CI-IA
Centro de Inovação em Inteligência Artificial

Proteção de Dados em Pesquisa na Saúde

Gabriella da Silva Reis
Zilma Silveira Nogueira Reis

Realização CI-IA Centro de Inovação em Inteligência Artificial
Apoio UFMG Universidade Federal de Minas Gerais

Belo Horizonte, MG
2024

CENTRO DE INOVAÇÃO EM INTELIGÊNCIA ARTIFICIAL PARA A SAÚDE

CI-IA
Centro de Inovação em Inteligência Artificial

Proteção de Dados em Pesquisa na Saúde

Gabriella da Silva Reis
Zilma Silveira Nogueira Reis

Belo Horizonte, MG
2024

Autores
Gabriella da Silva Reis
Zilma Silveira Nogueira Reis

Equipe de Tecnologia da Informação, Ambiente Virtual de Aprendizagem (Moodle) e Site do Curso
Isaias José Ramos de Oliveira Joabe Dias Salgueiro

DOI:
https://doi.org/10.5281/zenodo.14677910

ISBN:
978-65-86593-46-4

Universidade Federal de Minas Gerais

Reitora
Sandra Regina Goulart Almeida
Vice-Reitor
Alessandro Fernandes Moreira

Centro de Inovação em Inteligência Artificial para a Saúde - CI-IA Saúde

Diretoria
Virgílio Augusto Fernandes Almeida
Wagner Meira Junior
Antônio Luiz Pinho Ribeiro
Coordenadora de educação e difusão do conhecimento
Zilma Silveira Nogueira Reis
Coordenador de transferência de tecnologia
Gilberto Medeiros Ribeiro

Gerência de projetos
Fabiana Costa Pereira Peixoto
Letícia Santos Neto

Site: https://ciia-saude.medicina.ufmg.br
Email: cursosciiasaude@medicina.ufmg.br

Dados Internacionais de Catalogação na Publicação
(CIP) (Câmara Brasileira do Livro, SP, Brasil)

Reis, Gabriella da Silva; Reis, Zilma Silveira Nogueira.
R375p Proteção de dados em pesquisa na saúde. / Gabriella da Silva Reis; Zilma Silveira Nogueira Reis. – 1ª edição – Belo Horizonte: Centro de Inovação em Inteligência Artificial para a Saúde da UFMG, 2024.
51p.: il.

Formato: PDF
Requisitos do Sistema: Adobe Digital Editions.
ISBN: 978-65-86593-46-4

1. Saúde Digital. 2. Proteção de Dados. 3. Inteligência Artificial. 4. Ética em Pesquisa. I. Título.

NLM: W 26.5

Bibliotecário responsável: Marina Nogueira Ferraz CRB-6/2194

Sobre os Direitos Autorais

Prefácio

A introdução da Saúde Digital trouxe a promessa de ampliar o acesso ao cuidado, qualificar a prestação de cuidados e a gestão dos serviços de saúde. Com isso, um grande volume de dados em formato digital vem sendo coletado, compartilhado e armazenado em sistemas eletrônicos. Se por um lado vislumbram-se o potencial da tecnologia digital para reduzir desperdícios, aprimorar a gestão da saúde da população e para dar suporte para um sistema de saúde mais resiliente e menos oneroso, são grandes os desafios éticos e legais no tratamento dos dados pessoais.

O eBook *Proteção de Dados em Pesquisa na Saúde* surge em um momento oportuno para promover, em todos os interessados no tema, as reflexões necessárias diante do desafio de conciliar os avanços tecnológicos com as normativas de privacidade. É com grande satisfação que o Centro de Inovação em Inteligência Artificial para Saúde apresenta esta obra, que acompanha o curso com o mesmo nome, oferecido pela sua Diretoria de Educação e Disseminação do Conhecimento. A autora reúne expertise acadêmica e aplicada, oferecendo uma perspectiva abrangente sobre como a proteção de dados influencia a pesquisa na saúde. Os capítulos estão estruturados de maneira a fornecer não apenas uma base teórica sobre as legislação vigente, mas também orientações práticas sobre como implementá-las nas práticas de pesquisa científica.

Alinhando-se às necessidades de pesquisadores, profissionais da saúde e gestores de dados, com a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, o conteúdo do eBook apresenta uma abordagem consciente e responsável sobre o tema, sendo de grande relevância para que todos os envolvidos em pesquisa e tratamento de dados de saúde estejam não apenas cientes das exigências legais, mas também capacitados para aplicá-las de forma eficiente e ética.

Profa Zilma Reis
Universidade Federal de Minas Gerais

Sumário

1. Introdução

Este eBook foi elaborado no contexto do curso de capacitação *"Proteção de Dados em Pesquisa na Saúde"*, ofertado pelo Centro de Inovação em Inteligência Artificial para Saúde. Seu objetivo é auxiliar pesquisadores, órgãos de pesquisas, empresas e profissionais da área da saúde a navegarem pelas complexidades da Proteção de Dados em Pesquisa no cenário contemporâneo.

O conteúdo oferece uma visão abrangente das normas e regulamentações que orientam o uso e o tratamento de dados sensíveis em pesquisas de saúde, destacando as melhores práticas para assegurar a confidencialidade e a integridade das informações.

Voltado a pesquisadores, profissionais de saúde e demais interessados na proteção de dados, este material busca oferecer uma abordagem prática e informativa sobre como lidar com os desafios de conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD).

O conteúdo foi estruturado em tópicos que abrangem o panorama legislativo e regulatório, a gestão de riscos relacionados à privacidade, a implementação de medidas de segurança e protocolos de pesquisa, na salvaguarda dos dados de saúde.

1.1 A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a legislação brasileira que regula o tratamento de dados pessoais em todo o território nacional. Seu principal objetivo é assegurar a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, garantindo que o uso de dados pessoais seja realizado de maneira ética, transparente e segura.[1]

Lei Geral de Proteção de Dados Pessoais (LGPD)

A LGPD se aplica a qualquer operação de tratamento de dados pessoais, desde a coleta até o descarte, abrangendo dados tanto no meio físico quanto digital, e impondo uma série de requisitos para a conformidade das organizações e indivíduos que realizam esse tratamento. No contexto das pesquisas em saúde, o tratamento de dados pessoais sensíveis, como informações sobre a saúde dos indivíduos, exige ainda mais cuidado, pois envolve dados de alto valor e relevância, tanto para o titular quanto para a sociedade em geral.

[1] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Embora a LGPD estabeleça regras rigorosas, sua intenção não é inviabilizar ou dificultar a pesquisa científica.[2] O legislador, ao elaborar a LGPD, teve o cuidado de equilibrar a proteção dos dados pessoais com a promoção do desenvolvimento científico e tecnológico. Isso está expresso já no artigo 2º da lei, que menciona como fundamentos a inovação e o desenvolvimento tecnológico. A proteção de dados, portanto, deve ser vista como um meio para fomentar a pesquisa ética e responsável, em vez de um obstáculo ao progresso científico.

É importante que os pesquisadores compreendam que o tratamento inadequado de dados pessoais pode gerar riscos não apenas ao titular dos dados, mas também à reputação das instituições e à confiança da sociedade no sistema de pesquisa. A adoção de boas práticas, em conformidade com a LGPD, representa um compromisso com a proteção dos direitos dos participantes da pesquisa e contribui para a criação de um ambiente de confiança e transparência.

Assim, o objetivo deste eBook é conscientizar os profissionais de saúde e pesquisadores sobre a importância de aplicar processos e rotinas adequadas para garantir a proteção dos dados utilizados em suas pesquisas.

Em suma, a LGPD não deve ser vista apenas como uma imposição legal, mas como uma ferramenta essencial para a construção de uma sociedade mais segura e ética no uso de dados, permitindo que a evolução científica e tecnológica continue de forma responsável e respeitosa aos direitos dos indivíduos.

1.2 Definição de Tratamento de Dados Pessoais

Na legislação brasileira, o tratamento de dados é definido[3] como qualquer operação realizada com dados pessoais. Isso inclui um vasto conjunto de atividades, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O conceito abrange todas as fases do ciclo de vida dos dados, desde a coleta até a eliminação, e implica que qualquer manipulação de dados de saúde dentro de uma pesquisa precisa ser conduzida em conformidade com as normas da LGPD.

---

[2] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética, 2024.

[3] LGPD, art. 5º X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

1.3 Conceito de Dado Pessoal Sensível de Saúde

O conceito de dado pessoal sensível, para fins do Programa SUS Digital, foi formalmente introduzido na legislação brasileira pela Portaria GM/MS Nº 3.232, de 1º de março de 2024.[4] Esta portaria, foi um marco para a transformação digital no Sistema Único de Saúde (SUS), ampliando o acesso da população a ações e serviços, com o objetivo de melhorar a integralidade e a resolutividade da atenção à saúde. A saúde digital, conforme abordada pela Portaria, adota uma abordagem multidisciplinar, integrando tecnologia, informação e saúde, com a incorporação de software, hardware e serviços como parte da transformação digital.

Portaria GM/MS Nº 3.232, de 1º de março de 2024

No artigo 4º, inciso II, da Portaria GM/MS Nº 3.232/2024, o conceito de “dado pessoal sensível de saúde” é definido como "dados relativos à saúde de um titular ou à atenção à saúde a ele prestada, que revelem informações sobre sua saúde física ou mental no presente, passado ou futuro." Essa definição reflete uma visão ampliada de saúde e proteção de dados, alinhando-se com o artigo 3º da Lei 8.080/1990 (Lei Orgânica da Saúde) e com o Regulamento da União Europeia 2016/679 (GDPR)[5].

Importante destacar que a LGPD não define diretamente o conceito de dado de saúde. Embora ela estabeleça no artigo 5º, inciso II, o que são dados sensíveis, englobando dados de saúde entre eles, a LGPD não traz uma definição detalhada de “dados de saúde.”

Por outro lado, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[6] oferece uma definição clara e abrangente. No Artigo 4(15) da GDPR, "dados de saúde" são definidos como: "Dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o estado de saúde dessa pessoa." Essa definição é ampla e foi elaborada para cobrir uma grande variedade de informações, não se limitando apenas a serviços médicos tradicionais. Ela abrange também informações sobre o bem-estar físico ou mental, doenças, deficiências, riscos de doença, histórico clínico, tratamentos ou procedimentos, ou qualquer outra informação que possa revelar o estado de saúde de um indivíduo.

---

[4] https://bvsms.saude.gov.br/bvs/saudelegis/gm/2024/prt3232_04_03_2024.html

[5] DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. Disponível online em: https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude#_ftn2. Acesso em: 30 jun. 2024.

[5] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Regulamento Geral de Proteção de Dados da União Europeia (GDPR)

O conceito de "dado pessoal sensível de saúde" adotado pelo Ministério da Saúde se alinha com o artigo 11, §1º da LGPD, ampliando as hipóteses de tratamento para dados pessoais cuja finalidade possa revelar, a depender das técnicas aplicadas, informações sensíveis que possam causar dano ao titular.

Essa definição também ressalta a importância de tratar dados sensíveis de forma responsável, especialmente em contextos onde as inferências baseadas em dados comuns, como geolocalização e perfil de consumo, podem revelar informações de saúde. Nesse sentido, algoritmos preditivos, diagnósticos genéticos e sistemas de IA aplicados à saúde devem seguir rigorosamente as previsões da LGPD e do GDPR, garantindo que os dados sejam tratados de forma ética e segura.

A adoção deste conceito pelo Ministério da Saúde, que abrange informações de saúde do passado, presente e futuro, é um avanço significativo para a proteção dos direitos de privacidade e liberdade dos indivíduos, especialmente em um contexto de transformação digital acelerada. Ele oferece um arcabouço mais robusto para a proteção de dados no setor de saúde, promovendo o uso ético e responsável dessas informações essenciais, ao mesmo tempo em que possibilita a evolução contínua das inovações tecnológicas na área da saúde.

1.4 Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade governamental responsável pela fiscalização da aplicação da LGPD no Brasil. Criada pela Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, a ANPD tem como missão garantir o cumprimento da LGPD por todas as entidades que realizam o tratamento de dados, sejam elas públicas ou privadas.

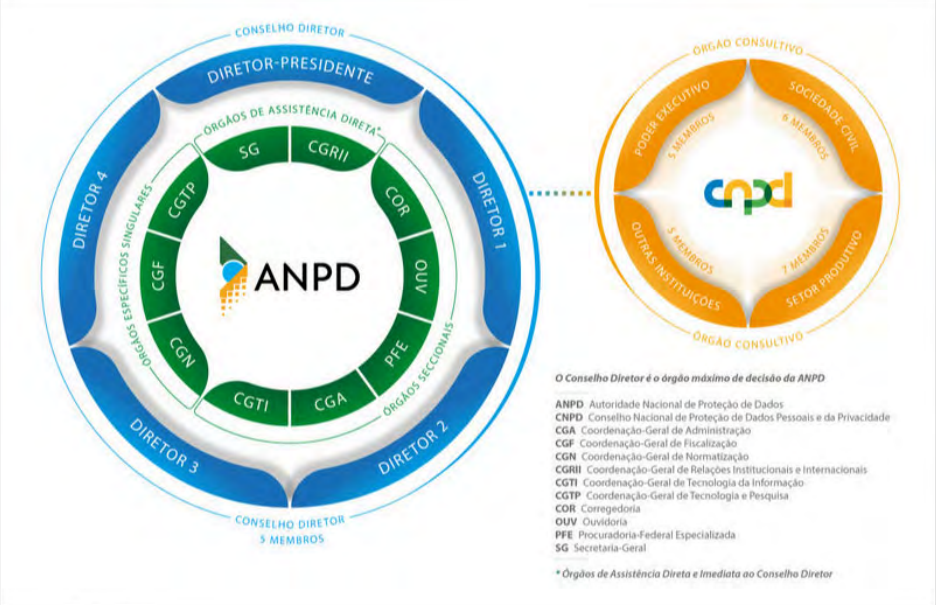
Entre as suas principais atribuições, destacam-se a formulação de diretrizes e regulamentações complementares à LGPD, a orientação das organizações e da sociedade quanto às boas práticas de proteção de dados e a fiscalização do cumprimento das normas estabelecidas.

---

[4] DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. Disponível online em: https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude#_ftn2. Acesso em: 30 jun. 2024.

Além disso, a ANPD tem o poder de editar normas técnicas e regulamentos que detalham e especificam as obrigações das empresas, organizações e órgãos públicos que tratam dados pessoais. Isso inclui, por exemplo, a regulamentação de procedimentos para a comunicação de incidentes de segurança envolvendo dados pessoais, a realização de auditorias e a definição de parâmetros para a aplicação de sanções administrativas.

Por fim, a ANPD é composta por um Conselho Diretor, que é responsável por sua administração e pelas decisões mais importantes relacionadas à regulação e fiscalização da LGPD, e por um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão consultivo que contribui para o aprimoramento das políticas públicas voltadas à proteção de dados. A criação e o fortalecimento da ANPD representam um marco na proteção da privacidade no Brasil, promovendo um ambiente de maior confiança e segurança no uso de dados pessoais, especialmente no setor da saúde, onde o tratamento de dados sensíveis exige rigor e responsabilidade.



Organograma Circular da ANPD

Fonte: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/estrutura-organizacional-1

2. Introdução à Proteção de Dados de Saúde

O conceito de dado pessoal sensível, para fins do Programa SUS Digital, foi formalmente introduzido na legislação brasileira pela Portaria GM/MS Nº 3.232, de 1º de março de 2024.[4] Esta portaria, foi um marco para a transformação digital no Sistema Único de Saúde (SUS), ampliando o acesso da população a ações e serviços, com o objetivo de melhorar a integralidade e a resolutividade da atenção à saúde. A saúde digital, conforme abordada pela Portaria, adota uma abordagem multidisciplinar, integrando tecnologia, informação e saúde, com a incorporação de software, hardware e serviços como parte da transformação digital.

2.1 Conceitos Importantes

Dados de saúde são considerados dados sensíveis de acordo com o art. 5º, II da LGPD, o que significa que eles requerem um nível mais elevado de proteção e cuidado durante o tratamento. A referida lei também estabelece diretrizes específicas para o tratamento desses dados sensíveis, exigindo medidas rigorosas de segurança e transparência. Para os pesquisadores que lidam com dados de saúde, é essencial compreender os princípios e exigências da LGPD, garantindo não apenas o cumprimento da legislação, mas também a proteção dos direitos dos titulares dos dados.

Ao longo deste capítulo, detalharemos os conceitos fundamentais da LGPD[8] que todo pesquisador deve conhecer, como o que caracteriza um dado pessoal e um dado sensível, o que define um banco de dados e quem são os agentes de tratamento responsáveis pelo manuseio dessas informações. Esses conceitos são essenciais para que os pesquisadores possam cumprir as exigências legais e proteger adequadamente os dados que tratam.

Imagem criado no Canva:
https://www.canva.com/design/DAGQ2_p1hlw/3l1FRW8-upVlD9PmvqSjAQ/edit

[8] Art. 5º LGPD - https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

• **Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável. Isso significa qualquer informação pela qual seja possível identificar uma pessoa ou que, usada em conjunto com outras informações, possa levar à sua identificação.

• **Dado sensível:** São dados pessoais que revelam origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

• **Dado anonimizado**: Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

• **Banco de dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

• **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

• **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

• **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Em outras palavras, é a entidade ou pessoa que efetivamente processa os dados pessoais sob as instruções do controlador.

• **Encarregado (DPO - Data Protection Officer):** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Para os pesquisadores que lidam com dados de saúde, em documentos de papel ou em meio digital, é essencial compreender que, na perspectiva de uma pessoa jurídica, a determinação do controlador ou do operador de dados pessoais deve ser feita com base no caráter institucional da organização, e não em suas pessoas físicas[9]. Ou seja, o agente de tratamento será sempre a organização responsável pelo tratamento de dados, mesmo que isso seja feito em nome de terceiros, e não os indivíduos subordinados a ela, como funcionários, colaboradores ou servidores públicos, dependendo da natureza da instituição.

Essa distinção foi amplamente abordada pela ANPD em seus estudos sobre a aplicação da

[9] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024.

legislação de proteção de dados no contexto de pesquisas acadêmicas[10]. A ANPD enfatiza que, em pesquisas científicas, o órgão de pesquisa deve ser identificado como o agente de tratamento responsável, seja ele controlador ou operador. De acordo com o artigo 5º da LGPD, os órgãos de pesquisa submetidos ao regime especial de tratamento de dados são, necessariamente, pessoas jurídicas, podendo ser de direito público ou privado, sem fins lucrativos. Para tanto, é exigido que a pesquisa básica ou aplicada, de caráter histórico, científico, tecnológico ou estatístico, esteja incluída em sua missão institucional ou objetivo social.

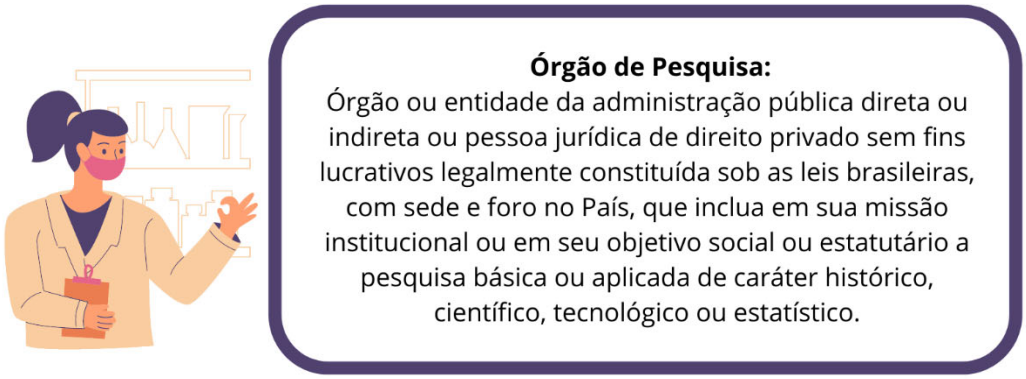


Imagem gerada via Canva:
https://www.canva.com/design/DAGQ2_p1hlw/3l1FRW8-upVID9PmvqSjAQ/edit

Ainda, a ANPD esclarece que as pessoas naturais que realizam o tratamento de dados pessoais subordinadas a uma organização, como funcionários ou colaboradores, não são consideradas agentes de tratamento[11]. Esse entendimento é particularmente relevante no caso de pesquisas científicas, onde membros da equipe de pesquisa atuam sob a responsabilidade do órgão de pesquisa, que é o controlador ou operador dos dados.

No âmbito das pesquisas acadêmicas, a ANPD destaca a importância de que os órgãos de pesquisa estabeleçam estratégias claras de prevenção e segurança para proteger os dados pessoais[12]. Essas estratégias devem ser adaptadas à especificidade de cada pesquisa, levando em consideração fatores como as exigências de segurança, a tecnologia disponível no momento e os esforços razoáveis para garantir a conformidade com a LGPD. Além disso, essas estratégias devem estar alinhadas com as disposições éticas específicas de cada pesquisa.

---

[10] Fonte: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf

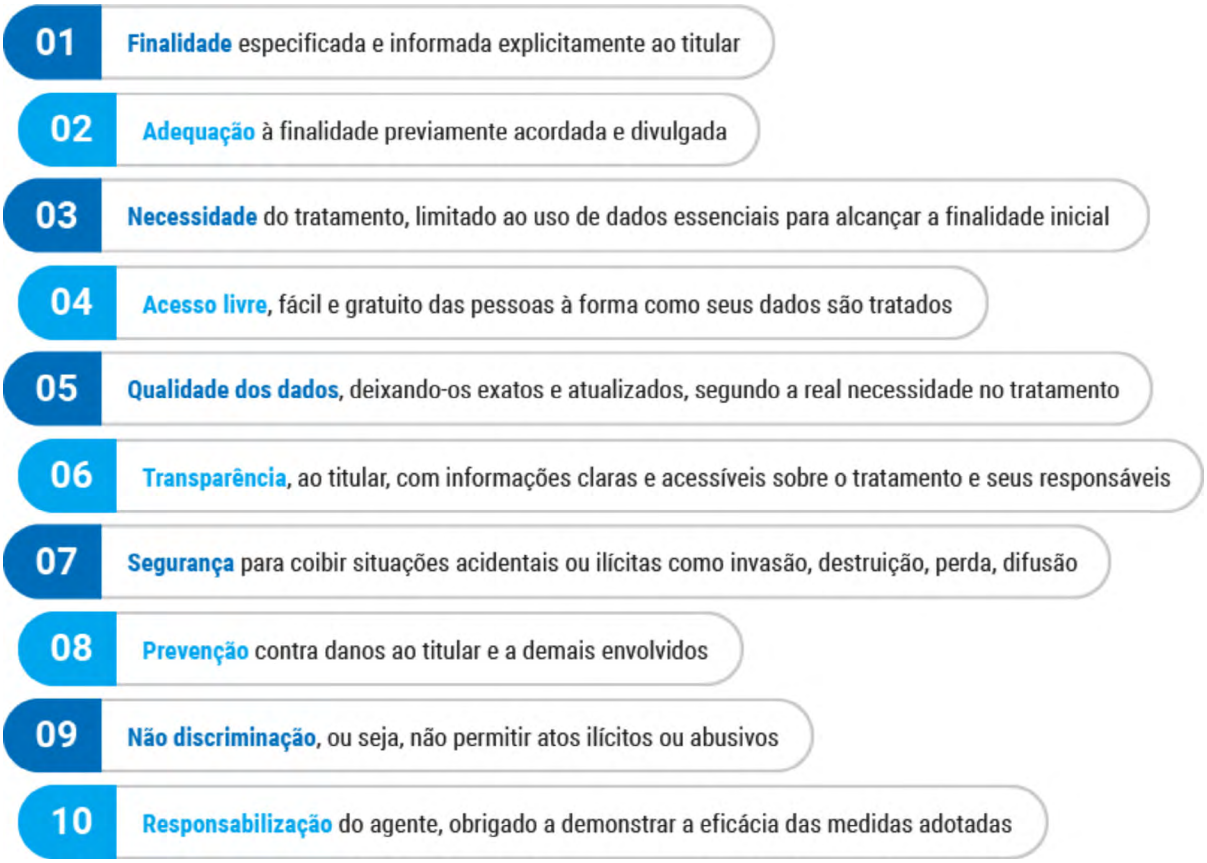
[11] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

[12] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdff

Por fim, a ANPD reforça a responsabilidade dos controladores de dados que pretendem compartilhar dados pessoais com órgãos de pesquisa para a realização de estudos acadêmicos. Antes de efetivar esse compartilhamento, é importante verificar se o órgão de pesquisa tenha adotado todas as medidas necessárias para proteger os dados pessoais envolvidos. Dessa forma, a proteção dos dados pessoais deve ser assegurada em todas as etapas do processo de pesquisa, desde a coleta de informações até a eliminação ou arquivamento dos dados.

2.2 Princípios da LGPD

A LGPD, em seu artigo 6º, estabelece uma série de princípios que orientam o tratamento de dados pessoais em qualquer contexto, inclusive na pesquisa em saúde. Tratamento de dados é qualquer operação realizada com dados pessoais. Isso inclui um vasto conjunto de atividades, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Esses princípios são fundamentais para assegurar que os dados sejam tratados de maneira ética, transparente e segura, protegendo os direitos dos titulares e garantindo que as finalidades da pesquisa sejam alcançadas de forma responsável. Para os pesquisadores que lidam com dados de saúde, a aplicação desses princípios é essencial, dada a natureza sensível dessas informações.



Fonte: Brasil, Ministério da Fazenda, Serpro (acesso em 16 set. 2024) . Os 10 princípios para um efetivo tratamento de dados, segundo a Lei Geral de Proteção de Dados Pessoais https://www.serpro.gov.br/lgpd/menu/arquivos/os-10-principios-para-um-efetivo-tratamento-de-dados/view

• **Finalidade**

O princípio da finalidade estabelece que os dados devem ser coletados e tratados para propósitos específicos, legítimos e claramente definidos, os quais devem ser comunicados aos participantes de forma transparente.

• **Adequação**

Já o princípio da adequação implica que o tratamento dos dados deve ser compatível com os objetivos da pesquisa e as expectativas dos titulares, ou seja, os dados coletados devem ser pertinentes e apropriados ao estudo em questão.

• **Necessidade**

Este princípio determina que a coleta e o tratamento dos dados sejam limitados ao estritamente necessário para atingir os objetivos da pesquisa. Isso significa que apenas os dados essenciais devem ser coletados, evitando o acúmulo de informações irrelevantes ou excessivas. Para os pesquisadores, é recomendado realizar uma avaliação criteriosa dos dados que serão utilizados, sempre ponderando a relação entre a quantidade de dados coletados e a finalidade do estudo, evitando riscos desnecessários à privacidade dos participantes.

• **Livre Acesso**

Os titulares dos dados têm o direito de acessar as informações que forneceram, entendendo como estão sendo tratadas, por quanto tempo serão mantidas e em quais contextos podem ser compartilhadas.

• **Qualidade dos Dados**

Os dados coletados devem ser exatos, completos e atualizados, conforme necessário. A qualidade dos dados é imprescindível em pesquisas na área da saúde, pois informações imprecisas podem comprometer os resultados e a validade da pesquisa.

• **Transparência**

O princípio da transparência exige que os participantes sejam informados de forma clara e acessível sobre como seus dados serão tratados. Isso inclui explicações detalhadas sobre as finalidades da pesquisa, os métodos de coleta, as medidas de segurança implementadas e a possibilidade de compartilhamento dos dados com terceiros. Para cumprir esse princípio, os pesquisadores devem elaborar termos de consentimento que expliquem, de forma simples e direta, todos os aspectos relacionados ao tratamento de dados.

- **Segurança**

O princípio da segurança requer a adoção de medidas técnicas e organizacionais robustas para proteger os dados contra acessos não autorizados, perda, vazamento ou qualquer forma de tratamento inadequado. Isso inclui a implementação de criptografia, controles de acesso, sistemas de monitoramento e treinamento de toda a equipe envolvida na pesquisa. Essas práticas garantem a integridade, a confidencialidade e a segurança dos dados coletados, reduzindo o risco de incidentes de segurança.

- **Prevenção**

O princípio da prevenção estabelece que os agentes de tratamento de dados devem adotar medidas proativas para evitar a ocorrência de danos aos titulares dos dados durante o tratamento. Isso significa que, os responsáveis devem implementar políticas, práticas e mecanismos destinados a prevenir problemas que possam afetar a privacidade, a segurança ou a integridade dos dados pessoais.

- **Não Discriminação**

A LGPD proíbe o uso de dados para fins discriminatórios ou abusivos. Na pesquisa em saúde, isso significa que os dados não podem ser utilizados de maneira a prejudicar ou discriminar os participantes com base em características pessoais, como etnia, orientação sexual ou condições de saúde. A análise e o tratamento dos dados devem ser realizados com o máximo respeito à dignidade dos indivíduos.

- **Responsabilização e Prestação de Contas**

Por fim, o princípio da responsabilização exige que os pesquisadores demonstrem a conformidade com a LGPD, adotando e documentando medidas adequadas para garantir a proteção dos dados. Os pesquisadores devem ser capazes de prestar contas às autoridades competentes e aos participantes sobre como os dados estão sendo tratados, assegurando que as práticas adotadas estão de acordo com a legislação e com as normas éticas da pesquisa científica.

Esses princípios formam a base para o tratamento de dados em qualquer contexto, inclusive na pesquisa envolvendo dados de saúde e são fundamentais para proteger a privacidade dos titulares e e garantir a conformidade da pesquisa com as regras de utilização de dados sensíveis.

> **Exemplo:** Um grupo de pesquisadores da Universidade Federal de Minas Gerais está conduzindo um projeto de pesquisa sobre a eficácia de um novo medicamento para o tratamento da hipertensão. Para realizar a pesquisa, os pesquisadores planejam coletar dados de saúde de 500 pacientes que estão em tratamento em clínicas parceiras.

```
Finalidade: Coletam apenas dados necessários para o estudo.

Adequação: Limitam-se a informações relacionadas à hipertensão.

Necessidade: Evitam dados excessivos, mantendo o foco no
essencial.

Livre Acesso: Pacientes podem acessar seus dados pessoais.

Transparência: Informam os participantes por meio de um
Termo de Consentimento Livre e Esclarecido (TCLE).

Segurança: Usam criptografia e servidores seguros.

Prevenção: Implementam medidas para evitar incidentes de
segurança.

Não Discriminação: Garantem que os dados não sejam usados de
forma discriminatória.

Responsabilização: Documentam todo o processo.
```

3. Utilização de Dados de Saúde

3.1 Base Legal para Utilização de Dados de Saúde em Pesquisa

A LGPD estabelece que o tratamento de dados pessoais, especialmente os dados sensíveis, como os de saúde, só pode ser realizado se atender à uma das das bases legais previstas na legislação. No contexto da pesquisa científica, a utilização desses dados pode ocorrer com ou sem o consentimento dos titulares, dependendo de quem realizada a pesquisa e da finalidade do tratamento de dados.

Entre as principais hipóteses para o tratamento de dados sensíveis, destaca-se o consentimento informado, que permite ao titular exercer sua autodeterminação informacional. O consentimento informado, como apontado por Bioni e Luciano[13], tem suas origens na área da saúde, onde foi introduzido para garantir que os pacientes tivessem plena compreensão dos riscos, benefícios e implicações de procedimentos médicos. Na LGPD, o consentimento do titular é visto como um reflexo dos direitos de personalidade, consolidando a capacidade do indivíduo de controlar o uso de seus dados pessoais.

[13] BIONE, Bruno Ricardo. LUCIANO, Maria. O Consentimento Como Processo: Em Busca do Consentimento Válido. In: MENDES, Laura et al. (Org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.p. 243-258.

No entanto, o consentimento não é a única base legal aplicável. A LGPD também permite o tratamento de dados de saúde sem consentimento quando ele é indispensável para a tutela da saúde, a realização de pesquisas científicas por órgãos de pesquisa ou para a execução de políticas públicas pela administração pública. Nesses casos, o legislador reconhece que o interesse público e o avanço científico justificam a flexibilização da exigência do consentimento, desde que sejam adotadas medidas adequadas de segurança e anonimização sempre que possível.

3.3.1 Consentimento Informado

O consentimento informado é essencial para assegurar que o titular dos dados tenha plena compreensão de como seus dados serão tratados. Teffé e Viola[15] observam que o consentimento é uma manifestação direta dos direitos de personalidade, permitindo que o titular controle sua esfera privada e decida o uso que terceiros farão de suas informações.

A LGPD reforça que o consentimento só será válido se for informado, livre, específico e inequívoco, o que significa que o titular deve receber informações claras e compreensíveis sobre o tratamento de seus dados. O consentimento será considerado nulo[16] se houver comprovação de que as informações fornecidas foram enganosas ou abusivas, ou se não forem suficientemente claras.

Além disso, a LGPD exige que os agentes de tratamento informem o titular de forma destacada sobre os direitos previstos no artigo 18, que incluem o direito de acesso, correção, exclusão, e informações sobre a possibilidade de revogação do consentimento. Isso é fundamental, especialmente no caso de pesquisas científicas, onde o uso de dados sensíveis pode ter um impacto direto na privacidade e nos direitos dos participantes.

---

[14] Art. 11 LGPD - Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
(...)
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
(...)
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

[15] DE TEFFE, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica. com, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510

[16] LGPD, Art. 9º, § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

3.1.2 Exceções ao Consentimento na Pesquisa Científica

No âmbito das pesquisas científicas, a LGPD prevê situações nas quais o consentimento do titular pode ser dispensado. A LGPD dispensa a necessidade de consentimento para tratamentos de dados realizados pela administração pública, para a proteção da vida e tutela da saúde, assim como para a realização de pesquisas científicas por órgãos de pesquisa, desde que sejam garantidas medidas de segurança adequadas, como a anonimização dos dados sempre que possível.

Essa flexibilidade visa facilitar o desenvolvimento de estudos que promovam o avanço da ciência e a melhoria dos serviços de saúde, direito garantido pela Constituição Brasileira. No entanto, mesmo quando o consentimento não é exigido, os agentes de tratamento devem seguir as normas de segurança e responsabilidade previstas na LGPD.

3.3 Utilização de Dados de Saúde por Órgãos de Pesquisa

A LGPD estabelece um regime jurídico diferenciado para o uso de dados pessoais sensíveis em estudos científicos conduzidos por órgãos de pesquisa[17]. Esses órgãos incluem instituições de ensino superior públicas e privadas sem fins lucrativos, centros de pesquisa nacionais e entidades públicas, como o Instituto Brasileiro de Geografia e Estatística (IBGE) e o Instituto de Pesquisa Econômica Aplicada (IPEA). O objetivo desse regime especial é permitir que as pesquisas de interesse público possam avançar sem comprometer a proteção dos dados pessoais.

Uma das flexibilidades oferecidas pela LGPD aos órgãos de pesquisa é a possibilidade de tratar dados pessoais sensíveis sem o consentimento dos titulares, desde que isso seja necessário para a realização do estudo e que os dados sejam anonimizados sempre que possível. Essa medida visa facilitar o progresso científico, ao mesmo tempo em que protege a privacidade dos participantes por meio de técnicas que dificultem sua identificação.

Para se beneficiar das flexibilidades previstas na LGPD, os órgãos de pesquisa devem se enquadrar como entidades públicas ou privadas sem fins lucrativos, com foco em pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Essas instituições devem garantir que suas práticas de tratamento de dados estejam em conformidade com os princípios da LGPD.

Os dados pessoais acessados para estudos em saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e para as finalidades específicas de estudos e pesquisas. Os dados devem ser armazenados em ambientes controlados e seguros, com a aplicação

[17] Fonte: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf

de medidas como a anonimização ou pseudonimização sempre que possível. Além disso, a LGPD reforça a necessidade de seguir os padrões éticos relacionados à pesquisa, garantindo a proteção dos dados dos titulares.

A flexibilização das normas de tratamento de dados para fins acadêmicos e de pesquisa, como previsto nos artigos 7º e 11 da LGPD, aplica-se a contextos acadêmicos, respeitando as liberdades de expressão e inovação. No entanto, mesmo nesse cenário, a ANPD recomenda que as exceções sejam aplicadas com cautela, aconselhando que as entidades privadas obtenham o consentimento dos titulares dos dados e adotem medidas de segurança robustas.

> **Exemplo:** Num cenário hipotético, a Secretaria de Saúde de Belo Horizonte colabora com o Centro de Inovação para Inteligência Artificial para a Saúde (CI-IA Saúde), compartilhando dados de saúde pública anonimizados para desenvolver desenvolvimento de algoritmos de inteligência artificial que possam prever surtos de doenças infecciosas na região. Esses modelos são destinados a identificar padrões que prevejam surtos de doenças. A colaboração inclui acordos estritos de uso de dados e segurança, supervisionados por um comitê de ética, garantindo conformidade com a LGPD e proteção dos direitos individuais.

3.3 Utilização de Dados de Saúde por Empresas Privadas

A LGPD oferece uma estrutura jurídica principiológica para o tratamento de dados pessoais sensíveis. No entanto, o tratamento de dados de saúde por empresas privadas com fins lucrativos possui restrições, especialmente em comparação com os órgãos de pesquisa, que gozam de maior flexibilidade para o uso desses dados.

As bases jurídicas mais relevantes para o tratamento de dados de saúde estão nas alíneas "c" e "f" do inciso II do artigo 11 da LGPD. Essas bases permitem o processamento de dados de saúde para:

- O desenvolvimento de pesquisas por órgãos de pesquisa;
- A tutela da saúde, exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

Quando se trata de empresas privadas, essas organizações não podem se beneficiar das flexibilidades legais previstas para os órgãos de pesquisa, no entanto, podem conduzir pesquisas desde que baseiem o tratamento de dados em outras justificativas legais, como o consentimento explícito dos titulares, ou em outras bases que sejam aplicáveis.

3.3.1 Compartilhamento de Dados entre Entidades Privadas

A LGPD permite o compartilhamento de dados de saúde entre entidades privadas para fins como a prestação de serviços de saúde, assistência farmacêutica e diagnósticos. Contudo, o uso desses dados por operadoras de planos de saúde está estritamente proibido para a seleção de riscos na contratação ou para a exclusão de beneficiários, assegurando que os dados de saúde não sejam utilizados de maneira discriminatória ou abusiva.

Essa regulamentação é prevista nos §§ 4º e 5º do artigo 11 da LGPD, estabelecendo limites para a comunicação e o uso compartilhado de dados sensíveis no setor privado, especialmente em contextos comerciais.

3.3.2 Diferença entre Pesquisa com Dados de Saúde Financiadas por Empresas Privadas e Órgãos de Pesquisa

Uma diferença fundamental entre pesquisas realizadas por empresas privadas e órgãos de pesquisa é que as empresas privadas não podem se beneficiar das flexibilidades legais reservadas exclusivamente aos órgãos de pesquisa sem fins lucrativos. Isso significa que, embora empresas privadas possam realizar pesquisas científicas utilizando dados de saúde, elas devem basear esse tratamento em fundamentos legais distintos, como o consentimento dos titulares.

Essa questão torna-se ainda mais relevante em parcerias entre universidades, órgãos de pesquisa e entidades privadas, nos quais o tratamento de dados pessoais pode ser realizado para atividades comerciais corporativas. Para garantir a conformidade com a LGPD, é essencial que o regime jurídico seja claramente definido, incluindo:

- A identificação das naturezas, funções e responsabilidades de cada agente envolvido no tratamento de dados;
- A determinação da base legal apropriada para o tratamento de dados, seja o consentimento ou outra hipótese legal aplicável;
- A especificação das categorias de dados tratados e suas finalidades.
- Prudência na aplicação das exceções para pesquisa

Em caso de dúvida sobre se o tratamento de dados pessoais se enquadra nas exceções para atividades acadêmicas ou se requer outras bases legais, é recomendável buscar orientação especializada para evitar o descumprimento das normas de proteção de dados.

> **Exemplo:** Vamos considerar uma empresa privada com fins lucrativos focada no desenvolvimento de tecnologias, incluindo inteligência artificial aplicada à saúde. Segundo a LGPD, para ser considerada um órgão de pesquisa, uma instituição não deve ter fins lucrativos e deve realizar pesquisa básica ou aplicada.

4. Legislação e Ética na Pesquisa com Dados de Saúde

O tratamento de dados de saúde, devido à sua proteção especial como dado sensível, exige não apenas a conformidade com a base legal estabelecida pela LGPD, mas também a observância de ações éticas durante a pesquisa. Abaixo estão as principais considerações éticas e de segurança que os pesquisadores devem observar:

• **Natureza dos Dados Sensíveis:** Dados de saúde são considerados sensíveis, pois podem revelar informações sobre a condição física ou mental de uma pessoa. Essa natureza exige um cuidado redobrado no tratamento, e os pesquisadores devem estar cientes dos riscos potenciais que o uso desses dados pode representar para os participantes, como discriminação ou violação de privacidade.

• **Anonimização e Pseudoanonimização:** Para proteger os dados de saúde, a anonimização é uma técnica fundamental. Ela consiste em remover qualquer informação que possa identificar o titular, tornando os dados anônimos e impossibilitando a associação direta com a pessoa. Quando a anonimização completa não é viável, a pseudoanonimização pode ser aplicada. Nesse processo, os dados ainda podem ser relacionados a um indivíduo, mas essa associação é possível apenas com o uso de informações adicionais mantidas em ambiente separado e seguro.[18]

• **Medidas de Segurança:** A LGPD impõe a implementação de medidas técnicas e administrativas adequadas para garantir a segurança dos dados de saúde. Isso inclui o uso de sistemas de criptografia, controles de acesso, auditorias de segurança e a segregação de dados sensíveis em ambientes protegidos. Essas práticas são essenciais para evitar acessos não autorizados, vazamento ou manipulação inadequada dos dados de saúde. Além disso, é importante que os dados sejam armazenados em infraestruturas seguras, com backups regulares e monitoramento contínuo.

---

[18] Uma lista de elementos que identifiquem um paciente, parentes, profissionais de saúde e entidades devem ser eliminados de forma que seja impossível a identificação de um indivíduo. 1. Nomes e sobrenomes; 2. Todas as subdivisões geográficas menores que estado, incluindo endereço, cidade, distrito, vila, código de endereçamento postal e seus códigos geográficos equivalentes; 3. Todos os elementos de datas diretamente relacionados ao indivíduo como nascimento, admissão, alta e óbito; 4. Todas as idades acima de 89, bem como elemento de dados indicativos de tal idade; 5. Números de telefone; 6. Números de fax; 7. Endereços de e-mail; 8. Números ou códigos de previdência social; 9. Números ou códigos de registros e prontuários de pacientes; 10. Números ou códigos de beneficiários de planos de saúde; 11. Números ou códigos de contas-correntes; 12. Números ou códigos de certificados ou licenças; 13. Números ou códigos seriais ou de identificação de veículos, incluindo placas e licenças para dirigir; 14. Números ou códigos seriais ou de identificação de dispositivos, incluindo patrimônio, IMEI e licenças; 15. Endereços da web de qualquer tipo, sejam URLs, URIs, IPs ou similares; 16. Identificadores biométricos, incluindo impressões digitas, voz e íris; 17. Fotografias da face e imagens parciais, mas comparáveis; 18. Qualquer outro código único de identificação, caracterização ou codificação. NORONHA, Guilherme Francis de. Tratamento da informação de saúde para atendimento à necessidade de privacidade: desidentificação textual de documentos clínicos na língua portuguesa do Brasil. 2022. Tese (Doutorado em Gestão e Organização do Conhecimento) - Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2022.

• **Prevenção e Mitigação de Riscos:** Os pesquisadores devem adotar uma postura proativa na prevenção de incidentes relacionados ao tratamento de dados pessoais, implementando práticas preventivas para mitigar riscos à privacidade dos participantes. Isso pode incluir a realização de avaliações de impacto à proteção de dados, que ajudam a identificar possíveis vulnerabilidades e permitem a adoção de medidas corretivas antes que ocorra qualquer problema.

• **Expectativas Legítimas dos Titulares:** A pesquisa deve sempre considerar as expectativas legítimas dos titulares dos dados, especialmente no que diz respeito à forma como as informações serão utilizadas e armazenadas. Os titulares devem ser informados de maneira clara e acessível sobre os riscos envolvidos no tratamento dos dados, e suas escolhas e consentimento devem ser respeitados em todo o processo de pesquisa.

4.1 Legislação e Regulamentação Aplicáveis à Pesquisa com Dados de Saúde

Diversas leis e regulamentos formam a base legal e ética para o tratamento de dados de saúde no Brasil. Entre os principais estão:

• **Constituição Federal (CF):** Estabelece o direito à privacidade e à proteção da intimidade, servindo como base para a proteção de dados pessoais no Brasil.

• **Agência Nacional de Proteção de Dados (ANPD):** Responsável por regulamentar, implementar e fiscalizar a aplicação da LGPD, assegurando que as entidades que tratam dados pessoais cumpram a legislação.

• **Lei Geral de Proteção de Dados (LGPD):** Principal norma brasileira de proteção de dados pessoais, que regula o tratamento de dados em todo o território nacional e estabelece diretrizes específicas para dados sensíveis, como os de saúde.

• **Marco Civil da Internet:** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

• **Decreto 8.777/16:** Institui a Política de Dados Abertos do Poder Executivo federal.

• **Estratégia da Saúde Digital:** Iniciativa que visa modernizar os serviços de saúde por meio de soluções tecnológicas, integrando o uso de dados de saúde para políticas públicas e assistência.

• **Lei 8.080/90:** Lei Orgânica da Saúde, que regulamenta o Sistema Único de Saúde (SUS) e

estabelece diretrizes para a proteção e promoção da saúde pública no Brasil.

• **Resolução CFM 2.314/22:** Estabelece normas sobre o uso de tecnologias da informação e comunicação no âmbito da medicina, particularmente no que tange ao uso de telemedicina e tratamento de dados médicos.

4.2 Conselho Nacional de Saúde e a Nova Lei 14.874/2024

Antes da LGPD, a Resolução 466/2012 do Conselho Nacional de Saúde (CNS) já tratava da confidencialidade e privacidade dos dados dos participantes de pesquisa, estabelecendo padrões éticos para o tratamento de dados de saúde em pesquisas científicas.

Resolução 466/2012 do Conselho Nacional de Saúde (CNS)

A Resolução CNS nº 466/2012 reforça a responsabilidade dos pesquisadores pela segurança e pelo bem-estar dos participantes de pesquisas que envolvem seres humanos. Essa resolução estabelece que o uso de qualquer material ou dado coletado deve ser restrito aos objetivos especificados no protocolo de pesquisa ou conforme o consentimento obtido do participante.

Pesquisas que envolvem seres humanos, além de dados de saúde, exigem aprovação por Comitês de Ética em Pesquisa (CEP) ou pela Comissão Nacional de Ética em Pesquisa (CONEP). O sistema CEP/CONEP foi criado para garantir a proteção dos direitos e da dignidade dos participantes das pesquisas, promovendo ao mesmo tempo o avanço científico de maneira ética. É fundamental que qualquer pesquisa envolvendo seres humanos siga padrões éticos rígidos estabelecidos pelo Conselho Nacional de Saúde e cumpra os requisitos da LGPD.

A combinação das diretrizes da LGPD e dos padrões éticos visa assegurar que os indivíduos cujos dados são utilizados em pesquisas tenham seus direitos protegidos, com ênfase no tratamento seguro e controlado dos dados pessoais. O artigo 13 da LGPD reforça essa necessidade ao prever que os padrões éticos devem ser sempre considerados em estudos de saúde pública.

Um ponto importante a ser destacado é que a dispensa de consentimento prevista na LGPD, em razão da presença de outra base legal, não elimina a necessidade de obter o consentimento dos participantes de pesquisa sob a ótica ética. Ou seja, pode haver situações em que o consentimento não seja obrigatório pela LGPD, mas continua sendo exigido do ponto de vista ético, de acordo com as normas e regulamentos de pesquisa.

Com a Lei 14.874/2024, um novo marco legal foi instituído no Brasil, regulamentando a pesquisa com seres humanos e criando o Sistema Nacional de Ética em Pesquisa com Seres Humanos. Essa lei reforça a necessidade de os patrocinadores de pesquisas adotarem mecanismos rigorosos para proteger a confidencialidade das informações, compartilhando apenas dados anonimizados ou codificados. A chave para a codificação deve ser mantida separada pelo gestor de dados, garantindo que os dados pessoais dos participantes permaneçam protegidos.

4.3 Autoridades Envolvidas na Regulação de Pesquisa com Dados de Saúde

As autoridades que desempenham um papel central na regulação e fiscalização de pesquisas envolvendo dados de saúde no Brasil incluem:

• **Agência Nacional de Vigilância Sanitária (ANVISA):** Responsável pela regulamentação de produtos e serviços relacionados à saúde, incluindo medicamentos e dispositivos médicos.

• **Comissão Nacional de Ética em Pesquisa (CONEP):** Órgão vinculado ao Conselho Nacional de Saúde, com a função de avaliar e acompanhar os aspectos éticos das pesquisas que envolvem seres humanos, garantindo que os estudos sejam conduzidos de maneira ética e segura.

• **Comitê de Ética em Pesquisa (CEP):** Instituído em instituições de pesquisa, o CEP tem a responsabilidade de avaliar e aprovar projetos de pesquisa, assegurando que os direitos dos participantes sejam respeitados e que os estudos sigam padrões éticos rigorosos.

Cada uma dessas autoridades tem atribuições específicas para garantir que as pesquisas em saúde, especialmente aquelas que envolvem dados pessoais, sejam conduzidas de acordo com as normas éticas e regulatórias vigentes, protegendo tanto os direitos dos participantes quanto a integridade científica das pesquisas.

A pesquisa científica que envolve dados de saúde no Brasil está sujeita a uma série de normas éticas e legais que visam proteger os direitos dos titulares dos dados e garantir a segurança e integridade das informações tratadas. A conformidade com essas regras não apenas assegura a legalidade do tratamento de dados, mas também promove a confiança entre os participantes e a comunidade científica, permitindo que as pesquisas avancem de forma ética e responsável.

4.4 Ética na Coleta e Uso de Dados em Saúde

A ética no tratamento de dados em saúde é um dos pilares fundamentais para garantir que a privacidade e os direitos dos indivíduos sejam protegidos. A coleta, uso e compartilhamento de dados de saúde devem sempre estar em conformidade com as normas legais e os padrões éticos estabelecidos. A LGPD, juntamente com outras regulamentações, estabelece um conjunto robusto de diretrizes que visam garantir que esses dados sejam tratados com o devido respeito à confidencialidade e ao bem-estar dos titulares.

4.4.1 Base de Dados de Saúde

O artigo 13 da LGPD estabelece que o tratamento de dados pessoais para fins de pesquisa deve ser realizado exclusivamente para os objetivos declarados, vedando a transferência desses dados a terceiros. O parágrafo 2º desse artigo destaca que o órgão de pesquisa é responsável pela segurança da informação e que, em nenhuma circunstância, os dados podem ser compartilhados com terceiros sem a devida proteção.

Isso significa que o acesso a bases de dados de saúde por pesquisadores e instituições de ensino é permitido apenas para finalidades específicas de estudos e pesquisas, e os dados não podem ser repassados ou utilizados para outras finalidades sem o devido alinhamento com os objetivos originais estabelecidos no momento em que o acesso foi concedido. O descumprimento dessas regras pode gerar responsabilidades legais, reforçando a necessidade de rigor na proteção da confidencialidade.

Além disso, qualquer pessoa que tenha acesso a esses dados deve assinar um Termo de Responsabilidade, comprometendo-se a garantir que os dados pessoais sejam utilizados de acordo com os objetivos definidos e tratados com o mesmo nível de confidencialidade aplicado por profissionais como médicos e advogados em relação às informações de seus clientes. Portanto, é essencial que os dados pessoais sejam tratados de forma ética e segura, limitando seu uso aos fins de pesquisa declarados e respeitando os direitos de privacidade dos titulares.

4.5 Uso e Compartilhamento de Dados de Saúde

A LGPD estabelece regras sobre o uso e o compartilhamento de dados, especialmente aqueles de natureza pública. No artigo 7º, há diversas disposições sobre o tratamento e o compartilhamento de dados pessoais.

Tratamento de Dados Públicos (Art. 7º, § 3º): Quando os dados pessoais que são de acesso público forem utilizados, é necessário que o uso respeite a finalidade original para a qual os

dados foram disponibilizados, e o tratamento deve ser conduzido com boa-fé e de acordo com o interesse público. Em termos práticos, isso significa que o uso de dados públicos deve estar alinhado com o objetivo que justificou sua publicação inicial e deve ser feito de forma honesta e transparente.

Dispensa de Consentimento para Dados Públicos (Art. 7º, § 4º): O consentimento do titular não é necessário para o uso de dados que foram disponibilizados publicamente pelo próprio titular. No entanto, é necessário observar que os direitos do titular e os princípios da LGPD ainda devem ser respeitados, mesmo que o consentimento não seja necessário. Isso garante que o uso desses dados públicos seja feito de maneira justa e responsável.

Consentimento para Compartilhamento de Dados (Art. 7º, § 5º): Caso um controlador já tenha obtido o consentimento do titular para o uso de seus dados e deseje compartilhá-los com outros controladores, um novo consentimento específico deve ser obtido para esse compartilhamento, a menos que a legislação permita que essa nova autorização seja dispensada. Isso reforça a necessidade de que os dados só sejam compartilhados com a devida autorização do titular, garantindo sua proteção.

Obrigações Adicionais Mesmo com Dispensa de Consentimento (Art. 7º, § 6º): Mesmo quando o consentimento não é exigido para o tratamento de dados, as demais obrigações da LGPD permanecem válidas. Isso inclui o cumprimento dos princípios gerais da lei e a garantia dos direitos do titular, como transparência e acesso às informações. Em outras palavras, o fato de o consentimento ser dispensado não exime o controlador de cumprir com as demais disposições da LGPD.

Novas Finalidades para Dados Públicos (Art. 7º, § 7º): Dados pessoais públicos ou tornados públicos podem ser utilizados para novas finalidades, desde que esses novos fins sejam legítimos, específicos e estejam de acordo com os princípios da LGPD. Isso significa que os dados públicos podem ser reutilizados, mas sempre com base em propósitos legítimos.

Essas diretrizes da LGPD sobre o uso e compartilhamento de dados buscam equilibrar o avanço da pesquisa científica com a proteção da privacidade dos indivíduos, garantindo que os dados pessoais, sejam públicos ou privados, sejam tratados de maneira ética, segura e legal.

> **Exemplo:** Uma Secretaria Estadual de Saúde desenvolve um sistema público de monitoramento epidemiológico que disponibiliza informações sobre a incidência de doenças respiratórias em diferentes regiões do estado. Esses dados, fornecidos por hospitais e clínicas, incluem dados de saúde agregados, como número de casos por faixa etária, sexo e região geográfica, e são publicamente acessíveis para análise por pesquisadores, órgãos de saúde e o público em geral.

1. Tratamento de Dados Públicos (Art. 7°, § 3°)

A Universidade Federal de Ciências da Saúde decide utilizar os dados do sistema público para um estudo que visa identificar padrões geográficos de propagação de doenças respiratórias. De acordo com a LGPD, os dados podem ser utilizados, desde que o uso seja alinhado com a finalidade original para a qual os dados foram disponibilizados, ou seja, o monitoramento de doenças respiratórias.

A pesquisa é conduzida em conformidade com o interesse público, uma vez que o objetivo do estudo é auxiliar na prevenção e controle de doenças. A universidade, portanto, utiliza os dados respeitando a finalidade inicial, sem violar os direitos dos titulares.

2. Dispensa de Consentimento para Dados Públicos (Art. 7°, § 4°)

Os dados de saúde agregados, que foram tornados públicos pela Secretaria Estadual de Saúde, podem ser utilizados pela universidade sem necessidade de novo consentimento dos titulares, visto que já foram disponibilizados publicamente. No entanto, mesmo sem a necessidade de consentimento, a LGPD exige que os princípios da lei sejam respeitados, como a transparência e o respeito à privacidade dos indivíduos.

Embora os dados não permitam a identificação direta dos pacientes, a universidade toma precauções adicionais para garantir que não haja nenhum risco de reidentificação dos indivíduos, reforçando o compromisso com a segurança e a ética no tratamento dos dados.

3. Consentimento para Compartilhamento de Dados (Art. 7°, § 5°)

Dado que os dados já são públicos e anonimizados, o compartilhamento com a empresa pode ocorrer sem consentimento adicional, desde que a finalidade original seja respeitada e os dados continuem sendo tratados de maneira segura e ética.

4. Obrigações Adicionais Mesmo com Dispensa de Consentimento (Art. 7°, § 6°)

Mesmo com a dispensa de consentimento para o uso dos dados públicos, a universidade e a empresa parceira ainda precisam cumprir as demais obrigações da LGPD, como garantir a segurança dos dados, proteger os direitos dos titulares e manter a transparência em todas as etapas do tratamento.

Isso inclui informar ao público sobre a pesquisa e garantir que os dados sejam usados exclusivamente para as finalidades legítimas do estudo.

5. Novas Finalidades para Dados Públicos (Art. 7°, § 7°)

Ao final da pesquisa, a universidade decide que os dados analisados podem ser úteis para um novo estudo sobre a relação entre poluição do ar e doenças respiratórias. De acordo com a LGPD, os dados públicos podem ser reutilizados para novas finalidades, desde que os novos fins sejam legítimos, específicos e sigam os princípios da LGPD. A universidade, portanto, poderá continuar utilizando os dados para esta nova pesquisa, assegurando que a finalidade seja claramente justificada e que os direitos dos titulares sejam protegidos.

Resultado

No decorrer do estudo, a Universidade Federal de Ciências da Saúde e a empresa privada cumpriram todas as exigências da LGPD, utilizando os dados públicos de forma responsável, transparente e ética. O estudo resultou em insights importantes sobre a propagação de doenças respiratórias, ajudando na implementação de políticas públicas para melhorar a saúde da população, sem comprometer a privacidade dos indivíduos cujos dados foram utilizados.

5. Responsabilidade Civil na Pesquisa

O tratamento de dados pessoais na pesquisa científica, especialmente os dados sensíveis, como os de saúde, impõe uma série de obrigações de segurança e responsabilidade aos agentes envolvidos. Segundo Bodin de Morais[19], os artigos 42 a 45 da LGPD criam um sistema de responsabilidade civil alinhado com o princípio da Responsabilidade e Prestação de Contas do artigo 6º da LGPD. Esse sistema visa não apenas a reparação de danos causados aos titulares dos dados, mas também a prevenção de incidentes por meio da adoção de medidas preventivas de segurança e transparência.

Pesquisadores e instituições de pesquisa devem ser cautelosos no tratamento de dados de saúde, garantindo a confidencialidade e o uso adequado das informações. De acordo com

[19] DE MORAES, Maria Celina Bodin. LGPD: um novo regime de responsabiliza-ção civil dito proativo. civilistica. com, v. 8, n. 3, p. 1-6, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448

a LGPD, tanto controladores quanto operadores de dados podem ser responsabilizados por danos causados durante o tratamento de informações pessoais. A responsabilidade solidária entre os agentes envolvidos estabelece que todos aqueles que contribuem direta ou indiretamente para o incidente de segurança podem ser chamados a reparar os danos sofridos pelos titulares dos dados[20].

A classificação do tratamento de dados como irregular ocorre quando não são seguidas as disposições da LGPD ou quando as medidas de segurança adequadas não são implementadas. A falta de segurança esperada, especialmente quando os dados são usados em processos de pesquisa, pode configurar violação dos direitos dos titulares e levar à responsabilização legal dos pesquisadores e das instituições.

Além da conformidade legal, é fundamental que os pesquisadores compreendam que a responsabilidade vai além de cumprir as normas: envolve um compromisso ético com os participantes da pesquisa, garantindo que seus dados sejam tratados de maneira segura e transparente.

5.1 Delimitação de Responsabilidades

Para garantir a conformidade com a LGPD, é essencial que haja uma delimitação clara de responsabilidades entre os diferentes agentes envolvidos no tratamento de dados. Isso inclui a comprovação da identidade do pesquisador e de seu vínculo com o órgão de pesquisa[21]. Esses elementos são fundamentais para a instrução de processos que envolvem a disponibilização de acesso a dados pessoais ou seu compartilhamento para a realização de estudos científicos.

Como visto, a LGPD permite o tratamento de dados pessoais sem o consentimento dos titulares, desde que seja para fins de pesquisa por órgãos devidamente reconhecidos, como instituições de ensino e centros de pesquisa. No entanto, mesmo quando o consentimento não é exigido, o princípio da transparência deve ser respeitado. Isso implica garantir que os titulares dos dados tenham acesso a informações claras e precisas sobre o tratamento de suas informações, sempre que possível.

Os pesquisadores devem garantir que os dados sejam tratados exclusivamente para os fins da pesquisa, e essas informações devem ser mantidas em ambientes controlados e seguros dentro da instituição de pesquisa. Essa responsabilidade impõe às instituições a necessidade de investir em infraestrutura tecnológica adequada, bem como em governança de dados para proteger os dados processados durante os estudos.

---

[20] SCHREIBER, Anderson. RESPONSABILIDADE CIVIL NA LEI GERAL DE PRO-TEÇÃO DE DADOS PESSOAIS. In: MENDES, Laura et al. (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

[21] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024.

5.2 Estrutura e Governança de Dados em Instituições de Pesquisa

A realização de pesquisas envolvendo dados sensíveis exige que as instituições de pesquisa desenvolvam uma infraestrutura robusta e um pessoal especializado para garantir a segurança e a conformidade com a LGPD[22]. Muitas instituições podem não ter a estrutura necessária para atender a todas as exigências da lei, mas podem trabalhar em parceria com centros de pesquisa mais avançados para continuar produzindo ciência de forma colaborativa.

Para cumprir as normas da LGPD, as instituições precisam reorganizar suas práticas, especialmente no que diz respeito ao armazenamento seguro de dados e à capacitação da comunidade acadêmica, com destaque para os coordenadores dos projetos de pesquisa. A governança de dados se torna um pilar essencial para garantir que os dados sejam tratados com segurança, e que o uso dessas informações seja transparente e em conformidade com as normas legais[23].

5.3 Responsabilidade Civil de Pesquisadores

Os pesquisadores são responsáveis pela proteção e bem-estar dos participantes de suas pesquisas. De acordo com a Resolução CNS 466/2012, eles devem manter a confidencialidade dos dados coletados, utilizando essas informações exclusivamente para os fins estabelecidos no protocolo de pesquisa. A transferência de dados para terceiros sem autorização é estritamente proibida, e a violação dessa regra pode resultar na responsabilização civil tanto do pesquisador quanto da instituição à qual ele está vinculado.

Se houver um vazamento de dados em decorrência de uma falha de segurança, o pesquisador e a instituição podem ser responsabilizados e obrigados a pagar indenizações por danos morais e materiais aos participantes afetados. Além disso, podem ser aplicadas sanções administrativas pela ANPD.

> **Exemplo:** Um pesquisador acadêmico da Faculdade de Medicina da Universidade Federal de Minas Gerais está conduzindo um estudo sobre a eficácia de um novo tratamento para diabetes. Para isso, ele coleta dados sensíveis de saúde de centenas de pacientes, incluindo históricos médicos detalhados e informações genéticas.

---

[22] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024.

[23] MENEZES, Daniel Francisco Nagao; SAAVEDRA, Giovani Agostini. COMPARTI-LHAMENTO DE DADOS CIENTÍFICOS E A PROTEÇÃO JURÍDICA NA EU-ROPA. Duc In Altum-Cadernos de Direito, v. 14, n. 33, 2022.

Suponha que, devido a uma falha de segurança no sistema de armazenamento de dados usado pelo pesquisador, essas informações confidenciais são indevidamente acessadas e divulgadas publicamente. O vazamento inclui nomes, datas de nascimento e detalhes médicos dos participantes, levando a preocupações significativas sobre sua privacidade e bem-estar.

Neste caso, o pesquisador e a Universidade Federal de Minas Gerais podem ser responsabilizados civilmente. A responsabilidade do pesquisador surge de sua obrigação direta de proteger os dados confidenciais dos participantes, conforme estabelecido pelas normas de ética em pesquisa e pela legislação de proteção de dados. A universidade, como instituição à qual o pesquisador está vinculado, também pode ser responsabilizada por não ter implementado medidas de segurança adequadas para prevenir tal vazamento.

As consequências para ambas as partes podem incluir a necessidade de pagar indenizações por danos morais aos participantes afetados, que podem sofrer discriminação ou outros prejuízos devido à exposição de seus dados sensíveis. Além disso, podem ocorrer sanções administrativas ou penalidades conforme determinado pela legislação aplicável, refletindo a gravidade do descumprimento das obrigações de proteção de dados.

Exemplo: Uma seguradora de saúde adquire, de forma indevida, um extenso banco de dados contendo informações médicas detalhadas de milhares de indivíduos. Em seguida, ela emprega técnicas de inteligência artificial para analisar esses dados e estimar os riscos de saúde dos potenciais clientes.

Com base nesses riscos, a seguradora passa a oferecer planos de saúde com preços variáveis: tarifas mais elevadas para indivíduos com maior probabilidade de desenvolver doenças de alto custo e condições mais vantajosas para aqueles com menor risco de saúde.

Esse procedimento viola a Lei Geral de Proteção de Dados Pessoais (LGPD) em diversos aspectos. Primeiramente, há uma violação do princípio da finalidade, pois os dados coletados para cuidados de saúde são utilizados para fins econômicos.

Além disso, o uso de informações sensíveis para definir preços pode ser considerado discriminatório, pois beneficia ou prejudica economicamente os indivíduos com base em sua condição de saúde.

Este caso destaca a importância crítica da LGPD na proteção dos direitos dos cidadãos, assegurando que dados sensíveis, como informações de saúde, não sejam usados de maneira abusiva ou prejudicial.

5.4 Boas Práticas no Tratamento de Dados de Saúde

A adoção de boas práticas no tratamento de dados é fundamental para evitar incidentes e garantir a conformidade com a LGPD. Algumas dessas práticas incluem:

• Definição clara de finalidade e fundamentação legal: Toda pesquisa deve ter uma finalidade específica e ser baseada em uma das hipóteses legais previstas na LGPD, como o consentimento informado ou a tutela da saúde.

• Consentimento explícito quando necessário: Quando a base legal for o consentimento, este deve ser claro, informado e registrado de forma adequada.

• Controle de acesso: Apenas pesquisadores autorizados devem ter acesso aos dados, e medidas de segurança, como autenticação de dois fatores, devem ser implementadas.

• Proteção de dados: Os dados devem ser protegidos com técnicas como criptografia e sistemas de segurança atualizados para prevenir ataques cibernéticos.

• Políticas de retenção de dados: Definir o período de retenção de dados e garantir que sejam destruídos de maneira segura após o término da pesquisa.

• Auditoria e transparência: Manter registros detalhados sobre o tratamento de dados, desde a coleta até o compartilhamento, para fins de auditoria e prestação de contas.

• Treinamento dos pesquisadores: Todos os envolvidos na pesquisa devem receber treinamento contínuo em segurança de dados e conformidade regulatória.

A responsabilidade civil no contexto da pesquisa com dados de saúde exige não apenas o cumprimento das normas da LGPD, mas também uma postura ética por parte dos pesquisadores e das instituições. Ao adotar boas práticas de tratamento de dados e garantir a segurança, os pesquisadores podem evitar incidentes que comprometam a privacidade dos participantes e possam resultar em responsabilizações legais.

6. Consentimento Informado

6.1 Diferença entre o Consentimento na Relação Médico-Paciente e na Pesquisa

No campo da saúde, o consentimento informado é amplamente conhecido, mas é preciso diferenciar o consentimento para o ato médico e o consentimento para o tratamento de dados pessoais. No contexto médico-paciente, o consentimento refere-se à autorização do paciente para a realização de procedimentos médicos, como cirurgias. O médico deve informar ao paciente sobre os benefícios, alternativas, riscos, orientaçãoes pós-operatórias e obter o consentimento explícito do paciente[24].

O consentimento nesse caso é um procedimento contínuo que começa com a prestação de informações durante o atendimento, passa pela verificação da compreensão do paciente, e se encerra com a formalização em um Termo de Consentimento Livre e Esclarecido (TCLE),

[24] FRANÇA, Genival Veloso de. Direito Médico. Rio de Janeiro: Forense, 2021.

quando aplicável. O TCLE é uma forma escrita de consentimento, mas todo o processo é baseado em uma comunicação contínua entre médico e paciente[25].

Já no tratamento de dados pessoais, o consentimento é específico e deve ser fundamentado em uma base legal clara, conforme exigido pela LGPD. Para coleta e uso de dados pessoais, é necessário informar a finalidade, o prazo e outras informações relevantes para o tratamento de dados.

6.2 Termo de Consentimento e de Responsabilidade

Quando órgãos públicos ou entidades governamentais fornecem acesso a bases de dados para fins de pesquisa, é comum a exigência de um termo de ciência e responsabilidade. Esse documento garante que a instituição que receberá os dados compreende as obrigações legais e éticas relacionadas ao uso desses dados, comprometendo-se a proteger a privacidade e a confidencialidade das informações.

A documentação de cada acesso ao banco de dados é essencial, registrando quem acessou, quando e por que. Isso é similar aos procedimentos em pesquisas que envolvem seres humanos, onde os projetos devem passar por um Comitê de Ética em Pesquisa (CEP) ou pela Comissão Nacional de Ética em Pesquisa (CONEP) para garantir a conformidade com normas éticas.

A LGPD não especifica um método rígido de identificação de pesquisadores, permitindo que instituições adotem formatos de identificação legítimos, como meios digitais. O documento de identificação deve, no entanto, ser assinado pela instituição responsável, confirmando o vínculo do pesquisador com o órgão de pesquisa.

O Termo de Consentimento Livre e Esclarecido (TCLE) desempenha um papel fundamental nesse contexto, pois detalha os direitos dos participantes, os procedimentos, os riscos e os benefícios da pesquisa. O pesquisador é responsável por garantir que o TCLE seja claro e compreensível, para que o participante ou seu representante legal possa consentir de maneira informada e consciente. Para menores de 18 anos, além do TCLE, é necessário um Termo de Assentimento Livre e Esclarecido (TALE), redigido em linguagem acessível.

Nas Ciências Humanas e Sociais, o consentimento pode ser obtido em diferentes formatos, como gravações de áudio, vídeos ou documentos digitais, conforme estabelecido pela Resolução CNS nº 510/2016. O objetivo é adaptar o processo de consentimento ao contexto cultural e à metodologia do estudo, garantindo que os participantes estejam plenamente informados.

[25] FRANÇA, Genival Veloso de. Direito Médico. Rio de Janeiro: Forense, 2021.

Resolução CNS nº 510/2016

Ao redigir o TCLE, é importante que o documento use uma linguagem simples e que o formato seja invitativo, conforme orienta o item IV.5.b da Resolução CNS nº 466/12. O título do documento deve ser "Termo de Consentimento Livre e Esclarecido", sem variações.

6.3 Exceções à Obrigatoriedade do TCLE

Embora o consentimento seja uma prática fundamental na proteção dos direitos dos titulares dos dados, existem exceções previstas na LGPD e nas normas éticas brasileiras. O artigo 11, inciso II da LGPD estabelece que o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento do titular nas seguintes situações:

• Políticas Públicas pela Administração Pública: Dados pessoais podem ser usados sem consentimento quando forem indispensáveis para a execução de políticas públicas previstas em leis ou regulamentos.

• Estudos por Órgãos de Pesquisa: Dados sensíveis podem ser tratados para estudos por órgãos de pesquisa, desde que, sempre que possível, os dados sejam anonimizados.

• Tutela da Saúde: Dados sensíveis podem ser tratados sem consentimento para proteger a saúde em procedimentos realizados por profissionais de saúde ou autoridades sanitárias.

Além disso, de acordo com a Resolução CNS 466/2012, o TCLE pode ser dispensado em casos excepcionais, quando sua obtenção for inviável ou causar riscos à privacidade do participante. Nesses casos, o pesquisador deve solicitar a dispensa ao Sistema CEP/CONEP para avaliação.

A Resolução CNS nº 510/2016 também prevê a dispensa do TCLE em pesquisas específicas nas ciências humanas e sociais, como:

• Pesquisas de opinião pública com participantes não identificados;
• Uso de informações de acesso público;
• Pesquisas censitárias;
• Uso de bancos de dados com informações agregadas que não permitem a identificação individual;
• Revisões de literatura com base em textos científicos;
• Estudos teóricos sem identificação de participantes e atividades educacionais.

Essas exceções reconhecem que, em certos casos, a obtenção de consentimento pode ser desnecessária ou impraticável, mas reforçam a necessidade de transparência e segurança no tratamento de dados pessoais em todas as circunstâncias.

> **Exemplo:** A pesquisa, conduzida por uma renomada universidade de medicina, visa avaliar a eficácia e segurança de um novo medicamento para diabetes. O estudo envolve múltiplos centros e um grande número de participantes de diversas idades e regiões.

Desenvolvimento do TCLE: O Dr. Silva, o pesquisador principal, está consciente da importância de um TCLE bem elaborado para garantir o consentimento informado dos participantes. Ele decide rever o documento cuidadosamente para assegurar que esteja em conformidade com a Resolução CNS nº 466/12.

Ações tomadas:

Linguagem Acessível:
O Dr. Silva utiliza uma linguagem clara e direta, evitando termos técnicos sem explicações simples e compreensíveis.
Para atender às necessidades de todos os participantes, o termo é traduzido para vários idiomas predominantes na região dos centros de pesquisa.

Formato de Convite:

O documento é estruturado como um convite para participar do estudo, explicando detalhadamente os procedimentos, riscos, benefícios e alternativas ao tratamento proposto.
É enfatizado que a participação é totalmente voluntária e que os participantes podem se retirar a qualquer momento sem penalidades.

Clareza nos Direitos e Responsabilidades:

O TCLE esclarece o direito dos participantes de acessar suas informações e receber resultados relevantes do estudo.
São detalhadas as medidas de confidencialidade para proteger a identidade e os dados dos participantes.

Processo de Assentimento para Menores:

Para participantes menores de 18 anos, um Termo de Assentimento Livre e Esclarecido (TALE) é preparado com linguagem adequada à idade.
São realizadas sessões informativas com os pais ou responsáveis legais para garantir sua compreensão e concordância com os termos do estudo.

Conclusão: A implementação cuidadosa do TCLE e do TALE assegura que todos os participantes estejam adequadamente informados sobre todos os aspectos da pesquisa. Isso não só fortalece a validade ética do estudo, mas também promove a confiança entre os participantes e a equipe de pesquisa, contribuindo para o sucesso geral do projeto.

7. Prevenção de Vazamento de Dados

7.1 Resposta a Incidentes de Segurança da Informação em Pesquisas de Saúde

A LGPD impõe uma série de obrigações às instituições de saúde que conduzem pesquisas científicas, especialmente no que tange à prevenção e resposta a incidentes de segurança. Esses incidentes podem comprometer a integridade, confidencialidade e disponibilidade das informações pessoais dos participantes da pesquisa, o que exige uma ação rápida e eficaz para evitar danos aos titulares dos dados.

A resposta a esses incidentes deve seguir um procedimento claro e organizado, que inclui tanto a comunicação à ANPD quanto a adoção de medidas para mitigar os impactos do incidente.

Passo a Passo para Comunicação de Incidente de Segurança à ANPD[27]:

• Identificação do Incidente: O controlador (responsável pelo tratamento dos dados) deve identificar imediatamente que ocorreu um incidente de segurança que afetou dados pessoais.

• Prazo para Comunicação: A comunicação do incidente deve ser feita à ANPD no prazo de até três dias úteis a partir do momento em que o controlador tomou conhecimento do evento.

• Informações a Serem Incluídas na Comunicação:

  • Descrição da natureza e categoria dos dados pessoais afetados.
  • Número de titulares impactados, incluindo crianças, adolescentes ou idosos, se aplicável.
  • Medidas de segurança adotadas antes e após o incidente.
  • Avaliação dos riscos decorrentes do incidente e possíveis impactos sobre os titulares.
  • Motivos de qualquer atraso na comunicação à ANPD.
  • Medidas que estão sendo ou serão adotadas para mitigar os efeitos do incidente.
  • Data da ocorrência e do conhecimento do incidente.
  • Informações do encarregado de proteção de dados ou representante do controlador.
  • Identificação do controlador, com sua classificação como agente de pequeno porte, se aplicável.
  • Identificação do operador de dados, se aplicável.

[27] https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

- Detalhes do incidente, incluindo a causa principal, se possível.
- Número total de titulares cujos dados estão sendo tratados nas atividades afetadas.

• Formulário Eletrônico: A comunicação à ANPD deve ser feita por meio do formulário eletrônico disponibilizado no site da autoridade.

• Documentação Complementar: Devem ser apresentados documentos que comprovem o vínculo do encarregado com o controlador ou um instrumento de outorga de poderes para representação junto à ANPD.

• Prazos Especiais: Para agentes de pequeno porte, os prazos de comunicação podem ser contados em dobro.

• Solicitação de Sigilo: O controlador pode solicitar à ANPD que determinadas informações sejam mantidas em sigilo para proteger segredos comerciais ou industriais.

• Requisição de Informações Adicionais pela ANPD: A ANPD pode solicitar informações complementares sobre o incidente, como registros de operações de tratamento e relatórios de impacto.

Implementar uma resposta eficaz a incidentes de segurança é fundamental não apenas para o cumprimento das obrigações legais, mas também para preservar a confiança dos participantes de pesquisa e a integridade dos sistemas de dados utilizados.

7.2 Boas Práticas para Prevenir Vazamentos de Dados

Para prevenir vazamentos de dados e evitar as consequências legais e reputacionais associadas a esses incidentes, as organizações devem adotar boas práticas de proteção de dados, tais como:

Controle de Acesso: Garantir que apenas pessoas autorizadas tenham acesso a dados pessoais, utilizando autenticação de dois fatores e senhas fortes.

Criptografia: Proteger os dados em trânsito e em repouso por meio de criptografia, dificultando o acesso não autorizado.

Treinamento de Funcionários: Todos os envolvidos no tratamento de dados devem ser treinados para reconhecer e evitar riscos de segurança.

Políticas de Retenção de Dados: Definir claramente por quanto tempo os dados serão

mantidos e garantir que sejam eliminados de forma segura ao final do período de retenção.

Auditorias Regulares: Realizar auditorias periódicas dos sistemas de dados para identificar possíveis vulnerabilidades e corrigi-las antes que causem problemas.

Simulação de Incidentes: Testar regularmente os procedimentos de resposta a incidentes para garantir que a equipe esteja preparada para agir rapidamente em caso de vazamento de dados.

Implementar essas práticas não apenas ajuda a prevenir incidentes de segurança, mas também demonstra um compromisso com a proteção de dados e a conformidade com a LGPD.

7.3 O Papel da ANPD

A ANPD é a entidade responsável por fiscalizar, regular e educar a respeito da LGPD, com o objetivo de garantir a proteção de dados pessoais no Brasil. A ANPD desempenha diversas funções que incluem:

Monitoramento da Conformidade: A ANPD fiscaliza o cumprimento da LGPD por meio de inspeções e auditorias em organizações que tratam dados pessoais, inclusive no setor de saúde e pesquisa científica.

Emissão de Diretrizes: A autoridade emite orientações e regulamentações que ajudam as organizações a seguirem as melhores práticas de proteção de dados.

Fiscalização de Infrações e Aplicação de Sanções: Quando necessário, a ANPD aplica sanções que variam de advertências a multas significativas, dependendo da gravidade da infração.

Educação e Conscientização: A ANPD também realiza seminários, workshops e outras atividades educativas para promover o cumprimento da LGPD e conscientizar as organizações e o público sobre a importância da proteção de dados.

As sanções aplicadas pela ANPD visam, além de punir as infrações, incentivar a conformidade com a legislação. Além das sanções administrativas, a LGPD também permite a responsabilização judicial, incluindo ações civis para indenizações por danos morais e materiais[28].

---

[28] WIMMER, Miriam. OS DESAFIOS DO ENFORCEMENT NA LGPD: FISCALI-ZAÇÃO, APLICAÇÃO DE SANÇÕES ADMINISTRATIVAS E COORDENAÇÃO INTERGOVERNAMENTAL. In: MENDES, Laura et al. (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

7.4 Sanções Previstas na LGPD

A LGPD estabelece um regime de sanções administrativas para o caso de descumprimento de suas disposições. Essas sanções podem variar em grau de severidade, dependendo do tipo de infração e do impacto causado aos titulares dos dados pessoais. Entre as sanções mais comuns estão[29]:

Advertência: Para infrações leves, a ANPD pode emitir uma advertência, exigindo que a organização corrija a falha dentro de um prazo determinado.

Multa Simples: A organização pode ser multada em até 2% do faturamento da empresa no Brasil, limitada a R$ 50 milhões por infração.

Multa Diária: Além da multa simples, a ANPD pode aplicar uma multa diária para forçar o cumprimento das obrigações.

Publicização da Infração: A ANPD pode exigir que a infração seja tornada pública para expor a organização e alertar os titulares dos dados.

Bloqueio dos Dados: Em casos graves, a ANPD pode determinar o bloqueio do uso dos dados pessoais afetados pela infração até que o problema seja resolvido.

Eliminação dos Dados: A eliminação definitiva dos dados pessoais relacionados à infração também pode ser exigida, como medida extrema para proteger os direitos dos titulares.

Essas sanções visam tanto punir as infrações quanto incentivar a conformidade com a LGPD, preservando os direitos dos titulares dos dados e incentivando a adoção de boas práticas de segurança e privacidade.

7.5 Protocolo para Realização de Pesquisa com Dados de Saúde

Para garantir que uma pesquisa com dados de saúde seja conduzida de maneira segura e em conformidade com a LGPD, os pesquisadores devem seguir um protocolo claro e objetivo. Abaixo segue uma sugestão de protocolo de pesquisa com dados de saúde, estruturado em sete passos, que visa auxiliar os pesquisadores a planejarem e executarem suas pesquisas respeitando os princípios da minimização de dados, segurança e transparência.

---

[29] LGPD, art. 52

Passo 1: Definição de Objetivos e Coleta de Dados

No planejamento da pesquisa, é essencial definir objetivos específicos e determinar quais dados pessoais serão necessários para atingir esses objetivos[30]. A coleta deve ser limitada ao mínimo necessário, em conformidade com o princípio da minimização de dados estabelecido pelo art. 6º, inciso III da LGPD. Caso dados desnecessários sejam coletados, eles devem ser retidos apenas o tempo necessário para a sua identificação e, em seguida, eliminados[31].

Passo 2: Armazenamento e Precauções de Segurança

Durante o planejamento da pesquisa, também devem ser abordadas questões relacionadas ao armazenamento dos dados e às precauções de segurança que serão adotadas. O ambiente onde os dados serão armazenados deve ser seguro, controlado e protegido contra acessos não autorizados, conforme as melhores práticas de segurança da informação[32].

Passo 3: Consultoria em Segurança de Dados

Se necessário, é aconselhável que o pesquisador conte com o auxílio de profissionais especializados em segurança de dados para garantir que todas as práticas de tratamento de dados pessoais estejam de acordo com a legislação e os padrões de segurança recomendados.

Passo 4: Coleta de Dados Primários

Na coleta de dados primários, o pesquisador deve utilizar um instrumento de coleta que seja compatível com o plano de pesquisa, garantindo que apenas os dados estritamente necessários sejam coletados[33]. Caso não seja possível evitar a coleta de dados desnecessários, eles devem ser imediatamente eliminados ou anonimizados. Se a exclusão ou anonimização não for viável, o acesso a esses dados deve ser restrito, e o pesquisador deve justificar a impossibilidade de eliminar ou anonimizar as informações.

Passo 5: Cessão de Dados por Terceiros

Quando houver a cessão de dados pessoais por terceiros para a realização da pesquisa, o controlador original dos dados deve garantir que o pesquisador cumpra todas as imposições legais, como autorização para o uso dos dados e a adoção das medidas de segurança

[30] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024.

[31] BUCHAIN, Luiz Carlos. Minimização e proporcionalidade na coleta de dados. Direitos Democráticos & Estado Moderno, v. 2, n. 5, 2022.

[32] ALMEIDA TEIXEIRA, G., MIRA DA SILVA, M., & PEREIRA, R. The critical suc-cess factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance, 21(4), 402-418, 2019.

[33] MONTEIRO, Gina Torres Rego; DA HORA, Henrique Rego Monteiro. Pesquisa em saúde pública: como desenvolver e validar instrumentos de coleta de dados. Editora Appris, 2013

necessárias. Embora a LGPD dispense o consentimento específico do titular dos dados para pesquisas em saúde por órgãos de pesquisa, o controlador deve garantir a transparência e que os dados sejam tratados de acordo com a legislação.

Passo 6: Anonimização e Pseudoanonimização

Sempre que possível, o tratamento de dados pessoais em pesquisas de saúde deve ser feito com a anonimização dos dados. Quando a anonimização completa não for viável, recomenda-se o uso de técnicas de pseudoanonimização para proteger a privacidade dos titulares. Caso essas técnicas não possam ser aplicadas, o pesquisador deve justificar a impossibilidade e adotar outras medidas de segurança adequadas.

Além disso, os pesquisadores devem estar atentos às questões éticas envolvidas na manipulação de dados de saúde. Diagnósticos ou informações sensíveis descobertas durante a pesquisa devem ser tratados com extrema cautela, respeitando não apenas a LGPD, mas também as recomendações éticas e deontológicas da área da saúde[34].

Passo 7: Eliminação de Dados ao Final da Pesquisa

Ao término da pesquisa, os dados pessoais tratados devem ser eliminados, a menos que haja uma justificativa legal para sua retenção, como a necessidade de utilização em novas pesquisas ou para uso interno do controlador[35]. Caso os dados precisem ser mantidos, devem ser anonimizados, impedindo o acesso de terceiros. É importante que o pesquisador consulte os órgãos técnicos, como o Departamento de Tecnologia da Informação ou o Departamento de Arquivologia, para garantir a correta eliminação dos dados.

Em casos de dados que foram anonimizados de maneira eficiente, a eliminação não será necessária, uma vez que, conforme a LGPD, dados anonimizados não são mais considerados dados pessoais[36].

Além disso, a ABNT NBR ISO/IEC 27555:2023, que trata de segurança da informação e remoção de dados pessoais, pode servir como um guia adicional para assegurar que todas as etapas de tratamento e eliminação de dados pessoais sejam realizadas de forma segura e em conformidade com as melhores práticas de proteção de dados.

Seguindo este protocolo, os pesquisadores estarão melhor preparados para conduzir suas pesquisas com dados de saúde de maneira ética, segura e em conformidade com a legislação, minimizando riscos de vazamentos e garantindo a proteção dos direitos dos titulares dos dados.

---

[34] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024

[35] FEITOSA, Lukas Darien Dias. A proteção de Dados Pessoais na Pesquisa em Saúde. São Paulo: Editora Dialética,2024

[36] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica. com, v. 9, n. 3, p. 1-23, 2020.

Referências bibliográficas

1. ALMEIDA TEIXEIRA, G., MIRA DA SILVA, M., & PEREIRA, R. The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4), 402-418, 2019.

2. BARRETO, Mauricio L.; ALMEIDA, Betânia; DONEDA, Danilo. Uso e proteção de dados pessoais na pesquisa científica. In: MENDES, Laura et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

3. BIONE, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, v. 9, n. 3, p. 1-23, 2020.

4. BIONE, Bruno Ricardo; LUCIANO, Maria. O Consentimento Como Processo: Em Busca do Consentimento Válido. In: MENDES, Laura et al. (Org.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 243-258.

5. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Guia de tratamento de dados pessoais para fins acadêmicos*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 01 set. 2024.

6. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). G*uia orientativo para os agentes de tratamento de dados pessoais*. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 01 set. 2024.

7. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 15, de 24 de abril de 2024. *Diário Oficial da União*: seção 1, Brasília, DF, 25 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 01 set. 2024.

8. BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 set. 2024.

9. BRASIL. *Ministério da Saúde*. Portaria GM/MS nº 3.232, de 4 de março de 2024. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2024/prt3232_04_03_2024.html. Acesso em: 01 set. 2024.

10. BUCHAIN, Luiz Carlos. Minimização e proporcionalidade na coleta de dados. *Direitos Democráticos & Estado Moderno*, v. 2, n. 5, 2022.

11. DALLARI, Analluza Bolivar. *SUS Digital e o conceito de dado pessoal sensível de saúde*. Disponível online em: https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude#_ftn2. Acesso em: 30 jun. 2024.

12. DE MORAES, Maria Celina Bodin. LGPD: um novo regime de responsabilização civil dito proativo. *Civilistica.com*, v. 8, n. 3, p. 1-6, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448.

13. DE TEFFE, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica*.com, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510.

14. FEITOSA, Lukas Darien Dias. *A proteção de Dados Pessoais na Pesquisa em Saúde*. São Paulo: Editora Dialética, 2024.

15. FRANÇA, Genival Veloso de. *Direito Médico*. Rio de Janeiro: Forense, 2021.

16. MENEZES, Daniel Francisco Nagao; SAAVEDRA, Giovani Agostini. Compartilhamento de dados científicos e a proteção jurídica na Europa. *Duc In Altum-Cadernos de Direito*, v. 14, n. 33, 2022.

17. MONTEIRO, Gina Torres Rego; DA HORA, Henrique Rego Monteiro. *Pesquisa em saúde pública: como desenvolver e validar instrumentos de coleta de dados*. Editora Appris, 2013.

18. SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: MENDES, Laura et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

19. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (*Regulamento Geral sobre a Proteção de Dados - RGPD*). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 01 set. 2024.

20. WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: MENDES, Laura et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

Sobre os autores

Gabriella da Silva Reis

Advogada. Mestranda em Direito na Universidade Federal de Minas Gerais. Membro e Pesquisadora do Centro de Pesquisa em Direito, Tecnologia e Inovação - Centro DTIBR. Pesquisadora do Grupo de Estudos em Direito e Tecnologia - DTec (UFMG, Brasil). Editora Executiva da Brazilian Journal of Law, Technology and Innovation (ISSN 2965-1549). Pós-Graduada Lato Sensu em Direito Médico pela Faculdade CERS (2022). Bacharela em Direito pela Universidade Federal do Maranhão (2018).

Currículum Lattes: http://lattes.cnpq.br/9083642276664249

Profa. Zilma Silveira Nogueira Reis

Professora Associada da Faculdade de Medicina da UFMG, onde coordena o Centro de Informática em Saúde. Bolsista de Produtividade, Desenvolvimento Tecnológico e Extensão Inovadora do CNPq (Nível 2). Coordenadora de Educação e Difusão do Conhecimento do CI-IA Saúde.

Currículum Lattes: http://lattes.cnpq.br/569566480824


CI-IA
Centro de Inovação em
Inteligência Artificial

Realização

CI-IA
Centro de Inovação em Inteligência Artificial

Apoio

UFMG
UNIVERSIDADE FEDERAL DE MINAS GERAIS

9 786586 593464