VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Caio Augusto Souza Lara; Claudia Maria Da Silva Bezerra; José Carlos Francisco dos Santos. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-160-8
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. Direito. 3. Governança e novas tecnologias. 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

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Os artigos contidos nesta publicação foram apresentados no Grupo de Trabalho Direito, Governança e Novas Tecnologias I durante o VIII Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, realizado nos dias 24 a 28 de junho de 2025, sob o tema geral “Direito, Governança e Políticas de Inclusão”. Trata-se da oitava experiência de encontro virtual do CONPEDI em mais de três décadas de existência.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central grupo. Essa temática traz consigo os desafios que as diversas linhas de pesquisa jurídica enfrentam no tocante ao estudo dos referenciais teóricos do tema governança e seus impactos no universo tecnológico.

A publicação reúne pesquisas que que exploram os impactos jurídicos, éticos e sociais da inteligência artificial e das tecnologias digitais sobre o Estado Democrático de Direito, com foco especial na proteção de direitos fundamentais. As discussões abrangem temas como o uso de IA na Defensoria Pública e na dosimetria da pena, o risco de vieses algorítmicos no policiamento preditivo, e os limites constitucionais da automação decisória. Também são abordadas as responsabilidades civis dos agentes de IA, a regulação do mercado de criptoativos, a proteção de dados sensíveis (como prontuários médicos), e a necessidade urgente de regulamentar ilícitos eleitorais e obras autorais geradas por IA. A interseção entre transparência, governança algorítmica e acesso à justiça é outro eixo central, com reflexões

tecnologia, com base em autores como Douglas Rushkoff, e sugere caminhos para um novo paradigma regulatório que una inovação, equidade, sustentabilidade e respeito aos direitos humanos.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, com artigos rigorosamente selecionados, por meio de dupla avaliação cega por pares (double blind peer review). Dessa forma, todos os artigos ora publicados guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

Caio Augusto Souza Lara

Claudia Maria Da Silva Bezerra

José Carlos Francisco dos Santos

A PROTEÇÃO DE DADOS DE PRONTUÁRIOS MÉDICOS

MEDICAL RECORDS DATA PROTECTION

Edith Maria Barbosa Ramos [1]
Pedro Gonçalo Tavares Trovão do Rosário [2]
Dennys Damião Rodrigues Albino [3]

Resumo

O presente artigo científico aborda como a proteção adequada dos dados contidos em prontuários médicos é um desafio crucial na era da digitalização da saúde. A pesquisa explora e analisa as principais soluções e abordagens para garantir a privacidade e segurança dos dados médicos sensíveis. Abordou-se a implementação de medidas técnicas, organizacionais e legais para enfrentar os desafios relacionados ao acesso não autorizado, vazamentos de dados, conformidade com as legislações de proteção de dados, integração de sistemas, conscientização dos profissionais de saúde e a responsabilidade das instituições médicas. Trata-se de pesquisa bibliográfica promovida mediante o método de abordagem indutivo, por meio de procedimento jurídico-descritivo e jurídico-propositivo. Conclui-se que a proteção de dados de prontuários médicos é um desafio contínuo que requer um esforço conjunto de profissionais de saúde, instituições médicas e autoridades reguladoras. A implementação de medidas técnicas, organizacionais e legais é fundamental para garantir a privacidade e segurança das informações sensíveis dos pacientes. Tal pesquisa é relevante, visto que, em virtude do crescente avanço tecnológico e do aumento das atividades de tratamento de informações médicas, urge a necessidade de aperfeiçoamento dos mecanismos de proteção de dados sensíveis, não apenas para cumprir as legislações vigentes, mas também como um compromisso ético com os pacientes.

Palavras-chave: Dados sensíveis, Direito à saúde, Prontuários médicos, Lei geral de proteção de dados, Regulamento geral de proteção de dados

Abstract/Resumen/Résumé

analyzes the main solutions and approaches to ensure the privacy and security of sensitive medical data. The implementation of technical, organizational and legal measures to address the challenges related to unauthorized access, data leaks, compliance with data protection laws, system integration, awareness of health professionals and the responsibility of medical institutions were addressed. This is bibliographic research promoted through the inductive approach method, through legal-descriptive and legal-prepositive procedures. It is concluded that the protection of medical record data is an ongoing challenge that requires a joint effort of health professionals, medical institutions and regulatory authorities. The implementation of technical, organizational and legal measures is essential to ensure the privacy and security of sensitive patient information. Such research is relevant, given that, due to the growing technological advances and the increase in medical information processing activities, there is an urgent need to improve mechanisms for protecting sensitive data, not only to comply with current legislation, but also as an ethical commitment to patients.

Keywords/Palabras-claves/Mots-clés: Sensitive data, Right to health, Medical records, General data protection law, General data protection regulation

1. Introdução

A proteção de dados pessoais no contexto da área da saúde tem se tornado um tema de extrema relevância na sociedade contemporânea, em virtude do crescente avanço tecnológico e do aumento das atividades de tratamento de informações médicas. Nesse cenário, o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) do Brasil se destacam como marcos legais que buscam estabelecer diretrizes robustas e fundamentais para assegurar a privacidade e segurança dos dados pessoais contidos nos prontuários médicos.

O RGPD, vigente desde 25 de maio de 2018, é uma legislação abrangente da União Europeia que estabelece princípios, regras e requisitos para o tratamento de dados pessoais de cidadãos da UE, bem como para organizações que atuam em território europeu. Seu escopo de aplicação extraterritorial e alcance global coloca-o como uma referência internacional em matéria de proteção de dados. Por sua vez, a LGPD, em vigor no Brasil desde 18 de agosto de 2020, foi concebida inspirada no RGPD, porém com particularidades adaptadas à realidade brasileira. Essa legislação visa garantir a proteção dos dados pessoais de cidadãos brasileiros, bem como regular as atividades de tratamento de dados realizadas por organizações estabelecidas no país.

Ambos os marcos legais trazem em sua essência princípios fundamentais, tais como a transparência no tratamento de dados, o consentimento do titular das informações, a finalidade legítima do processamento, a minimização dos dados coletados e a prestação de contas das instituições responsáveis pelo tratamento. Contudo, mesmo diante de suas semelhanças, o RGPD e a LGPD apresentam diferenças importantes, tais como a amplitude territorial de sua aplicação e as sanções previstas em caso de descumprimento das normas.

Dessa forma, a presente pesquisa visa trazer alguns pontos de convergência e divergência entre o RGPD e a LGPD, e fazer uma análise focando na proteção de dados pessoais em prontuários médicos à luz da LGPD. Foram abordados os desafios e implicações para instituições de saúde e profissionais do setor, considerando as exigências e direitos dos titulares dos dados. Além disso, foram discutidas as medidas técnicas e organizacionais necessárias para a conformidade com as leis e a promoção de uma cultura de proteção de dados sólida e efetiva.

Por meio dessa pesquisa, buscou-se contribuir para uma compreensão mais aprofundada das legislações de proteção de dados e seus impactos na área da saúde, promovendo a conscientização sobre a importância da privacidade e segurança dos prontuários médicos em

consonância com a LGPD. Ademais, pretendeu-se fornecer subsídios para aprimorar políticas e práticas de proteção de dados nas instituições de saúde, visando garantir o respeito aos direitos dos pacientes e o tratamento adequado das informações sensíveis em prontuários médicos, sem renunciar ao progresso tecnológico que a área médica vem experimentando.

2. Breves considerações sobre a Lei Geral de Proteção de Dados

A sociedade da informação designa a sociedade que se desenvolve a partir da revolução tecnológica iniciada no final do século XX (Castells, 1999). Essa revolução foi marcada pelo surgimento de novas tecnologias de informação e comunicação (TICs), como computadores, internet e redes sociais, que possibilitaram a criação de uma nova infraestrutura tecnológica que conecta pessoas e organizações em todo o mundo.

O mundo hiperconectado traz uma série de benefícios, como a facilidade de acesso à informação, a comunicação instantânea e a colaboração entre pessoas de diferentes partes do mundo. No entanto, também traz uma série de desafios, como a exposição a dados pessoais, a manipulação de informações e a disseminação de desinformação. Acerca dessa nova realidade, Castells (1999, 363) descreve que:

> As pessoas começaram a filmar seus eventos, de férias a comemorações familiares, assim produzindo as próprias imagens, além do álbum fotográfico. Apesar de todos os limites dessa autoprodução de imagens, tal prática realmente modificou o fluxo de mão única das imagens e reintegrou a experiência de vida e a tela. Em muitos países, da Andaluzia ao sul da Índia, a tecnologia de vídeo da comunidade local permitiu o surgimento da transmissão local rudimentar que misturava difusão de filmes de vídeo com eventos e anúncios locais, muitas vezes à margem dos regulamentos de telecomunicações.

Diante dessa nova conjuntura, um dos principais desafios da sociedade da informação passa a ser a proteção de dados pessoais. Os dados pessoais são informações que identificam ou permitem identificar uma pessoa, como nome, endereço, telefone, e-mail, Cadastro de Pessoa Física - CPF, Registro Geral - RG etc. (Pinheiro, 2020). Esses dados podem ser coletados por uma variedade de organizações, como empresas, governos e instituições financeiras.

Os dados pessoais podem ser usados para uma série de fins, como *marketing*, publicidade, análise de mercado, crédito e segurança pública. No entanto, os dados pessoais também podem ser usados para fins maliciosos, como fraudes, chantagens e roubo de identidade. Independente da finalidade, o ponto crucial é que a proteção de dados pessoais é

importante para salvaguardar os direitos fundamentais à preservação da honra, da intimidade e da privacidade (Mulholland, 2018).

Esses direitos são garantidos por diversas leis internacionais e pela própria Constituição Federal brasileira de 1988, que recentemente foi emendada com o acréscimo do inciso LXXIX ao artigo 5º, por meio da Emenda Constitucional nº 115/2022, passando a prever expressamente o direito à proteção dos dados pessoais, inclusive nos meios digitais, como um direito fundamental (Brasil, 2022).

No plano infraconstitucional, se destaca a Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), é o mais importante marco legal brasileiro com o objetivo principal proteger os direitos dos indivíduos em relação aos seus dados pessoais de forma mais abrangente. Em suma, a lei estabelece um conjunto de normas e diretrizes para o tratamento adequado das informações pessoais, com o intuito de promover a privacidade e a segurança dos dados.

A LGPD buscou inspiração no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, que foi implementado pela União Europeia e entrou em vigor em 25 de maio de 2018 (União Europeia, 2016). Seu objetivo é fornecer uma abordagem uniforme para a proteção de dados pessoais dentro dos países membros da União Europeia (UE). O RGPD se aplica a todas as organizações, independentemente de sua localização geográfica, que processam dados pessoais de cidadãos da União Europeia ou que oferecem bens ou serviços a esses cidadãos (União Europeia, 2016). Suas disposições incluem a necessidade de obter o consentimento explícito do indivíduo antes de processar seus dados, a obrigação de informar sobre o uso dos dados pessoais e a imposição de sanções rigorosas para as organizações que não estejam em conformidade.

A partir desse referencial, a Lei Geral de Proteção de Dados Brasileira (LGPD) surgiu, tendo sua edição motivada pela crescente preocupação com o tratamento inadequado e a exploração indevida das informações pessoais, impulsionada pelo avanço tecnológico e a proliferação de serviços e plataformas digitais.

As discussões para a criação da LGPD tiveram início no Congresso Nacional brasileiro e foram iniciadas em 2015 pelo Ministério da Justiça, que recebeu mais de 1.000 contribuições de diversos atores da sociedade. O texto final foi consolidado no PL nº 5.276/2016, destacando a inviolabilidade da intimidade e da vida privada na sociedade de informação. Foi apensado ao PL nº 4.060/2012, seguindo o Regimento Interno da Casa Legislativa (Ramos et al., 2020).

Diversos fatores impulsionaram o debate, entre eles, os escândalos envolvendo o vazamento de dados pessoais em grandes empresas e plataformas online, além da pressão internacional para que a República Federativa do Brasil se adequasse aos padrões de proteção de dados, como os estabelecidos pelo Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Entre esses casos, destaca-se o do *Facebook* e a *Cambridge Analytica*, no qual a empresa de consultoria política utilizou indevidamente dados pessoais de milhões de usuários da rede social para influenciar eleições (Paulo, 2021). Esse incidente levou a uma maior conscientização sobre a privacidade e a necessidade de regulamentações mais rígidas para proteger os dados pessoais.

Outro exemplo é o caso da empresa de tecnologia Google, que recebeu multas significativas por violações do RGPD. Em 2019, a empresa foi multada em 50 milhões de euros pela autoridade de proteção de dados francesa, a Commission Nationale de l'Informatique et des Libertés - CNIL, por falta de transparência e informações inadequadas fornecidas aos usuários em relação ao uso de seus dados (Valente, 2019).

Durante as discussões legislativas, diversos setores da sociedade civil, especialistas em tecnologia, juristas e representantes de empresas, tiveram participação ativa, o que levou a uma elaboração mais abrangente e equilibrada da lei. Foram meses de debates intensos para encontrar o melhor equilíbrio entre a proteção dos direitos individuais e a necessidade de fomentar a inovação e o desenvolvimento econômico do país.

A LGPD foi aprovada em 2018 e entrou em vigor em setembro de 2020, com o objetivo de garantir maior controle sobre o tratamento de dados pessoais e estabelecer regras claras para as empresas e órgãos públicos que lidam com informações pessoais de cidadãos brasileiros (Ramos, et al., 2020). Para Pinheiro (2018, p. 15):

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Os principais aspectos da Lei Geral de Proteção de Dados Brasileira incluem:

Consentimento: O tratamento de dados pessoais só pode ocorrer com o consentimento do titular, que deve ser livre, informado e inequívoco. Isso significa que as empresas precisam solicitar permissão aos usuários antes de coletar, armazenar ou utilizar seus dados.

Direitos dos titulares: A LGPD confere aos titulares dos dados diversos direitos, como o acesso aos dados, a correção de informações incompletas, inexatas ou desatualizadas, a eliminação de dados desnecessários ou tratados em desconformidade com a lei, entre outros.

Responsabilidade das empresas: As organizações que coletam e tratam dados pessoais são responsáveis por garantir a segurança e a privacidade dessas informações, devendo adotar medidas técnicas e administrativas para evitar o acesso não autorizado, a perda ou o vazamento dos dados.

Autoridade Nacional de Proteção de Dados (ANPD): Foi criada a ANPD como órgão responsável pela fiscalização e aplicação da LGPD. A autoridade tem a função de orientar, normatizar e zelar pelo cumprimento da legislação.

Sanções: A LGPD estabelece sanções para as empresas que não cumprirem suas disposições, podendo ser aplicadas advertências, multas, suspensão das atividades de tratamento de dados e até mesmo a proibição total das atividades relacionadas ao tratamento de dados pessoais.

Apesar de trazer diversos elementos da norma de proteção de dados da União Europeia, há algumas diferenças entre o RGPD e a LGPD, entre as quais o fato de que a lei brasileira se aplica apenas a organizações brasileiras, enquanto o RGPD tem alcance internacional.

Tanto a LGPD do Brasil quanto o RGPD da União Europeia possuem disposições relacionadas ao tratamento de dados sensíveis. De acordo com o Art. 11 da LGPD, os dados sensíveis contam com proteção especial e seu tratamento só é permitido nas hipóteses previstas na lei, independentemente do consentimento do titular (Brasil, 2018). Já o GDPR, em seu Art. 9, §2º, 'd' e 'e', proíbe o tratamento de dados sensíveis, com algumas exceções estabelecidas.

Quanto à proteção de dados pessoais de menores, ambas legislações buscam tutelas, mas estabelecem diferentes critérios para a obtenção do consentimento, considerando a idade dos indivíduos envolvidos. De acordo com o Art. 14, §1º da LGPD, todos os menores de 18 anos requerem o consentimento dos pais ou responsáveis para o tratamento de seus dados (Brasil, 2018). Já o RGPD, em seu Art. 8, §1º, aceita o consentimento dado por adolescentes a partir dos 16 anos, porém, para menores de 16 anos, o consentimento deve ser fornecido pelos pais (União Europeia, 2016).

As políticas de proteção de dados também diferem em relação à abordagem para a implementação de programas de governança e privacidade. De acordo com o Art. 50 da lei brasileira, a adoção desses programas é uma escolha facultativa dos controladores de dados (Brasil, 2018). Por outro lado, o RGPD da União Europeia, em seu Art. 24, §2º, estabelece

como obrigação dos controladores a adoção de medidas técnicas e administrativas apropriadas para garantir o cumprimento da legislação (União Europeia, 2016). Dessa forma, o RGPD apresenta uma abordagem mais rígida e mandatória em relação às medidas de segurança e privacidade, enquanto a LGPD permite maior flexibilidade aos controladores na implementação desses programas.

A LGPD e o RGPD abordam ainda a questão dos representantes de empresas de maneira distinta. Segundo o Art. 61 da LGPD, empresas estrangeiras devem designar um agente, representante ou pessoa responsável por sua filial, agência, estabelecimento ou escritório no Brasil, para receber notificações e intimações referentes a atos processuais (Brasil, 2018). Já o RGPD, em seu Art. 27, requer que o controlador ou processador designe, por escrito, um representante em um dos Estados-Membros da União Europeia. Esses representantes têm papel importante na comunicação e interação com as autoridades competentes em questões relacionadas à proteção de dados (União Europeia, 2016).

A responsabilização dos agentes no contexto da proteção de dados é tratada de forma semelhante na LGPD e no RGPD, mas com alguns pontos distintos. De acordo com o Art. 42 e seguintes da LGPD, o controlador/operador não é responsabilizado em três situações: quando não está envolvido no tratamento dos dados, quando o tratamento é realizado de acordo com a legislação, e quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros (Brasil, 2018). Já o RGPD, em seu Art. 82, estabelece duas hipóteses em que o controlador ou operador não é responsabilizado: quando não está envolvido no tratamento dos dados e quando o tratamento é realizado em conformidade com a legislação (União Europeia, 2016). Esses dispositivos visam proporcionar uma base para a responsabilização adequada dos agentes de tratamento de dados, garantindo que sejam responsáveis por suas ações, ao mesmo tempo em que consideram circunstâncias que podem eximi-los de responsabilidade em casos específicos.

No que diz respeito à relação entre controlador e operador, de acordo com o Art. 39 da lei brasileira, o operador é responsável por realizar o tratamento de dados de acordo com as instruções do controlador, sem a exigência de formalização por meio de contrato (Brasil, 2018). Por outro lado, o regulamento da UE, em seu Art. 28 §3º, determina que o tratamento de dados realizado por operador deve ser regido por um contrato ou outro ato jurídico que estabeleça os vínculos entre o controlador e o operador (União Europeia, 2016).

O requisito de Relatório de Impacto à proteção de dados pessoais também fica disciplinado de forma diferente nos normativos. No Art. 38 da LGPD não são especificadas as situações em que o controlador será obrigado a elaborar o relatório, deixando essa definição

para regulamentação posterior (Brasil, 2018). Por outro lado, o RGPD, em seu Art. 25, estabelece que o controlador deve fornecer um relatório de impacto quando o tratamento de dados resultar em elevado risco para os direitos e liberdades das pessoas (União Europeia, 2016). Além disso, o RGPD detalha o conteúdo que deve ser abordado no relatório, proporcionando uma abordagem mais abrangente e específica sobre esse importante mecanismo de proteção de dados.

A Lei Geral de Proteção de Dados (LGPD), nos artigos 33 e seguintes, permite a transferência de dados pessoais para países ou organizações internacionais que ofereçam um nível adequado de proteção de dados, conforme estabelecido. No entanto, a lei é concisa em relação a esse procedimento e aos elementos que devem ser considerados como adequados, fornecendo apenas diretrizes genéricas a serem observadas pelas autoridades nacionais (Brasil, 2018).

Por outro lado, o Regulamento Geral de Proteção de Dados (RGPD), em seus artigos 44 e seguintes, afirma que a transferência internacional de dados pode ser realizada sem autorização específica, caso a Comissão Europeia reconheça que o país terceiro assegura um nível adequado de proteção. Caso contrário, a transferência internacional estará sujeita a garantias apropriadas, que devem ser fornecidas pelo controlador dos dados. Todos os procedimentos e elementos considerados pela Comissão para a autorização da transferência são descritos no RGPD (União Europeia, 2016).

Por último, as sanções previstas na LGPD são proporcionais ao contexto econômico brasileiro, com multas que podem chegar a 2% do faturamento anual da organização ou R$ 50 milhões (Brasil, 2018). Já o RGPD estabelece multas de até 4% do faturamento anual da organização ou € 20 milhões (União Europeia, 2016).

Apesar das diferenças, ambas legislações de proteção de dados, como o RGPD e a LGPD, são reflexo de uma preocupação crescente com a privacidade e a segurança das informações pessoais em um mundo cada vez mais digitalizado. É fundamental que as organizações estejam cientes dessas leis, cumpram seus requisitos e adotem medidas adequadas para proteger os dados pessoais dos indivíduos, sobretudo quando se tratar de dados pessoais sensíveis, tais como os constantes em prontuário médicos.

3. Os desafios de proteger os prontuários médicos

Os prontuários médicos são fontes ricas e detalhadas de informações sobre a saúde dos pacientes, contendo dados sensíveis e confidenciais que refletem seu histórico médico, diagnósticos, tratamentos, exames e outras informações clínicas relevantes. De acordo com o Conselho Federal de Medicina (CFM), pela Resolução n.º 1.638/02, prontuário é o (CFM, 2022, p. 2):

> Documento único, constituído de um conjunto de informações, sinais e imagens registrados, gerados a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo.

Atualmente, há uma crescente quantidade de dados disponíveis sobre pacientes e usuários dos sistemas de saúde. Isso ocorre tanto por meio do uso do prontuário eletrônico, conforme estipulado pela Lei nº 13.787/2018, quanto através do intercâmbio de informações sobre pacientes entre laboratórios, hospitais, clínicas, médicos e grupos de pesquisa (Ramos et al., 2020).

Essa natureza dos dados contidos nos prontuários médicos os torna especialmente valiosos para o cuidado e tomada de decisões clínicas, permitindo que os profissionais de saúde forneçam tratamentos personalizados e eficazes aos pacientes.

No entanto, a violação desses dados pode acarretar graves consequências para os pacientes e para a sociedade em geral. Primeiramente, a exposição indevida de informações pessoais e médicas pode levar à perda de privacidade e confidencialidade, gerando sentimento de insegurança e violação da intimidade dos indivíduos (Leme, Blank, 2020). Essa quebra de confiança pode ter um impacto significativo no relacionamento entre os pacientes e os profissionais de saúde, podendo até mesmo impedir que alguns pacientes busquem tratamento médico quando necessário.

Além disso, a violação dos prontuários médicos pode levar à discriminação e ao estigma dos pacientes. Por exemplo, informações sobre condições médicas específicas, histórico de tratamentos ou exames podem ser usadas indevidamente para rotular ou discriminar indivíduos em situações como emprego, acesso a seguros de saúde ou participação em pesquisas médicas. Essa discriminação pode resultar em consequências negativas na vida dos pacientes, prejudicando suas oportunidades e bem-estar.

Por essa razão, os próprios órgãos e entidades da área da saúde, sob a égide do próprio direito fundamental à inviolabilidade da honra, imagem, intimidade e vida privada, do art. 5º, X, da CF, editaram, mesmo antes do advento da LGPD, normativos e códigos de ética visando

asseverar o caráter sigiloso das informações de prontuários médicos e buscar proteger essas informações.

A título exemplificativo, o Código de Ética Médica estabelece claramente que o médico não pode divulgar informações às quais teve acesso no exercício de sua profissão, a menos que haja uma justa causa, um dever legal ou a autorização expressa do paciente. Além disso, é proibido facilitar o acesso e conhecimento de prontuários, anotações médicas e demais registros sujeitos ao sigilo profissional a pessoas que não estejam vinculadas ao mesmo compromisso de confidencialidade (Conselho Federal de Medicina, 2010).

Por sua vez, o artigo 81 do Código de Ética de Enfermagem estabelece de forma categórica que todas as informações presentes no prontuário médico estão protegidas pelo dever do profissional de enfermagem em manter absoluto sigilo.

Ainda na seara médica, destaca-se ainda, apenas na esfera regulatória do Conselho Federal de Medicina, diversos marcos regulatórios para garantir a proteção e o sigilo dos dados de saúde. A Resolução CFM nº 1.605, de 15 de setembro de 2000, proíbe a divulgação do prontuário ou ficha médica sem o consentimento do paciente. Já a Resolução CFM nº 1.638, de 9 de agosto de 2002, define o prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários em instituições de saúde. A Resolução CFM nº 1.643, de 26 de agosto de 2002 (reestabelecida pela Resolução CFM nº 2.228 de 26 de fevereiro de 2019), regulamenta a prestação de serviços através da Telemedicina. A Resolução CFM nº 1.821, de 23 de novembro de 2007, aprova normas técnicas para a digitalização e uso de sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, permitindo a eliminação do papel e a troca de informações identificadas em saúde. A Resolução CFM nº 1.819, de 22 de maio de 2007, proíbe a inclusão do diagnóstico codificado (CID) ou tempo de doença nas guias da TISS de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde, juntamente com a identificação do paciente. A Resolução CFM nº 2.217, de 27 de setembro de 2018, estabelece o Código de Ética Médica, enquanto a Resolução CFM nº 2.107, de 17 de dezembro de 2014, define e normatiza a Telerradiologia. Essas resoluções são fundamentais para garantir a confidencialidade dos dados de saúde e proteger a privacidade dos pacientes em diversas situações, incluindo o uso da telemedicina e a digitalização de prontuários médicos (Confederação Nacional de Saúde, 2021).

No que tange aos prontuários médicos é de extrema relevância ainda a Lei nº 13.787, de 27 de dezembro de 2018, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Todas essas normas se justificam sobretudo pelo fato de que a maioria dos dados contidos em prontuários médicos estão relacionados à saúde, que "está entre os problemas que mais afligem as pessoas. Desta feita, entende-se que todas as informações geradas em âmbito da saúde, sejam médicas ou de pesquisa, impactam decisivamente os usuários, as empresas e o Poder Público" (Ramos, et al., 2020, p. 246).

Sob a ótica da Lei Geral de Proteção de Dados, todas essas informações são classificadas como dados pessoais sensíveis, que podem ser definidos de acordo com o art. 5º, II, da LGPD como aqueles que se referem à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."

Ao analisar o fato de que os dados dos prontuários médicos podem variar, abrangendo desde informações genéticas e histórico de doenças crônicas até questões sensíveis de saúde mental, emerge a razão pela qual tais dados merecem tratamento legal especial, porque dizem respeito às "características da personalidade do indivíduo e suas escolhas pessoais" (Pinheiro, 2018, p. 26) e cuja exposição desses dados pode levar a uma violação ainda mais profunda da privacidade, gerando discriminação baseada em características individuais ou limitando as liberdades de escolha de uma pessoa (Doneda, 2011). Doneda (2011, p. 191) ensina nesse sentido que:

> O motivo dos dados sensíveis merecerem uma proteção mais intensa é justamente uma consideração probabilística de que tais dados são mais afeitos a apresentarem problemas mais graves quando de sua má utilização – daí exatamente o fato de denominá-los como "sensíveis" em relação aos demais, enfatizando sua peculiaridade neste sentido.

Um caso recente e emblemático de violação de dados sensíveis sobre saúde e como eles tem grande efeito lesivo à honra e à intimidade da pessoa foi o da atriz Klara Castanho. Em meados de 2022, a atriz publicou um texto em suas redes sociais, no qual relatou ter sido vítima de violência sexual, resultando em uma gravidez indesejada. Apesar de ter direito ao aborto legal, ela optou por levar a gestação até o fim e, posteriormente, entregar a criança para adoção. Klara explicou que decidiu compartilhar o "relato mais difícil" de sua vida devido aos diversos comentários e ataques que estava enfrentando nas redes sociais, embora seu nome não tivesse sido mencionado, outras informações divulgadas permitiam sua identificação. Além disso, ela relatou que, logo após o parto, ainda sob efeito da anestesia, uma enfermeira teria especulado em voz alta sobre a possível publicação das informações, causando desconforto e preocupação (BBC, 2022). A atriz vinha sendo alvo de chantagens e pressão por parte de jornalistas que

obtiveram essas informações de profissionais de saúde envolvidas no seu atendimento hospitalar (Dutra, 2022).

Observa-se que a inobservância dos preceitos éticos e das legislações aplicáveis ao sigilo e proteção de dados no caso acima denotam o potencial lesivo de expor a intimidade da pessoa, tornando públicas informações que invadem de forma arbitrária a vida privada do titular dos dados, ocasionando, como nesse exemplo, profundos abalos psicológicos e danos à honra e reputação.

Outro aspecto fundamental quando se trata de dados pessoais sensíveis é o fato de que a proteção desses dados está intrinsecamente relacionada com o princípio da não-discriminação, previsto no inciso IX, do art. 6º da LGPD. Esse princípio visa garantir que o tratamento de dados pessoais seja realizado de forma justa, igualitária e imparcial, assegurando que nenhum indivíduo seja objeto de tratamento discriminatório com base em suas informações pessoais. No que diz respeito à saúde e aspectos de cunho econômico, a legislação foi mais categórica ao proteger esses dados, ao dispor no art. 11 que (Brasil, 2018):

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto os casos de portabilidade de dados quando consentido pelo titular.

Outro aspecto, no contexto da Covid-19, a título ilustrativo, é como o compartilhamento de dados como forma de evitar a propagação do vírus e neutralização da pandemia, teve potencial de tornar o paciente passível de discriminação, de acordo com Ramos et al. (2020, p. 251):

> Ocorre que a adequação do tratamento a um dos dispositivos da LGPD não confere, por si só, o poder absoluto aos controladores e operadores a permissão de coleta, compartilhamento e o armazenamento indiscriminado dos dados pessoais sensíveis dos indivíduos, pois não está claro, na legislação ou nas ações das autoridades, os limites de seu tratamento e utilização. Deve-se, pois, questionar o compartilhamento de todo o prontuário médico do paciente sob o argumento da avaliação do risco da infecção da Covid-19, notadamente quando o paciente for portador de doença grave e passível de discriminação.

Diante da complexidade dessa questão, é preciso verificar que a proteção de dados de prontuários médicos é um desafio de extrema importância e complexidade, considerando a sensibilidade das informações contidas nesses registros e os riscos associados à violação de privacidade e segurança dos pacientes. Para ser possível pensar soluções para tais problemáticas, é necessário antes explorar os principais desafios enfrentados na proteção de dados de prontuários médicos.

Como já exposto, os prontuários médicos contêm informações altamente sensíveis, como histórico de saúde, diagnósticos, tratamentos, exames e dados genéticos. Esses dados são classificados como dados pessoais sensíveis e exigem um nível mais rigoroso de proteção de acordo com as legislações de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. O desafio é garantir que essas informações não sejam indevidamente acessadas, utilizadas ou compartilhadas por pessoas não autorizadas.

Nesse contexto, um dos principais desafios na proteção de dados de prontuários médicos é evitar o acesso não autorizado a essas informações. Isso pode ocorrer por meio de ataques cibernéticos, violação física de documentos ou mesmo por funcionários não autorizados (Demo, Priesnitz Filho, 2019). Em grande parte das redes hospitalares e laboratórios observa-se a ausência de sistemas de controle de acesso e autenticação robustos, que são fundamentais para evitar tais incidentes e garantir que apenas profissionais de saúde autorizados tenham acesso aos prontuários.

Levando em consideração, a crescente quantidade de dados armazenados digitalmente, tal fator aumenta o risco de vazamentos e incidentes de segurança. Os prontuários médicos são alvos atrativos para criminosos cibernéticos, devido à natureza sensível das informações. Um único vazamento de dados pode causar danos irreparáveis à reputação da instituição de saúde, além de prejudicar os pacientes envolvidos.

Dessa forma, ainda há uma dificuldade de compreensão acerca da necessidade de adoção de medidas avançadas de segurança cibernética, como criptografia, monitoramento contínuo e auditorias regulares para identificar e mitigar possíveis vulnerabilidades (Lóssio, 2020). No mesmo sentido, está também a ausência de integração de sistemas de informação para armazenar dados de prontuários médicos. A integração desses sistemas é um desafio, pois garante que os dados sejam consistentes, precisos e acessíveis de forma segura quando necessário. A falta de integração pode dificultar a rastreabilidade dos dados e aumentar o risco de erros ou violações.

Tais medidas são fundamentais para a conformidade com as legislações de proteção de dados, que por serem complexas e estarem em constante evolução, requerem ainda a adoção de políticas, procedimentos e tecnologias que garantam o cumprimento dos princípios e direitos estabelecidos nessas leis, como o direito de acesso, retificação e exclusão dos dados.

Outro grande desafio é a obtenção do consentimento informado e livre dos pacientes para o tratamento de seus dados. O consentimento deve ser obtido de forma clara e explícita,

garantindo que o paciente esteja plenamente ciente de como seus dados serão utilizados e compartilhados. Ainda, é fundamental permitir que o paciente revogue o consentimento a qualquer momento, se assim desejar. Motta (2003) ressalta que o conteúdo do prontuário pertence ao paciente, enquanto o hospital ou instituição é responsável apenas pela sua custódia. Nesse sentido, o acesso e uso das informações contidas no prontuário devem ser destinados exclusivamente ao cuidado do paciente, sendo vedada qualquer divulgação sem a devida autorização prévia do titular.

Ainda nesse sentido, deve ser observado ainda o princípio da finalidade, ainda que se trate de uso dados para fins de pesquisa. Embora a pesquisa médica seja crucial para avanços na área da saúde, o uso inadequado de dados de prontuários para fins de pesquisa pode ser um desafio ético. A anonimização adequada dos dados é fundamental para proteger a identidade dos pacientes e evitar o uso indevido das informações pessoais, de modo que as instituições de saúde devem estabelecer políticas claras para garantir que o uso de dados para pesquisa seja realizado de acordo com os princípios éticos e legais.

A LGPD e o RGPD estabelecem também que os dados pessoais devem ser retidos apenas pelo tempo necessário para a finalidade do tratamento e devem ser descartados de maneira segura após esse período. O desafio é garantir que os prontuários médicos sejam mantidos pelo tempo adequado e, posteriormente, descartados de forma apropriada, evitando a retenção desnecessária e o risco de exposição indevida dos dados.

Por fim, a conscientização e a educação dos profissionais de saúde são fundamentais para enfrentar os desafios na proteção de dados de prontuários médicos. Os profissionais devem ser treinados para compreender a importância da proteção de dados, as políticas institucionais e as práticas seguras de manuseio das informações dos pacientes (Lóssio, 2020).

Em conclusão, a proteção de dados de prontuários médicos é uma questão complexa e crítica que requer esforços contínuos para garantir a privacidade e a segurança dos pacientes. Os desafios incluem a sensibilidade dos dados, o acesso não autorizado, riscos de vazamentos e incidentes de segurança, conformidade com as legislações de proteção de dados, obtenção de consentimento informado e livre, uso adequado de dados para pesquisa, retenção e descarte adequado de dados, integração de sistemas de informação, e a conscientização e educação dos profissionais de saúde. Ao enfrentar esses desafios de maneira proativa e diligente, é possível estabelecer uma base sólida para a proteção de dados de prontuários médicos, assegurando o respeito aos direitos dos pacientes e promovendo um ambiente confiável e seguro para o tratamento médico.

4. Propostas de melhorias para a proteção de dados de prontuários médicos

Proteger as informações de pacientes é uma responsabilidade fundamental para os médicos, especialmente em um contexto de crescente digitalização da saúde, onde os dados sensíveis são armazenados em prontuários médicos eletrônicos e sistemas informatizados. Para garantir a confidencialidade e evitar vazamentos de dados, é essencial adotar um conjunto de medidas proativas de segurança cibernética e governança de informações (Lóssio, 2020).

Uma das principais medidas que podem ser tomadas é a implantação de medidas de segurança cibernética robustas. Isso inclui a utilização de firewalls para monitorar e filtrar o tráfego de rede, a instalação de antivírus atualizados para detectar e prevenir ameaças de malware, o uso de senhas fortes e a implementação de criptografia para proteger as informações em trânsito e em repouso (Brasil, 2020). Ao adotar essas medidas, os profissionais de saúde podem fortalecer a proteção das informações sensíveis dos pacientes contra-ataques cibernéticos.

Outro ponto crucial é limitar o acesso às informações apenas para profissionais de saúde autorizados, de modo a atender as disposições dos arts. 46 e 50 da LGPD. Para tanto, é fundamental a implementação de sistemas de controle de acesso garante que somente pessoas autorizadas possam visualizar, modificar ou compartilhar as informações contidas nos prontuários médicos (Confederação Nacional de Saúde, 2021). Além disso, é importante armazenar as informações em sistemas seguros, protegidos por medidas de segurança física e lógica.

A capacitação e treinamento da equipe também desempenham um papel importante na proteção de dados dos pacientes. Realizar treinamentos periódicos sobre segurança da informação e políticas de privacidade ajuda a conscientizar os profissionais sobre as melhores práticas de proteção de dados. Todos os membros da equipe devem estar cientes de sua responsabilidade na proteção das informações dos pacientes e do impacto que violações de segurança podem ter na confiança e reputação da instituição (Alvarez, 2020).

Outra medida relevante é o gerenciamento de riscos, que envolve a realização de avaliações regulares para identificar possíveis vulnerabilidades nos sistemas e processos. Com essas informações em mãos, as instituições de saúde podem implementar medidas de mitigação para minimizar o risco de violações de dados. Mesmo com todas as medidas preventivas, é possível que ocorram vazamentos de dados em algum momento. Nesses casos, é fundamental

que os médicos ajam rapidamente e de forma adequada para minimizar os danos e cumprir suas obrigações legais e éticas.

Uma das primeiras ações é notificar as autoridades competentes, como a Agência Nacional de Proteção de Dados (ANPD), sobre o incidente de vazamento de dados. Essa notificação é obrigatória de acordo com as legislações de proteção de dados e permite que as autoridades competentes tomem as medidas apropriadas (Brasil, 2018).

Além disso, os pacientes afetados pelo vazamento de dados devem ser prontamente comunicados sobre o ocorrido. É essencial fornecer informações claras sobre quais dados foram afetados, o que está sendo feito para remediar a situação e quais medidas corretivas estão sendo implementadas para evitar futuros incidentes. Coletar evidências sobre o vazamento de dados é outra etapa importante. Registros de atividades, logs e outros documentos relevantes devem ser preservados para documentar a violação e auxiliar nas investigações. Informar as seguradoras sobre o incidente também é essencial. A seguradora pode fornecer suporte financeiro e assistência jurídica para lidar com as consequências do vazamento de dados e mitigar os danos financeiros.

Em resumo, a proteção de dados dos prontuários médicos requer uma abordagem abrangente que combina medidas técnicas, organizacionais e legais. A adoção de medidas de segurança cibernética, o controle de acesso às informações, o treinamento da equipe, o gerenciamento de riscos e a resposta adequada em caso de vazamentos são elementos-chave para garantir a privacidade e segurança das informações dos pacientes. Com um compromisso contínuo com a proteção de dados, os médicos podem cumprir suas obrigações éticas e legais, mantendo a confiança dos pacientes e contribuindo para a excelência no cuidado de saúde.

5. Considerações finais

A proteção dos dados de prontuários médicos é uma questão de extrema importância e complexidade, especialmente em um contexto de crescente digitalização da saúde e aumento das ameaças cibernéticas. Ao longo deste artigo, foram abordados os principais desafios enfrentados pelos profissionais de saúde na proteção desses dados sensíveis, bem como as soluções e abordagens necessárias para enfrentá-los de forma eficaz.

Ficou evidente que a sensibilidade dos dados contidos nos prontuários médicos exige a implementação de medidas de segurança cibernética robustas, como criptografia, firewalls e autenticação de dois fatores. Além disso, a limitação do acesso às informações apenas para

profissionais de saúde autorizados é essencial para garantir a confidencialidade dos registros médicos.

A conscientização e o treinamento da equipe foram destacados como elementos fundamentais para criar uma cultura de segurança da informação, onde todos os membros da equipe estejam cientes de suas responsabilidades na proteção dos dados dos pacientes.

A conformidade com as legislações de proteção de dados, como o RGPD da União Europeia e a LGPD do Brasil, foi apontada como uma obrigação legal que as instituições de saúde devem cumprir. A adoção de políticas, procedimentos e tecnologias em conformidade com essas leis é crucial para garantir o respeito aos princípios de privacidade e proteção de dados.

Em casos de vazamentos de dados, foi ressaltada a importância de agir rapidamente para minimizar os danos e cumprir as obrigações legais e éticas. Notificar as autoridades competentes e comunicar os pacientes afetados são medidas fundamentais para lidar com incidentes de segurança de forma responsável e transparente.

Por fim, conclui-se que a proteção de dados de prontuários médicos é um desafio contínuo que requer um esforço conjunto de profissionais de saúde, instituições médicas e autoridades reguladoras. A implementação de medidas técnicas, organizacionais e legais é fundamental para garantir a privacidade e segurança das informações sensíveis dos pacientes. Ao enfrentar esses desafios com diligência e responsabilidade, é possível estabelecer uma base sólida para a proteção dos dados de prontuários médicos, preservando a confiança dos pacientes, promovendo a excelência no cuidado de saúde e avançando de forma ética na pesquisa médica. A proteção dos dados de prontuários médicos não é apenas uma obrigação legal, mas também um compromisso ético e uma demonstração de respeito à privacidade e dignidade dos pacientes.

Referências bibliográficas

ALVAREZ, Giovana Ferreira de Sá. **LGPD para médicos, dentistas e profissionais da área da saúde**. Migalhas, 16 dez.2020. Disponível em: https://www.migalhas.com.br/depeso/337966/lgpd-para-medicos--dentistas-e-profissionaisda-area-da-saude. Acesso em: 14 jul. 2023.

BRASIL. **Guia de Boas Práticas** – Lei Geral de Proteção de Dados (LGPD). 2020 Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf >. Acesso em: 13 de jul. de 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais** (LGPD). 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html>. Acesso em 10 jul. 2023.

BBC. **Caso Klara Castanho:** o que pode acontecer com profissional de saúde que divulga dados sigilosos. BBC, 2022. Disponível em: <https://www.bbc.com/portuguese/brasil-61961007 >. Acesso em: 13 de jul. de 2023.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de Boas Práticas:** Proteção de Dados para Prestadores Privados em Saúde. 2021. Disponível em: < https://www.gov.br/ans/pt-br/arquivos/assuntos/noticias/boas-praticas-protecao-dados-prestadores-privados-cnsaude_21.pdf>. Acesso em 13 de jul. de 2023

CONSELHO FEDERAL DE ENFERMAGEM (COREN-Brasil). **Código de ética de enfermagem.** Resolução nº 311. Brasília, 2012. Disponível em: http://www.cofen.gov.br/wpcontent/uploads/2012/03/resolucao_311_anexo.pdf. Acesso em: 07 set. 2021.

CONSELHO FEDERAL DE MEDICINA (CFM-Brasil). **Resolução CFM nº 1.821/2007**. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Diário Oficial da União, Brasília, 23 nov. 2007, Seção I, p. 252. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 07 set. 2021.

CONSELHO FEDERAL DE MEDICINA (CFM-Brasil). **Resolução CFM nº 1.638/2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Diário Oficial da União, Brasília, 9 ago. 2002, Seção I, p.184-5. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 13 jul. 2023.

CONSELHO FEDERAL DE MEDICINA (CFM-Brasil). **Resolução CFM nº 1.638/2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Diário Oficial da União, Brasília, 9 ago. 2002, Seção I, p.184-5.

Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 07 set. 2021.

CONSELHO FEDERAL DE MEDICINA. **Código de ética médica:** resolução CFM nº 1.931, de 17 de setembro de 2009 (versão de bolso) / Conselho Federal de Medicina – Brasília: Conselho Federal de Medicina, 2010.

DEMO, Fabio; PRIESNITZ FILHO, Walter. Gestão de Privacidade no Armazenamento de Dados do Paciente em Registros Médico-Hospitalares Eletrònicos. In: Escola Regional de Redes de Computadores (ERRC), 17, 2019 **Anais**[...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. P.57-64. Doi: https://dpo.org/10.5753/errc.2019.9212. Acesso em: 30 out. 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 02, p. 91-108, 2011. Disponível em: <https://editora.unoesc.edu.br/index.php/espacojuridico/article/viewFile/1315/658> Acesso em: 12 jul. de 2023.

DUTRA, Quésia Falcão de. **O caso Klara Castanho e a LGPD**. Migalhas, 30 de junho de 2022. Disponível em: <https://www.migalhas.com.br/depeso/368891/o-caso-klara-castanho-e-a-lgpd>. Acesso em: 13 jul. de 2023.

LEME, Renata Salgado; BLANK, Marcelo. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Cadernos Ibero-Americanos de Direito Sanitário**, v.9, n.3, p.210-224, jul./set. 2020.

LÓSSIO, Claudio Joel Brito. As profissões da saúde e o tratamento dos dados pessoais: Boas práticas e a conformidade. **Revista Jurídica da Universidade do Sul de Santa Catarina**, v. 10, n. 21, p. 29-35, set. 2020. Disponível em: http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/view/9816. Acesso em: 20 jul. de 2023.

MOTTA, G. H. M. B. **Um Modelo de Autorização Contextual para o Controle de Acesso ao Prontuário Eletrônico do Paciente em Ambientes Abertos e Distribuídos**.05/02/2004. 213 f. Tese (Escola Politécnica). USP, 2003.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados pessoais (Lei 13.709/18). **Revista de Direito e Garantias Fundamentais**, Vitória, 2018.

PAULO, Matheus Adriano. **Análise comparativa da cooperação internacional, das sanções administrativas e do controle judicial na proteção de dados Na União Européia e no Brasil**. Dissertação (Mestrado em Ciência Jurídica) – Universidade do Vale do Itajaí, Itajaí, 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei nº 13.709/2018 LGPD. Saraiva Educação, 2018.

RAMOS, Edith Maria Barbosa; DELDUQUE, Maria Célia; ALVES, Sandra Mara Campos. Dados pessoais sensíveis e a pandemia de Coronavírus: divulgar para proteger? **Revista**

Eletrônica de Direito do Centro Universitário Newton Paiva. Belo Horizonte, n. 42, p. 240-257, set./dez. 2020. Disponível em: https://revistas.newtonpaiva.br/redcunp/wpcontent/uploads/2021/01/DIR42-15.pdf. Acesso em: 20 jul. 2023.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados** (RGPD). (2016). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em 10 de jul. 2023.

VALENTE, Jonas. **França aplica multa máxima ao Google por violação de legislação**. Agência Brasil, Brasília, 23 de janeiro de 2019. Disponível em: < https://agenciabrasil.ebc.com.br/internacional/noticia/2019-01/franca-aplica-multa-maxima-ao-google-por-violacao-de-legislacaoL>. Acesso em: 13 jul. 2023.