, 2021).

Entre as bases legais para o tratamento de dados, destaca-se o consentimento, que deve ser livre e informado, mas há exceções, como em situações de emergência médica (BRASIL, 2018). As sanções previstas são majoritariamente administrativas, variando desde advertências até multas de até cinquenta milhões de reais por infração, aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável também pela regulamentação e fiscalização do cumprimento da lei (BRASIL, 2018).

A ANPD era vinculada à Presidência da República e foi transformada em autarquia. É estratégica na implementação da LGPD e no posicionamento do Brasil no mercado digital global (Peck, 2021). A adequação à LGPD envolve implementar políticas, treinamentos, controles de segurança e a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), que detalha o tratamento de dados e as medidas de mitigação de riscos (BRASIL, 2018). A LGPD é um marco regulatório essencial, equilibrando proteção de dados pessoais com direitos constitucionais e exigências internacionais de privacidade (BRASIL, 2018).

3 AS NORMAS E AS LEGISLAÇÕES REGULAMENTADORAS DA PROTEÇÃO DE DADOS NO BRASIL E NA SAÚDE SUPLEMENTAR

O setor de saúde suplementar no Brasil, que inclui planos de saúde, seguros e serviços privados, é regulado pela Agência Nacional de Saúde Suplementar (ANS), vinculada ao Ministério da Saúde. A ANS é responsável por normatizar, implementar e fiscalizar as regras do setor, além de proteger o interesse público (BRASIL, 2000). Dentro do contexto normativo, destacam-se as Resoluções Normativas da ANS, como a RN n.º 507 e a RN n.º 518, de 2022, que estabelecem diretrizes para a adoção de boas práticas nos planos de saúde, incluindo a proteção da privacidade e o tratamento adequado de dados pessoais dos usuários.

Além disso, os Conselhos Profissionais de Saúde, como o Conselho Federal de Medicina (CFM), desempenham papel relevante na regulamentação ética sobre o sigilo e a proteção das informações dos pacientes. A Resolução n.º 1.605, de 31 de dezembro de 2009, do CFM, proíbe a divulgação de informações em prontuários e fichas médicas sem o consentimento expresso do paciente (BRASIL, 2009).

A proteção de dados na saúde suplementar no Brasil se dá por meio da LGPD e de regulamentações específicas da ANS e dos Conselhos Profissionais, formando um sistema normativo cada vez mais atento à privacidade e aos direitos dos titulares de dados.

O Código de Ética Médica, estabelecido pela Resolução n.º 2.217, de 27 de setembro de 2018, do Conselho Federal de Medicina (CFM), impõe aos médicos a obrigação de preservar o sigilo sobre informações obtidas no exercício da profissão, salvo quando autorizado por legislação, motivo justo ou consentimento escrito do paciente (CFM, 2019). O art. 85 do mesmo Código proíbe o manuseio de prontuários por pessoas não obrigadas ao sigilo (CFM, 2021), e a Resolução CFM n.º 1.605, de 2009, reforça essa proibição ao vedar a divulgação de dados de prontuários sem consentimento (CFM, 2009).

Para os profissionais de enfermagem, o Código de Ética, instituído pela Resolução n.º 564/2017, do Conselho Federal de Enfermagem (COFEN) estabelece no art. 52, a obrigação de manter sigilo sobre as informações obtidas no exercício profissional, salvo por exigência legal, determinação judicial ou consentimento escrito do paciente (COFEN, 2017). O sigilo é mantido após o falecimento do paciente, exceto em situações específicas de ameaça à vida ou à dignidade (COFEN, 2017). Essas normas demonstram a importância do sigilo profissional como princípio ético na tutela dos direitos fundamentais dos pacientes e a integridade das informações sensíveis acessadas pelos profissionais de saúde.

A Resolução Normativa n.º 507/2022 da ANS estabelece o Programa de Acreditação de Operadoras de Planos Privados de Assistência à Saúde, visando à qualificação dos serviços prestados e a melhoria no modelo assistencial (ANS, 2022). A acreditação é facultativa, mas oferece benefícios, como bonificações no Índice de Desempenho da Saúde Suplementar (IDSS) e a redução de margens de solvência, impactando positivamente a competitividade das operadoras (ANS, 2022).

A norma aborda a proteção de dados pessoais e sensíveis, exigindo que as operadoras implementem um Plano Diretor de Tecnologia da Informação, com mecanismos de segurança, como criptografia, para evitar vazamentos de dados (ANS, 2022). Obriga a assinatura de termos de confidencialidade pelos colaboradores, garantindo o sigilo após o término do vínculo contratual, especificando consequências legais no descumprimento (ANS, 2022). Estabelece padrões para o armazenamento de dados, assegurando sua confidencialidade, integridade e disponibilidade, alinhados à norma ISO/IEC 27002 (ANS, 2022).

Essas diretrizes garantem que os dados sejam utilizados apenas para fins autorizados, preservando a privacidade e a conformidade com a Lei Geral de Proteção de Dados (LGPD), consolidando práticas seguras no tratamento de informações sensíveis no setor da saúde suplementar (ANS, 2022).

A Resolução Normativa n.º 518/2022 da Agência Nacional de Saúde Suplementar (ANS) estabelece diretrizes obrigatórias de governança corporativa, com foco na gestão de riscos e controles internos para operadoras de planos de saúde de médio e grande porte (ANS, 2022). Embora não trate diretamente da proteção de dados ou segurança da informação é relevante no campo regulatório, pois exige práticas éticas e transparentes nas operadoras.

Os artigos 11 e 12 da RN 518/22 determinam que as operadoras enviem anualmente o Relatório de Procedimentos Previamente Acordados, elaborado por auditor independente, com informações sobre governança, gestão de riscos e controles internos (ANS, 2022). O Anexo III lista as práticas avançadas de governança, incluindo a necessidade de regras de conduta e ética formalmente aprovadas pelo conselho de administração (ANS, 2022).

O item 1.4 do Anexo III exige a implementação de programas de integridade, auditoria e canais de denúncia para garantir a efetiva aplicação dos códigos internos de conduta. Esses programas devem prevenir atos ilícitos previstos na Lei n.º 9.613/1998, infrações da Lei n.º 9.656/1998 e atos lesivos à administração pública, conforme a Lei n.º 12.846/2013, com treinamentos regulares (ANS, 2022). Ao exigir essas medidas, a RN 518/22 reforça a obrigação das operadoras de atuar de forma ética e transparente, assegurando a proteção de direitos fundamentais, como a inviolabilidade da intimidade e a proteção de dados

pessoais, conforme a Constituição Federal (BRASIL, 1988).

A Lei n.º 12.846/2013 (Lei Anticorrupção) foi criada em um contexto global de crescente preocupação com a integridade nas relações entre os setores público e privado, inspirando-se em legislações internacionais como o *Foreign Corrupt Practices Act* dos Estados Unidos (ESTADOS UNIDOS DA AMÉRICA, 1977). A lei reflete o compromisso do Brasil ao ratificar a Convenção da OCDE contra a corrupção (BRASIL, 2013).

Os artigos 2ª e 3ª dessa Lei estabelecem a responsabilização objetiva das pessoas jurídicas por atos lesivos contra a administração pública, nacional ou estrangeira, abrangendo a esfera civil e administrativa, sem prejuízo da responsabilização individual de dirigentes ou administradores (BRASIL, 2013).

Além do caráter punitivo, a Lei Anticorrupção valoriza a prevenção e a integridade corporativa, pela adoção de Programas de Integridade, que são um conjunto de medidas institucionais e procedimentos internos voltados à prevenção, detecção e remediação de atos ilícitos. A existência e efetividade desses programas podem atenuar penalidades, conforme estipulado pela própria legislação (BRASIL, 2013).

O *compliance* empresarial surgiu como um instrumento necessário para garantir a aplicação prática das legislações e normativas no ambiente corporativo, visando estruturar mecanismos preventivos e promover uma cultura ética organizacional. *Compliance* deriva do verbo inglês *to comply* (conformar-se ou obedecer), refere-se à implementação de procedimentos e controles internos para assegurar o cumprimento da legislação, não eliminando totalmente a possibilidade de ilícitos, mas reduzindo sua incidência e estabelecendo formas eficazes de detecção e resposta (Mendes; Carvalho, 2017, p. 26).

De acordo com Pauseiro e Paiva (2019, p. 15), o *compliance* é uma ferramenta de combate à corrupção, mitigando responsabilidades empresariais e de administradores em relação a práticas antiéticas e ilícitas, além de preservar a imagem e reputação institucional. Embora essencial, não é obrigatório para todas as empresas brasileiras.

A Lei n.º 12.846/2013 (Lei Anticorrupção) e outras normativas setoriais, como as Resoluções da Agência Nacional de Saúde Suplementar (ANS), incentivam sua adoção, mas não há uma regulamentação unificada que obrigue sua estruturação. Empresas que optam por implementá-lo criam setores específicos voltados para a conformidade com normas, como a Lei Anticorrupção (BRASIL, 2013), a Lei de Lavagem de Dinheiro (BRASIL, 1998), a Lei de Licitações (BRASIL, 2021) e a Lei Geral de Proteção de Dados (BRASIL, 2018).

A importância do *compliance* é ressaltada pela baixa pontuação do Brasil no Índice de Percepção da Corrupção da Transparência Internacional (2024), que atribuiu ao país trinta

e quatro pontos, a pior marca desde o início da série histórica em 2012, refletindo alta percepção de corrupção. Giddens (1990, p. 40) destaca que a confiança, essencial para a reputação institucional, está associada à credibilidade de pessoas ou sistemas, baseada na integridade ou competência técnica, elementos cruciais para a valorização mercadológica das empresas.

O *compliance* digital, como extensão do *compliance* tradicional, visa implementar medidas alinhadas à LGPD nas empresas, abrangendo também a prevenção de incidentes no ambiente digital. Embora a LGPD exija formalmente apenas o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), sua elaboração pressupõe procedimentos internos conduzidos pelo *Data Protection Officer* (DPO), responsável pela interlocução entre a empresa, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), conforme art. 5º, VIII da LGPD (BRASIL, 2018).

Para Cunha et al. (2021) a adequação à LGPD começa pela criação de um comitê de proteção de dados, integrado pelos setores estratégicos da organização, incluindo gestão de pessoas, tecnologia da informação, financeiro, jurídico, *marketing*, *compliance* e alta direção. Esse comitê supervisiona o processo de adequação e aprova as políticas internas. Em seguida, realiza-se o *Data Mapping*, que identifica os dados tratados, seu ciclo de vida, formas de armazenamento, acesso e finalidade, possibilitando avaliar a maturidade e as vulnerabilidades da organização frente aos princípios da LGPD (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

Com esse mapeamento, os responsáveis pela segurança da informação elaboram relatórios, apontando os sistemas e processos mais suscetíveis a incidentes. A partir desses relatórios, o DPO elabora uma matriz de risco, classificando os riscos conforme seu impacto (financeiro, jurídico e reputacional) e a probabilidade de ocorrência, subsidiando decisões estratégicas de mitigação e fortalecendo a governança digital (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

Com base nessa matriz, o RIPD é então desenvolvido, visando identificar, analisar e mitigar riscos relacionados ao tratamento de dados pessoais. Esse relatório possui caráter dinâmico, devendo ser constantemente atualizado para acompanhar as mudanças nos processos internos, sendo o principal documento exigido pela LGPD e podendo ser requisitado pela ANPD, especialmente em caso de incidentes (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023).

Concluído esse diagnóstico, elabora-se a Política de Proteção de Dados Pessoais, documento de acesso amplo, que estabelece diretrizes e padrões de segurança para o

tratamento de dados, desde a admissão de colaboradores até o descarte de informações pessoais (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

A formalização desses procedimentos por si só não garante efetividade. Segundo a Controladoria-Geral do Estado do Paraná (2021), o sucesso do *compliance* digital depende do engajamento de todos, sendo essencial a realização de programas contínuos de capacitação e treinamento, voltados à identificação de riscos, boas práticas de segurança e consequências jurídicas e administrativas de vazamentos de dados.

No setor da Saúde Suplementar, a adoção de Programas de Integridade está alinhada às exigências da LGPD, do Decreto n.º 11.129/2022 e das Resoluções Normativas da ANS, contribuindo para mitigar riscos de vazamento de dados e violações de privacidade (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021). Embora não obrigatórios, são programas frequentemente adotados por empresas interessadas em benefícios regulatórios e em participar de determinadas operações.

O Programa de Integridade previsto no art. 56 do Decreto n.º 11.129/2022 reúne mecanismos internos, auditorias, incentivos à denúncia de irregularidades e aplicação de códigos de ética e conduta, reduzindo os efeitos da corrupção e promovendo a confiança institucional. Porto (2020) explica que sua efetividade depende da consolidação de nove pilares: comprometimento da alta administração, avaliação periódica de riscos, códigos e políticas claras, controles internos eficientes, treinamento contínuo, canal de denúncias seguro, investigações internas imparciais, due diligence em terceiros e auditorias sistemáticas.

O Decreto n.º 11.129/2022 estabelece critérios de avaliação desses programas, incluindo políticas abrangentes, treinamentos, gestão de riscos, registros contábeis fidedignos, canais de denúncia e mecanismos de correção de falhas (BRASIL, 2022).

No mesmo sentido, a RN n.º 507/2022 da ANS determina, no item 1.2.11, a criação de uma estrutura de *compliance* para implementar e fiscalizar o código de conduta (ANS, 2022). Os itens 1.2.12 e 1.2.17 exigem a formalização de políticas de integridade e a integração do programa a áreas estratégicas como recursos humanos, jurídico, auditoria e finanças (ANS, 2022). A implantação adequada de Programas de Integridade, estruturados conforme os pilares de Porto (2020) e os parâmetros legais vigentes é fundamental para operadoras de saúde que buscam certificações, vantagens regulatórias e reconhecimento de boas práticas, reforçando o compromisso com a ética, a segurança e a proteção dos usuários.

4 O CASO KLARA CASTANHO E O VAZAMENTO DE DADOS NA SAÚDE

Em 2022, a atriz Klara Castanho teve sua privacidade violada quando informações sobre seu parto foram divulgadas sem consentimento. O episódio começou em 24 de maio, com publicação de Matheus Baldi no Instagram, posteriormente retirada a pedido da atriz, mas já amplamente disseminada (FOLHA DE S.PAULO, 2022).

Em seguida, o caso foi indiretamente mencionado por Leo Dias no programa The Noite (CANAL THE NOITE, 2022) e, depois, por Antônia Fontenelle, que, em transmissão ao vivo, detalhou a situação e afirmou que uma atriz teria pedido a exclusão de registros hospitalares (FONTENELLE, 2022). A repercussão forçou Klara a se pronunciar por meio de carta aberta, em 25 de junho. No mesmo dia, Leo Dias publicou no portal Metrópoles a matéria "Estupro, gravidez indesejada e adoção: a verdade sobre Klara Castanho", expondo nome, imagem e dados do nascimento, o que configurou violação de privacidade, levando à exclusão da reportagem e a um pedido público de desculpas (FANTÁSTICO, 2022).

O Hospital Brasil, da Rede D'Or São Luiz, manifestou solidariedade e abriu apuração interna (PORTAL G1, 2022). O Conselho Federal de Enfermagem (COFEN) anunciou investigações (ESTADÃO, 2023), mas o COREN-SP arquivou o processo por falta de provas, mantendo-o aberto para eventuais novos elementos (COREN-SP, 2022).

Apesar da gravidade, a Autoridade Nacional de Proteção de Dados (ANPD) e a Agência Nacional de Saúde Suplementar (ANS), órgãos competentes pela fiscalização da proteção de dados sensíveis, não instauraram procedimentos ou se pronunciaram oficialmente.

O Hospital Brasil foi condenado em primeira instância a pagar um milhão de reais por danos morais, valor posteriormente reduzido para duzentos mil reais pelo Tribunal de Justiça de São Paulo. No acórdão, o relator Francisco Loureiro destacou a violação do sigilo profissional e a responsabilidade institucional sobre informações sensíveis, fundamentando-se na Constituição e na LGPD. Esse episódio ilustra as graves consequências do descumprimento das normas de proteção de dados na saúde e justifica o aprofundamento desta pesquisa sobre as sanções cabíveis e o papel do *compliance* na prevenção, mitigação de danos e promoção de ética e responsabilidade institucional.

A análise do caso Klara Castanho parte da Constituição Federal de 1988, que no art. 5º, X e LXXIX garante a inviolabilidade da intimidade, vida privada, honra, imagem e dados pessoais, assegurando indenização em caso de violação (BRASIL, 1988). A divulgação, sem consentimento, de informações médicas e pessoais violou diretamente esses direitos. O art. 17 do Código Civil veda a exposição ao desprezo público, mesmo sem intenção difamatória e o art. 21 protege a vida privada (BRASIL, 2015). A Súmula 403 do Superior Tribunal de Justiça (STJ) determina que a indenização pela publicação não autorizada da imagem independe da

prova de prejuízo, o que abrange os veículos que lucraram com o caso.

No campo digital, o Marco Civil da Internet proíbe práticas que atentem contra a privacidade e os dados pessoais, mesmo sob o argumento de liberdade de expressão (BRASIL, 2014), especialmente no art. 7º, I. Ainda mais grave foi a afronta à LGPD, que exige consentimento para o tratamento de dados, nos termos dos arts. 7º, I e 8º, § 3º (BRASIL, 2018). Foram violados princípios como finalidade, necessidade, transparência e segurança, além dos fundamentos de respeito à privacidade e intimidade, com a divulgação de dados sensíveis, conforme art. 5º, II da LGPD.

A responsabilidade do hospital é objetiva, baseada na teoria do risco, pois a instituição tinha o dever de proteger as informações (BRASIL, 2018, art. 42). Segundo Venosa (2023, p. 305), ainda que os direitos da personalidade sejam extrapatrimoniais, o ordenamento prevê compensação pelos danos morais.

Na esfera judicial, a indenização fixada inicialmente em um milhão de reais foi reduzida para duzentos mil reais. Frente ao "lucro bruto da Rede D'Or São Luiz, de R$ 9,462 bilhões" (REDE D'OR, 2024, p. 17), a condenação corresponde a apenas 0,0021%, muito abaixo do limite de 2% previsto no art. 52, II da LGPD (BRASIL, 2018). Venosa (2023, p. 797) defende que o valor deveria considerar a gravidade e extensão do sofrimento, o que não ocorreu, demonstrando a fragilidade na reparação.

Jurisprudência semelhante reforça essa conclusão: o TJSP aplicou a Súmula 479 do STJ em caso de vazamento por instituição financeira (TJSP, 2021), enquanto o TJCE condenou hospital pelo uso indevido de dados (TJCE, 2024).

Quanto à imprensa, embora o art. 43 da LGPD permita o tratamento de dados para fins jornalísticos, não autoriza a divulgação irresponsável de informações obtidas ilicitamente (BRASIL, 2018). O STJ já reconheceu o direito à desindexação de conteúdos ofensivos, exigindo a retirada de informações pessoais irrelevantes ao interesse público (STJ, 2020).

Assim, apesar da sólida proteção legal e de precedentes rigorosos, o caso evidencia a insuficiência das sanções e a dificuldade institucional em reconhecer a gravidade dos danos provocados pelo vazamento de dados sensíveis.

A análise administrativa do caso evidencia a ausência de atuação da Autoridade Nacional de Proteção de Dados (ANPD) que, segundo a LGPD, possui competência para aplicar sanções e adotar medidas preventivas e corretivas (BRASIL, 2018).

A atuação da ANPD tem caráter orientativo e responsivo, priorizando a prevenção e a colaboração antes da penalidade, sendo a comunicação prévia de incidentes considerada atenuante (BRASIL, 2018, art. 52, § 2º, II). Caso notificada a ANPD avaliaria a gravidade do

vazamento e poderia impor sanções, como publicização da infração ou eliminação de dados pessoais (BRASIL, 2018, art. 52, IV e VI), que, além de comprometer a imagem da empresa, impactariam seu valor de mercado.

No plano ético, o Código de Ética dos Profissionais de Enfermagem proíbe a divulgação de informações obtidas no exercício profissional sem consentimento, previsão legal ou decisão judicial, o que não ocorreu no caso (COFEN, 2017).

Institucionalmente, a Agência Nacional de Saúde Suplementar (ANS) impõe obrigações de governança e segurança da informação. A RN n.º 507/2022 exige termos de confidencialidade e armazenamento seguro dos dados (ANS, 2022a), enquanto a RN n.º 518/2022 determina a implementação de normas de conduta e programas efetivos de integridade (ANS, 2022b).

Apesar da Rede D'Or São Luiz declarar possuir treinamentos, Código de Conduta, Política de Integridade e Política de Privacidade (REDE D'OR, 2025), não há evidências públicas de que esses mecanismos estavam plenamente estruturados ou aplicados na época.

O Código de Conduta da operadora prevê genericamente a proteção de dados e o dever de sigilo, mas carece de menções específicas à divulgação de informações em ambiente digital ou à proibição de compartilhamento de prontuários (REDE D'OR, 2025). Sanções internas estão previstas, variando de advertências a suspensão ou substituição de terceiros (REDE D'OR, 2025).

Quanto à Política de Privacidade, a operadora afirma seguir os padrões da LGPD, nomeando encarregado e adotando mecanismos de segurança, mas não apresenta publicamente estruturas completas de *compliance* digital, como Comitê de Proteção de Dados, mapa de riscos ou Relatório de Impacto (REDE D'OR, 2025).

Embora existam normas legais e éticas claras houve falha na aplicação efetiva das medidas preventivas e de controle, tanto pelo hospital quanto pela profissional de enfermagem, além de condutas impróprias por jornalistas e veículos de imprensa. Esse cenário resultou na violação de direitos fundamentais como intimidade, privacidade e proteção de dados, com uma condenação judicial de valor simbólico e limitado efeito pedagógico.

5 CONCLUSÃO

A análise crítica do caso Klara Castanho, inserido no contexto da proteção de dados sensíveis no setor da saúde suplementar brasileira, evidencia profundas fragilidades

institucionais e operacionais na efetiva garantia dos direitos fundamentais relacionados à privacidade e à intimidade dos titulares de dados.

O episódio trouxe à tona não apenas a violação concreta da privacidade de uma paciente, mas também expôs a deficiência estrutural de mecanismos preventivos e sancionatórios, tanto no âmbito administrativo quanto judicial e ético-profissional.

Ao longo desta pesquisa, verificou-se que, apesar do avanço normativo representado pela Lei Geral de Proteção de Dados (LGPD), pela Constituição Federal, pelo Marco Civil da Internet e pelas resoluções da Agência Nacional de Saúde Suplementar (ANS), a aplicação prática dessas normas encontra obstáculos evidentes, sobretudo diante da ausência de uma cultura institucional sólida de proteção de dados.

A falta de uma governança informacional eficaz e a carência de ações integradas e articuladas entre os diversos atores envolvidos no caso contribuíram diretamente para a perpetuação das violações.

A atuação insuficiente e fragmentada das instituições responsáveis ficou patente na resposta limitada e tardia oferecida após a divulgação indevida dos dados da atriz. O caso resultou, até o momento, apenas em condenações pontuais, sem uma resposta institucional efetiva e coordenada que abarcasse a complexidade das infrações cometidas.

A ausência de sanções exemplares, de medidas administrativas rígidas e de orientações corretivas preventivas demonstra o descompasso entre o ordenamento jurídico brasileiro e a realidade institucional das práticas de segurança informacional no setor da saúde. Nesse cenário, a pesquisa confirmou a hipótese inicialmente sustentada, de que a inexistência de um *compliance* digital estruturado, associado à fragilidade na articulação entre as esferas administrativa, judicial e ético-profissional, potencializou a violação dos direitos fundamentais da atriz.

A falha no tratamento de dados sensíveis, agravada pela exposição pública da vítima, evidencia a urgente necessidade de fortalecimento das políticas institucionais voltadas à segurança da informação e à proteção dos dados pessoais na saúde suplementar.

A análise realizada demonstrou, ainda, que os programas de *compliance* digital, quando implementados com rigor técnico e compromisso ético, configuram-se como ferramentas estratégicas e indispensáveis para assegurar a conformidade regulatória e mitigar riscos relacionados ao vazamento de informações.

Elementos como o mapeamento de dados (*Data Mapping*), a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a capacitação contínua dos profissionais envolvidos no tratamento de dados revelaram-se medidas fundamentais para a consolidação

de um ambiente organizacional seguro e responsável.

Além disso, a pesquisa evidenciou a importância de ações preventivas e educativas voltadas à conscientização dos profissionais de saúde e de comunicação sobre as implicações éticas, jurídicas e sociais associadas à divulgação não autorizada de informações sensíveis.

A responsabilização ética, administrativa e judicial de todos os agentes envolvidos na cadeia do vazamento é imprescindível para garantir o respeito aos direitos dos titulares de dados, funcionando não apenas como reparação, mas também como medida pedagógica e preventiva.

No campo administrativo, destacou-se a necessidade de maior protagonismo da Agência Nacional de Proteção de Dados (ANPD) e da ANS na fiscalização, orientação e punição de infrações relacionadas ao tratamento de dados sensíveis no setor da saúde suplementar.

A ausência de sanções administrativas e de auditorias específicas evidencia a fragilidade da atuação regulatória no caso concreto, ressaltando a importância de mecanismos mais eficazes de monitoramento e controle.

O caso Klara Castanho constitui um marco simbólico e jurídico relevante para a evolução da proteção de dados no Brasil, sobretudo no ambiente sensível da saúde suplementar. Reforça a urgência de alinhar a legislação vigente a práticas institucionais consistentes e a uma cultura organizacional comprometida com a privacidade e a dignidade dos indivíduos. A efetividade das normas de proteção de dados não depende apenas de dispositivos legais bem elaborados, mas principalmente da internalização desses princípios pelas instituições e profissionais, do aprimoramento dos sistemas de *compliance* digital e da atuação coordenada e transparente dos órgãos de controle.

Assim, reafirma-se que a preservação da privacidade e da dignidade dos titulares de dados passa, necessariamente, pela adoção de políticas institucionais robustas, programas de *compliance* digital eficazes e uma atuação estatal proativa, preventiva e punitiva, capaz de resguardar os direitos fundamentais assegurados pela Constituição e pela legislação brasileira.

O episódio analisado deixa clara a necessidade de revisão e fortalecimento das práticas institucionais no setor da saúde suplementar, para que casos semelhantes não se repitam, garantindo-se, assim, a integridade, o respeito e a segurança informacional dos pacientes.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais** (RIPD). Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p9. Acesso em: 05 mar. 2025.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. **Constituição de 1988**. Brasília, DF: Diário Oficial da União, 1988.

BRASIL. **Decreto nº 11.129, de 11 de julho de 2022**. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Diário Oficial da União, 2022.

BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 14 abr. 2025.

BRASIL. **Lei nº 12.695, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 2014.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Diário Oficial da União, 2013.

BRASIL. **Lei nº 13.509, de 22 de novembro de 2017**. Dispõe sobre a adoção e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.542, de 1º de maio de 1943, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil). Brasília, DF: Diário Oficial da União, 2017.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Diário Oficial da União, 2018.

BRASIL. **Superior Tribunal de Justiça**. Recurso Especial nº 1.660.168/RJ. 3ª Turma. Relatora: Ministra Nancy Andrighi. Relator para Acórdão: Ministro Marco Aurélio Bellizze. Julgado em 08 maio 2018. Publicado no DJe em 05 jun. 2018.

BRASIL. **Superior Tribunal de Justiça**. Recurso Especial nº 2.086.404-MG. 3ª Turma. Relator: Ministro Moura Ribeiro. Julgado em 29 set. 2024. Informativo 835.

CANAL THE NOITE. Leo Dias – **The Noite**. YouTube, 2025. Disponível em: https://www.youtube.com/watch?v=8L-aZnhHO7M&t=49s. Acesso em: 30 mar. 2025.

CARVALHO, Vinicius Marques; MENDES, Francisco Schertel. **Compliance**: concorrência e combate à corrupção. São Paulo: Trevisan Editora, 2017.

CASTANHO, Klara Forkas Gonçalez. **Carta aberta**. 25 de junho de 2022. Instagram:

@klarafgcastanho. Disponível em: https://www.instagram.com/p/CfPvGDkuii1/?img_index=1. Acesso em: 30 mar. 2025.

CEARÁ. **Tribunal de Justiça**. 1ª Câmara de Direito Privado. Processo nº XXXXX-59.2022.8.06.0001. Rel. Des. Francisco Mauro Ferreira Liberato, Fortaleza. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ce/2782154644. Acesso em: 31 mar. 2025.

CHECK POINT. **Security Report 2022**. Check Point Research, 2022. Disponível em: https://research.checkpoint.com. Acesso em: 08 abr. 2025.

CHECK POINT RESEARCH. **Security Report 2025**. Check Point Research, 2025. Disponível em: https://research.checkpoint.com. Acesso em: 13 abr. 2025.

CONSELHO FEDERAL DE ENFERMAGEM (COFEN). **Resolução COFEN nº 311/2007**. Disponível em: http://www.cofen.gov.br. Acesso em: 10 de mar. de 2025.

CONSELHO FEDERAL DE ENFERMAGEM (COFEN). **Resolução nº 564/2017**. Disponível em: https://www.cofen.gov.br/resolucao-cofen-no-5642017/. Acesso em: 12 mar. 2025.

CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica**. Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019. Brasília: Conselho Federal de Medicina, 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Instrução Normativa nº 03/21**. Disponível em: https://portal.cfm.org.br/noticias/cfm-regulamenta-tratamento-de-dados. Acesso em: 08 mar. 2025.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução nº 1.605/2000**. Disponível em: https://www.saude.df.gov.br/documents/37101/0/CFM.pdf/e426a5e2-7143-d957-793b-0185b9018526?t=1660222456231. Acesso em: 11 mar. 2025.

CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO. **Nota Oficial**. Coren-SP. São Paulo, 2022. Disponível em: https://portal.coren-sp.gov.br/noticias/caso-klara-castanho-coren-sp-detalha-sindicancia-e-mantem-se-a-disposicao-da-atriz/. Acesso em: 10 mar. 2025.

CONTROLADORIA-GERAL DO ESTADO DO PARANÁ. **Manual de implementação da LGPD**. Curitiba: CGE/PR, 2021. Disponível em: https://www.cge.pr.gov.br/sites/default/ arquivos_restritos/files/documento/2021- 06/manual_implementacao_lgpd.pdf. Acesso em: 05 de mar de 2025.

CUNHA, Blenda Eduarda de Melo et al. **As dificuldades de implementação da LGPD no Brasil**. Revista Projeto Extensionistas, Pará de Minas, v.1, n. 2, p. 39-47,jul./dez. 2021. Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249. Acesso em: 05 mar. 2025.

DALLARI, A. B.; MARTINS, A. C. M. S. **Proteção e compartilhamento de dados entre profissionais e estabelecimentos de saúde**. São Paulo: Revista dos Tribunais, 2021.

DATA PROTECTION AUTHORITY. Disponível em: https://iapp.org/resources/article/data-protection-authority/. Acesso em: 19 mai. 2023.

ESTADÃO. **Conselho de Enfermagem arquiva investigação sobre caso Klara Castanho e nega vazamento de informação**. Estadão. São Paulo, 2023. Disponível em: https://www.estadao.com.br/emais/gente/coren-sp-arquiva-investigacao-sobre-caso-klara-castanho-e-nega-vazamento-de-informacao/. Acesso em: 07 mar. 2025.

ESTADOS UNIDOS DA AMÉRICA. **A Resource Guide to the FCPA U.S**. Foreign Corrupt Practices Act. Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, 2012. Disponível em: www.sec.gov/spotlight/fcpa.shtml. Acesso em: 14 mar. 2025.

ESTADOS UNIDOS DA AMÉRICA. **Foreign Corrupt Practices Act** (FCPA), 1977.

FANTÁSTICO. **Globoplay**. Disponível em: https://globoplay.globo.com/v/10704497/. Acesso em: 30 mar. 2025.

FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Direito civil**: teoria geral. 4. ed. Rio de Janeiro: Lumen Juris, 2006.

FOLHA DE S. PAULO. **Klara Castanho**: jornalista que expôs o caso é demitido. 2022. Disponível em: https://f5.folha.uol.com.br/celebridades/2022/07/klara-castanho-jornalista-que-expos-o-caso-e-demitido.shtml. Acesso em: 30 mar. 2025.

FONTENELLE, Antonia. **Entrevista com Antonia Fontenelle**. YouTube, 2022. Disponível em: https://www.youtube.com/watch?v=e-sCKj_9b5g. Acesso em: 30 mar. 2025.

GIDDENS, Anthony. **As consequências da modernidade**. Tradução de Raul Fiker. São Paulo: UNESP, 1991.

KELSEN, Hans. **Teoria geral do direito e do Estado**. Tradução de Luís Carlos Borges. 3. ed. São Paulo: Martins Fontes, 2000. Disponível em: https://estudos001.files.wordpress.com/ 2014/02/hans-kelsen-teoria-geral-do-direito-e-do- estado.pdf. Acesso em: 06 mar. 2025.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 20. ed. São Paulo: Saraiva, 2016.

MINAS GERAIS. **Tribunal de Justiça**. Processo nº XXXXX-47.2024.8.05.0001. Procedimento Comum Cível. Julgado em 27 abr. 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ba/2845982954/inteiro-teor-2845982958. Acesso em: 31 mar. 2025.

MINISTÉRIO DA SAÚDE. **Resolução Normativa - RN nº 507, de 30 de março de 2022**. Brasília, DF: Diário Oficial da União, 2022.

MINISTÉRIO DA SAÚDE. **Resolução Normativa - RN nº 518, de 29 de abril de 2022**. Brasília, DF: Diário Oficial da União, 2022.

PAUSEIRO, Sérgio Gustavo de Mattos; PAIVA, Marcella da Costa Moreira de. **Compliance e operadoras de planos de assistência à saúde**. In: V Seminário Internacional sobre Direitos Humanos Fundamentais. Anais. João Pessoa: UNIPÊ, 2019.

PECK, Patricia. **Proteção de dados pessoais**: comentários à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados). São Paulo: Saraiva Educação, 2021.

PORTAL G1. **Conselho de enfermagem vistoria hospital de SP acusado de vazar informações de Klara Castanho**. São Paulo, 2022a. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/06/28/conselho-de-enfermagem-vistoria-hospital-de-sp-acusado-de-vazar- informacoes-de-klara-castanho.ghtml. Acesso em: 07 mar. 2025.

PORTO, Ederson Garin. **Compliance e Governança Corporativa**. São Paulo: Lawboratory Press, 2020.

REDE D'OR SÃO LUIZ. **Aviso de Privacidade**. Disponível em: https://dpo.privacytools.com.br/policy-view/DPO8r0aQk/1/aviso-de-privacidade/pt_BR. Acesso em: 03 abr. 2025.

REDE D'OR SÃO LUIZ. **Central de Resultados**. Disponível em: https://ri.rededorsaoluiz.com.br/informacoes-financeiras/central-de-resultados/. Acesso em: 03 abr. 2025.

REDE D'OR SÃO LUIZ. **Código de Conduta**. Disponível em: https://www.rededorsaoluiz.com.br/sustentabilidade-2023/governanca/programa-de- integridade/index.html. Acesso em: 03 abr. 2025.

REDE D'OR SÃO LUIZ. **Programa de Integridade**. Disponível em: https://www.rededorsaoluiz.com.br/sustentabilidade-2023/governanca/programa-de-integridade/index.html. Acesso em: 03 abr. 2025.

SÃO PAULO. **Tribunal de Justiça**. 16ª Câmara de Direito Privado. Processo nº 1001588-65.2021.8.26.0268, Rel. Ana Rita de Figueiredo Nery, Itapecerica da Serra, 20 set. 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2641137443/inteiro-teor-2641137445. Acesso em: 31 mar. 2025.

SENADO FEDERAL. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Senado Notícias, 01 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 31 mar. 2025.

TARTUCE, Flávio. **Manual de Direito Civil**: volume único. 12. ed. Rio de Janeiro: Forense, 2022.

TRANSPARÊNCIA INTERNACIONAL. **Índice de Percepção da Corrupção 2024**. Disponível em: https://transparenciainternacional.org.br/ipc/2024. Acesso em: 16 mar. 2025.

TRIBUNAL REGIONAL DO TRABALHO DA 10ª REGIÃO. **Tutorial de Mapeamento de Riscos**. Disponível em: https://estrategia.trt10.jus.br/plano-de-gestao-de-riscos/item/485-tutorial-de-mapeamento-de-riscos.html. Acesso em: 06 mar. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. EUR-Lex, 2016. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 04 mar. 2025.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho**, de

27 de abril de 2016. EUR-Lex, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 04 mar. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho**, de 23 de outubro de 2018. EUR-Lex, 2018. Disponível em: https://eur-lex.europa.eu/eli/reg/2018/1725/oj. Acesso em: 04 mar. 2025.

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados** (GDPR). 2016. Disponível em:https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html. Acesso em: 03 mar. 2025.

VENOSA, Sílvio de Salvo. **Direito civil**: Obrigações e Responsabilidade Civil. 23. ed. Barueri: Atlas, 2023.

VENOSA, Sílvio de Salvo. **Direito civil**: Parte Geral. 23. ed. Barueri: Atlas, 2023.