

CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

AUGUSTO VINÍCIUS MORAES PANTOJA
PAULO VITOR BARRA MELO

IMPLEMENTAÇÃO DA LGPD NA ÁREA DA SAÚDE: impactos e desafios

BELÉM
2023

AUGUSTO VINÍCIUS MORAES PANTOJA
PAULO VITOR BARRA MELO

IMPLEMENTAÇÃO DA LGPD NA ÁREA DA SAÚDE: impactos e desafios

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Prof.^a Me. Amanda Maia Ramalho

BELÉM
2023

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca do CESUPA, Belém – PA

P198i Pantoja, Augusto Vinicius Moraes.

Implementação da LGPD na área da saúde: impactos e desafios / Augusto Vinicius Moraes Pantoja, Paulo Vitor Barra Melo. — Belém, 2023.

21 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2023.

Orientadora: Profa. Me. Amanda Maia Ramalho.

1. [Lei Geral de Proteção de Dados (2018)]. 2. Saúde. 3. Direito à privacidade. I. Melo, Paulo Vitor Barra. II. Título.

CDD 342.6

AUGUSTO VINÍCIUS MORAES PANTOJA
PAULO VITOR BARRA MELO

IMPLEMENTAÇÃO DA LGPD NA ÁREA DA SAÚDE: impactos e desafios

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Prof.^a Me^a Amanda Maia Ramalho

Data de aprovação: ____/____/____

Conceito:

Banca Examinadora:

Prof.^a Me. AMANDA MAIA RAMALHO - Orientadora
Centro Universitário do Estado do Pará (CESUPA)

Nome com titulação
Instituição a que pertence

Nome com titulação
Instituição a que pertence

IMPLEMENTAÇÃO DA LGPD NA ÁREA DA SAÚDE: IMPACTOS E DESAFIOS

LGPD IMPLEMENTATION IN THE HEALTHCARE SECTOR: IMPACTS AND CHALLENGES

Augusto Vinícius Moraes Pantoja, DI9NA, augustovmpantoja@gmail.com. 21060220

Paulo Vitor Barra Melo, DI9NA, paulovbmelo@gmail.com. 20060312

Amanda Maia Ramalho

RESUMO

Este estudo analisa os impactos e desafios da implementação da Lei Geral de Proteção de Dados (LGPD) na área da saúde no Brasil, através de uma revisão bibliográfica sobre o tema. O referencial teórico aborda os princípios, fundamentos e direitos garantidos pela LGPD, além dos requisitos específicos para planos de saúde e a gestão de dados sensíveis. A análise revela dificuldades como investimentos em tecnologia, mudanças culturais e complexidade dos dados. As conclusões trazem recomendações para adequação à LGPD no setor da saúde, destacando oportunidades como inovação, transparência e confiança. O estudo contribui para o entendimento dos desafios regulatórios e práticos da proteção de dados em saúde.

Palavras-chave: Lei Geral de Proteção de Dados; Coleta de dados; Dados sensíveis; Saúde; Privacidade.

ABSTRACT

This study analyzes the impacts and challenges of implementing the General Data Protection Law (LGPD) in healthcare in Brazil, through a literature review on the subject. The theoretical framework addresses the principles, fundamentals and rights guaranteed by LGPD, in addition to specific requirements for health insurance plans and the management of sensitive data. The analysis reveals difficulties such as investments in technology, cultural changes and data complexity. The conclusions bring recommendations for adequacy to LGPD in the health sector, highlighting opportunities such as innovation, transparency and trust. The study contributes to the understanding of regulatory and practical challenges of data protection in healthcare.

Key words: Brazilian General Data Protection Law; Data collection; Sensitive data; Healthcare; Privacy.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) é uma legislação que tem como objetivo proteger os dados pessoais dos cidadãos, garantindo que as empresas e organizações que coletam e utilizam esses dados sigam regras claras e transparentes. Na área da saúde, a LGPD tem um papel fundamental na proteção dos dados sensíveis dos pacientes, como informações sobre sua saúde, tratamentos e histórico médico. A coleta e gestão desses dados devem ser feitas de forma segura e responsável, garantindo a privacidade e a segurança dos pacientes.

No entanto, a implementação da LGPD na área da saúde apresenta desafios consideráveis, como a necessidade de adaptação dos sistemas de informação e a capacitação dos profissionais de saúde para lidar com as novas regras. Além disso, é preciso garantir que as empresas e organizações que atuam na área da saúde estejam em conformidade com a legislação, evitando possíveis sanções e prejuízos à imagem.

Diante desse cenário, este artigo tem como objetivo analisar os impactos e obstáculos da implementação da LGPD na área da saúde no Brasil, buscando contribuições relevantes às discussões sobre proteção de dados e privacidade na seara da saúde. Para tanto, realizamos uma revisão bibliográfica, examinando o referencial teórico disponível sobre o tema e os desafios enfrentados pelo setor. Foram consultadas fontes fidedignas nas áreas do direito, saúde e tecnologia, visando construir um panorama abrangente do cenário atual.

Os resultados desta pesquisa reforçam a importância da legislação como uma salvaguarda crucial para os direitos dos indivíduos, especialmente na sensível área da saúde.

O artigo identifica e discute desafios concretos enfrentados pelas organizações de saúde na implementação da LGPD, ao mesmo tempo em que destaca oportunidades trazidas pela lei.

As conclusões trazem recomendações práticas para adequação à LGPD no contexto da saúde, ressaltando a importância de investimentos em governança, tecnologia, processos e pessoas para uma conformidade efetiva. Revelam ainda o potencial da lei para melhorias em transparência, segurança e inovação.

Os resultados gerais indicam que, apesar de complexa, a adaptação dos agentes de tratamento de dados na área da saúde à LGPD é essencial para elevar os padrões éticos do setor e resguardar direitos dos pacientes na era digital. O estudo contribui para o avanço tanto das discussões acadêmicas quanto das práticas organizacionais relacionadas à proteção de dados na seara da saúde.

Em suma, este artigo não apenas evidencia a complexidade da implementação da LGPD nos planos de saúde, mas também oferece contribuições tangíveis para a prática e o

desenvolvimento futuro de políticas, promovendo uma integração harmoniosa da LGPD na área da saúde.

2 A EVOLUÇÃO HISTÓRICA DAS SOCIEDADES E A INFORMAÇÃO COMO NOVO PARADIGMA NA ERA DIGITAL

Conforme analisado por Bioni (2021), as sociedades humanas evoluíram ao longo da história passando por diferentes estágios, nos quais elementos centrais como a agricultura, a indústria e os serviços foram se tornando o motor propulsor das transformações econômicas e sociais em cada época. Hodiernamente, vive-se na era da informação, em que os dados valem cada vez mais. Isso faz com que aconteçam mudanças significativas, fazendo com que haja a necessidade de se estabelecer regulações para proteção da privacidade e uso ético das informações pessoais na atual era digital

A revolução da informação teve início em meados de 1960, com o surgimento de tecnologias que passaram das fases mecânica, analógica e digital. Nesse período, os computadores e os registros digitais se tornaram comuns. Essas tecnologias afetaram sobremaneira as formas de organização das relações econômicas e sociais, bem como as condições de realização de valores fundamentais como a liberdade e a democracia. (CUNHA, s.d.)

No centro da mudança, estão, de um lado, a informação como recurso estratégico e principal fonte de riqueza na “sociedade da informação”; e, de outro lado, a comunicação como veículo de múltiplos e variados contatos, mensagens e conteúdos informativos, no que também vem sendo chamado de “sociedade em rede”.

A escala do fenômeno permite afirmar que vivemos numa nova era marcada, em particular, por uma economia baseada, crescentemente, na informação, bem como em uma relação diferente das pessoas com o espaço, agora sem fronteiras, e com o tempo, mais acelerado pela automatização. Ademais, houve uma modificação das condições de acesso e de distribuição do poder, que é cada vez mais função do acesso às redes e do controle sobre os fluxos de informação e sobre a comunicação. (PERASSO, 2016)

Anteriormente, o acúmulo, o armazenamento e a transmissão da informação davam-se na forma de átomos, resultando em algo denso e material, como um livro ou um arquivo. Com o passar do tempo, todo tipo de informação foi digitalizada, tal como o áudio e o vídeo, em novas plataformas, como CDs, pen drives, computadores pessoais, entre outros.

A técnica binária possibilitou que a informação fosse mais precisamente organizada, facilitando, em última análise, o seu próprio acesso. Por exemplo, a busca por informação em arquivos digitais é muito mais fácil do que vasculhar pastas e papéis arquivados, como acontecia em outros tempos. A evolução binária da era da informação hoje permite comprimir o armazenamento da informação e, ao mesmo tempo, possibilitou um acesso mais facilitado. Houve, portanto, um progresso quantitativo e qualitativo na era da informação. (BIONI, 2021)

Ademais, a popularização da internet foi um fator determinante para que houvesse a evolução histórica que resultou na era da informação. A internet possibilitou a troca de informações de forma rápida e global, permitindo que pessoas em diferentes partes do mundo possam se comunicar e compartilhar informações quase que instantaneamente. Dessa forma, a internet mudou a nossa forma de interação com o mundo, tanto pessoal quanto profissionalmente.

Com a popularização da internet e das novas tecnologias, a informação se tornou amplamente disponível e acessível a todos, o que transformou a relação entre produtores e consumidores. Atualmente o consumidor tem um papel cada vez mais ativo na cadeia de produção, deixando de ser apenas um receptor passivo de informações e produtos, e passando a influenciar diretamente a produção e a distribuição dos produtos e serviços.

Não obstante, com essa facilidade de acesso à informação, surgiu o fenômeno das chamadas fake news, que nada mais são que notícias falsas que se espalham com grande rapidez na internet. Isso tem se transformado em gravíssimo problema, visto que, sua disseminação pode influenciar diretamente a sociedade e a política dos países. (CAMPOS, s.d.)

Desse modo, a era da informação trouxe consigo diversas mudanças significativas em vários aspectos da sociedade, e sua evolução histórica continua em curso. Tendo isso em vista, faz-se imprescindível que as pessoas estejam cientes dessas transformações e saibam lidar com as novas tecnologias para aproveitar ao máximo as vantagens que essas mudanças nos oferecem, bem como saibam identificar informações enganosas e nocivas, para que elas não sejam espalhadas para mais pessoas.

3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei no 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi um marco no ordenamento jurídico brasileiro ao introduzir regras gerais setoriais sobre a proteção, privacidade e tratamento ético de dados pessoais no país.

A referida lei tem como objetivos fundamentais proteger os direitos fundamentais de liberdade e privacidade; disciplinar de forma sistêmica o tratamento de dados pessoais; e garantir maior segurança jurídica aos agentes de tratamento por meio de regras claras.

Para isso, a LGPD estabelece princípios, conceitos, direitos dos titulares de dados pessoais e obrigações que recaem sobre as organizações públicas e privadas que realizam operações de tratamento de dados. Entre as principais obrigações incluem-se: publicar política de privacidade, designar encarregado de proteção de dados, adotar medidas de segurança da informação, realizar análises de impacto para mitigação de riscos, garantir os direitos de acesso, correção e eliminação de dados dos titulares, dentre outras.

A LGPD define em seu art. 5º, inciso II o conceito de dados pessoais sensíveis, elencando como tal os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. No contexto da saúde, diversos dados como histórico médico, resultados de exames, condições psicológicas e registro de maus tratos se enquadram no conceito de dado sensível por revelarem aspectos da intimidade do paciente. Portanto, o tratamento desse tipo de dado exige proteção especial e medidas de segurança rigorosas que preservem a privacidade, conforme preconizado pela LGPD. (BRASIL, 2018)

Assim, no contexto do setor da saúde, no qual são tratados com frequência os dados pessoais sensíveis de pacientes — tendo em vista a própria natureza da área da saúde —, a aplicação dos dispositivos previstos na LGPD a tais informações torna-se crucial. Isso visa preservar princípios éticos como a confiança, dignidade e privacidade nas relações entre profissionais de saúde, pacientes e organizações do setor. Além disso, fomenta a inovação responsável e a segurança no uso da tecnologia em benefício do cuidado à saúde.

3.1 PRINCÍPIOS E FUNDAMENTOS DA LGPD APLICADOS NA ÁREA DA SAÚDE

A LGPD é fundamentada em princípios essenciais que regem o tratamento de dados pessoais. Dentre eles, destacam-se a finalidade, necessidade, consentimento, transparência, segurança, prevenção, não discriminação e responsabilização. Compreender

esses princípios é crucial para a adequada aplicação da legislação na área da saúde, onde informações sensíveis são manipuladas diariamente.

A LGPD, no Art. 6º, I a X, estabelece princípios gerais que constituem os alicerces para a proteção de dados pessoais no Brasil. Esses princípios orientam e regulamentam as formas adequadas de coleta, armazenamento, tratamento e compartilhamento de dados pelos agentes de tratamento.

O princípio da finalidade impõe que os dados pessoais somente podem ser coletados para propósitos legítimos e específicos, os quais devem ser informados de forma clara e detalhada ao titular dos dados no momento da coleta. Além disso, os dados não podem ser tratados posteriormente de maneira incompatível ou contrária às finalidades originalmente definidas e autorizadas. Este princípio tem como objetivo prevenir o uso abusivo ou desvirtuado dos dados pessoais. Assim, esse princípio delimita os propósitos pelos quais hospitais, clínicas, planos de saúde e laboratórios podem coletar e utilizar dados pessoais de pacientes, restringindo essa coleta a fins específicos de diagnóstico, tratamento, prescrição de medicamentos, realização de exames e prestação de assistência direta à saúde. Utilizações para outros fins são vedadas.

O princípio da adequação determina que a coleta e o tratamento dos dados devem se limitar ao mínimo necessário para a concretização das finalidades pretendidas. Os dados não podem ser excessivos ou impertinentes considerando os propósitos informados para seu tratamento. Este princípio visa prevenir a construção desnecessária de grandes bancos de dados pessoais pelos agentes de tratamento. Portanto, esse princípio impede o excesso de dados coletados por agentes de saúde em relação à finalidade informada, coibindo a solicitação de grande número de informações desnecessárias ou impertinentes ao atendimento como perguntas sobre religião, vida sexual, opiniões políticas ou hábitos pessoais em um formulário médico de admissão hospitalar ou consulta ambulatorial.

O princípio da necessidade impõe a restrição dos dados pessoais tratados ao mínimo indispensável para a realização das finalidades. Mesmo que os dados sejam pertinentes e adequados para os propósitos informados, ainda assim deve ser feita uma análise de necessidade para coletar e tratar apenas dados estritamente necessários. Esse princípio tem como objetivo a redução máxima dos dados pessoais tratados. Nesse sentido, o princípio da adequação determina que a coleta e o tratamento dos dados devem se limitar ao mínimo necessário para a concretização das finalidades pretendidas. Os dados não podem ser

excessivos ou impertinentes considerando os propósitos informados para seu tratamento. Esse princípio visa prevenir a construção desnecessária de grandes bancos de dados pessoais pelos agentes de tratamento. Portanto, esse princípio impede o excesso de dados coletados por agentes de saúde em relação à finalidade informada, coibindo a solicitação de grande número de informações desnecessárias ou impertinentes ao atendimento como perguntas sobre religião, vida sexual, opiniões políticas ou hábitos pessoais em um formulário médico de admissão hospitalar ou consulta ambulatorial.

Já o princípio do livre acesso garante aos titulares o direito de consultar facilmente suas informações pessoais sob guarda dos agentes de tratamento a qualquer tempo. Os titulares podem solicitar cópias integrais dos dados armazenados para conferência das informações sobre si. Portanto, o princípio livre acesso faculta ao paciente obter cópias integrais de seu prontuário clínico armazenado por hospitais públicos ou privados, bem como de exames laboratoriais em posse de clínicas e laboratórios. Permitindo assim a supervisão ativa das informações coletadas e o controle social da qualidade dos registros.

O princípio da qualidade dos dados exige que todas informações pessoais tratadas sejam mantidas atualizadas, precisas e claras. Caso os dados estejam incompletos, inexatos ou desatualizados, o agente de tratamento deverá prontamente fazer as correções necessárias nos termos da lei. Esse princípio visa preservar a integridade e a fidedignidade das informações pessoais tratadas. A qualidade dos dados exige que os hospitais mantenham atualizados elementos críticos dos prontuários eletrônicos como tipo sanguíneo, histórico de alergias medicamentosas, prescrições atuais de medicamentos e dados cadastrais de contato dos pacientes internados ou atendidos em regime ambulatorial.

O princípio da transparência determina que os agentes de tratamento devem fornecer informações claras e acessíveis aos titulares sobre a realização do tratamento de seus dados pessoais. Isso inclui a utilização de linguagem simples e compreensível nos termos de consentimento e nas comunicações com o público em geral. O princípio da transparência requer que operadoras de planos privados de assistência à saúde informem de forma clara e acessível aos beneficiários dos planos quais dados coletam, para quais finalidades específicas os utilizam, por quanto tempo os armazenam, com quem são compartilhados e como podem ser acessados e corrigidos.

O princípio da segurança exige a adoção pelos agentes de tratamento de medidas técnicas e administrativas aptas a proteger os dados pessoais contra vários tipos de incidentes,

como acessos não autorizados, situações acidentais ou ilícitas de destruição, ou até mesmo desvios de finalidade não consentidos. Esse princípio demanda investimentos pelo Poder Público em sistemas seguros e rastreáveis de registro eletrônico e compartilhamento de dados de saúde, além de medidas rígidas de proteção das informações coletadas pelos órgãos do Sistema Único de Saúde contra incidentes e vazamentos.

O princípio da prevenção complementa o princípio da segurança ao determinar que os agentes de tratamento devem adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Isso inclui políticas internas de proteção de dados que visem antever e mitigar possíveis problemas antes que eles aconteçam. Por conseguinte, o princípio da prevenção determina que hospitais construam processos e políticas internas que antecipem e previnam problemas com o uso indevido ou incidentes com dados pessoais sensíveis de seus pacientes.

O princípio da não discriminação estabelece que os dados pessoais não podem ser utilizados para fins discriminatórios ilícitos ou abusivos contra os titulares dos dados. Por exemplo, não se deve usar indevidamente dados pessoais para segregar, distinguir ou excluir pessoas de alguns processos ou oportunidades. O princípio da não discriminação veda explicitamente o uso pelos profissionais, serviços e operadoras de saúde de informações pessoais sensíveis em prejuízo dos pacientes para distingui-los, segregá-los ou excluí-los ilicitamente de tratamentos e coberturas previstas contratualmente.

Por derradeiro, o princípio da responsabilização e prestação de contas determina que os agentes de tratamento possuem o dever de demonstrar aderência às normas de proteção de dados pessoais e às medidas técnicas exigidas pela lei. Eles devem ser capazes de comprovar que estão em conformidade com todos os princípios e regras aplicáveis ao tratamento de dados. O princípio da responsabilização cobra que operadoras de planos de saúde comprovem perante órgãos reguladores e fiscalizadores a adoção efetiva de todas as medidas técnicas, administrativas e organizacionais exigidas para a proteção integral de dados dos beneficiários dos planos.

3.2 DIREITOS DOS TITULARES DE DADOS PESSOAIS APLICADOS NA ÁREA DA SAÚDE

A LGPD confere aos titulares de dados pessoais diversos direitos, como o acesso às informações, a correção de dados incompletos ou incorretos, a eliminação de dados

desnecessários, entre outros. Na área da saúde, onde o acesso preciso e seguro a informações é vital, esses direitos ganham especial importância, demandando uma abordagem ética e técnica na implementação de processos que garantam o exercício desses direitos.

Nesse sentido, a LGPD estabelece um amplo rol de direitos conferidos aos titulares de dados pessoais em relação às suas informações pessoais tratadas pelas organizações públicas e privadas. Na seara da saúde, onde os dados pessoais e sensíveis dos pacientes são cotidianamente coletados e armazenados, a correta implementação desses direitos pelos agentes de tratamento no setor adquire especial relevância ética e prática, demandando a adoção de processos técnicos especificamente desenhados para viabilizar e facilitar o seu pleno exercício pelos pacientes.

Conforme estabelece o Capítulo III da Lei Geral de Proteção de Dados, os titulares de dados pessoais são assegurados de um conjunto substancial de prerrogativas e direitos oponíveis contra o controlador do tratamento de suas informações (BRASIL, 2018).

Nos termos do art. 18, o titular possui direito de obter do controlador, a qualquer tempo, mediante requisição formal, a confirmação da existência ou não de tratamento de seus dados pessoais. Tal direito permite ao indivíduo se certificar quanto a quais empresas e organizações públicas mantêm informações a seu respeito. Assim, o direito de confirmação e acesso, previstos no art. 18, permitem ao paciente verificar quais dados seus estão sendo tratados por hospitais, clínicas, planos de saúde e outros players do setor, solicitar cópias e conferir a qualidade dessas informações.

Desse modo, o art. 18 também garante o direito de acesso facilitado pelo titular aos seus próprios dados armazenados sob custódia do controlador (BRASIL, 2018). Possibilita assim que o indivíduo saiba exatamente quais dados lhe concernem estão sendo tratados, por quanto tempo e sob quais formas de uso.

Outrossim, o direito de correção de dados regulado pelo art. 19 empodera o titular a exigir a pronta retificação de informações pessoais desatualizadas, inexatas ou incompletas. Medida crucial para preservar a qualidade e utilidade dos dados na área da saúde. O direito de correção, disposto no art. 19, é crucial para garantir que erros ou desatualizações nos prontuários eletrônicos ou fichas de atendimento sejam prontamente sanados, assegurando a precisão das informações vitais para a prestação da assistência em saúde.

Por fim, o art. 20 prevê o direito de eliminação definitiva dos dados tratados a partir de consentimento do titular, ressalvadas as hipóteses legais de manutenção, como previsto no

art. 16. O titular pode assim “apagar” seus dados quando considerar que não possuem mais serventia ou desvirtuados de propósitos originais (BRASIL, 2018).

Por conseguinte, o disposto no art. 20, faculta ao paciente requerer que seus dados sejam totalmente apagados dos sistemas do controlador quando considere que não possuem mais serventia ou tenham seus propósitos originais desvirtuados.

Ressalte-se que há outros direitos relevantes tais como: o de revogação de consentimento, portabilidade e revisão de decisões automatizadas. Todos buscam, em conjunto, equilibrar a relação entre profissionais de saúde, operadoras e pacientes na era digital, resguardando autonomia e garantias aos cidadãos sobre seus dados mais sensíveis e íntimos.

3.3 APLICAÇÃO DA LGPD NA ÁREA DA SAÚDE

A LGPD impõe uma série de obrigações para as entidades que lidam com dados na área da saúde, pois considera esses dados como sensíveis, demandando um tratamento ético e seguro. Entre as obrigações legais, destacam-se a adoção de medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, vazamentos ou perdas, a realização de avaliações de impacto à privacidade para identificar e mitigar riscos, e a formalização de contratos específicos para o tratamento de dados, com cláusulas claras sobre as finalidades, os meios e os destinatários.

Outro aspecto importante é o respeito aos direitos dos titulares dos dados, que podem solicitar o acesso, a correção e a exclusão de suas informações, bem como a revogação do consentimento e a portabilidade dos dados. A adequada implementação da LGPD no cenário da saúde digital é essencial para elevar os padrões éticos e de transparência no uso dos dados dos pacientes.

Nesse sentido, a LGPD em seu artigo 11, inciso II, alínea “c” estabelece hipótese específica de tratamento legítimo de dados na área da saúde ao dispor que é dispensada a exigência do consentimento do titular dos dados quando for indispensável para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (BRASIL, 2018).

Essa previsão legal autoriza os agentes de tratamento no contexto do cuidado e assistência à saúde a realizarem o tratamento dos dados pessoais sensíveis de seus pacientes com fundamento na necessidade de proteção da saúde, independente de consentimento. No

entanto, mesmo nessas hipóteses, deverão ser rigorosamente observados todos os demais princípios e normas estabelecidos na LGPD.

A LGPD impõe ainda requisitos especiais para as operações de tratamento de dados pessoais na área da saúde. O artigo 46 estabelece que a comunicação ou o uso compartilhado de dados pessoais sensíveis entre agentes de tratamento somente poderá ocorrer para a proteção da vida ou da incolumidade física do titular ou de terceiro (BRASIL, 2018).

Outra exigência trazida no artigo 23 é a designação obrigatória de um encarregado específico de proteção de dados, que será o responsável interno por garantir a conformidade com a LGPD.

Além disso, poderá ser necessária a realização de relatórios formais de impacto à proteção de dados pessoais previstos no artigo 38, os quais deverão conter descrição dos fluxos de dados, avaliação dos riscos potenciais e medidas previstas para mitigação.

Portanto, o tratamento de dados pessoais sensíveis de pacientes impõe uma série de desafios e obrigações extras aos agentes de tratamento para adequada conformidade com a LGPD.

3.3.1 Dados Sensíveis na Área da Saúde

A LGPD categoriza alguns dados como sensíveis, incluindo informações relacionadas à saúde. Isso abrange dados sobre condições médicas, históricos clínicos, exames laboratoriais, entre outros. A gestão responsável dessas informações requer estratégias específicas para garantir a conformidade com a legislação, considerando a natureza especial desses dados e os potenciais riscos associados ao seu tratamento inadequado.

Nesse sentido, a LGPD em seu artigo 5o, inciso II traz a definição legal de dados pessoais sensíveis como sendo a informação relacionada à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando associado a uma pessoa natural.

No contexto específico da área da saúde, uma ampla variedade de dados pessoais dos pacientes pode ser enquadrada juridicamente no conceito amplo de dado sensível. Isso inclui, de forma não exaustiva, informações como: dados genéticos e biométricos, histórico médico pregresso, informações sobre doenças infectocontagiosas, resultados de todo tipo de exames

diagnósticos realizados, medicamentos prescritos e administrados, prognósticos médicos elaborados, relatórios de atendimentos, prontuários médicos, informações sobre condições psicológicas e psiquiátricas, registros de violência doméstica, abuso de substâncias químicas, maus tratos, dados sobre a sexualidade do paciente, entre outros.

Percebe-se, pois, que na área da saúde lida-se cotidianamente com um conjunto vasto e diversificado de informações pessoais que revelam detalhes íntimos sobre o estado físico ou mental das pessoas. Por conta de seu elevadíssimo potencial lesivo e discriminatório, tais dados são qualificados pelo ordenamento jurídico pátrio como “sensíveis”, carecendo por isso de um regime jurídico especial de tutela reforçada que imponha restrições, cuidados e técnicas especiais às entidades da área da saúde incumbidas de seu tratamento.

Nesse sentido, o tratamento dos referidos dados pessoais sensíveis na seara da saúde somente será considerado legítimo nas hipóteses taxativamente previstas no artigo 11 da LGPD. Mais especificamente quando: (i) o titular ou seu responsável legal consentir de forma específica e destacada para finalidades específicas; ou (ii) for indispensável para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde ou por entidades sanitárias.

Mesmo nessas hipóteses de tratamento legítimo, deverão ser rigorosamente observados pelos agentes de tratamento os demais princípios e normas gerais estabelecidos na LGPD e nas suas regulamentações setoriais. Sobretudo no que diz respeito à aplicação de medidas técnicas robustas de segurança, à realização de análises prévias dos impactos do tratamento, ao respeito integral aos direitos dos titulares e à adoção de padrões éticos rígidos de transparência e finalidade na coleta e processamento desse tipo especial de dados.

3.3.2 Aplicação da LGPD nos Planos de Saúde

As entidades gestoras de planos de saúde, enquanto detentoras de extensos conjuntos de informações pessoais dos seus beneficiários, encontram-se sujeitas a exigências específicas estabelecidas pela Lei Geral de Proteção de Dados (LGPD).

Uma das principais obrigações diz respeito à necessidade de realização adequada dos procedimentos de anonimização e/ou pseudonimização de dados. Isso significa blindar a identificação dos respectivos titulares e mitigar os riscos decorrentes do tratamento, por meio da dissociação ou do mascaramento das informações pessoais.

Outro ponto crucial é a implementação efetiva de medidas técnicas robustas de segurança da informação, incluindo ferramentas como criptografia, controle rígido de acessos, registro de logs, testes periódicos de vulnerabilidade, treinamento de pessoal, políticas e normativas internas, ferramentas de detecção de intrusão e etc. Tais providências buscam proteger os dados contra incidentes como vazamentos e acessos não autorizados.

Além disso, a LGPD determina a designação formal de agentes específicos, internamente nas operadoras de planos, encarregados de garantir a conformidade da empresa com a legislação. Esses profissionais atuarão como canais entre a organização e os órgãos de regulação, assegurando a correta aplicação das normas.

Outra exigência relevante se refere à elaboração de relatórios formais descritivos dos processos de tratamento e avaliações concretas dos impactos sobre a privacidade. Tais documentos devem evidenciar os fluxos de informações manipulados internamente, mapear os potenciais riscos existentes e delinear as providências previstas para sua mitigação, seguindo os padrões técnicos e controles aplicáveis.

Por fim, os planos de saúde precisarão rever seus formulários e bases contratuais para registrar, de forma clara e acessível aos usuários, detalhes sobre quais dados pessoais são coletados, os propósitos de uso, tempo de conservação, compartilhamentos realizados e medidas de segurança aplicadas à sua custódia. Isso visa garantir a transparência e o pleno exercício de direitos pelos beneficiários.

Compreender e incorporar tais diretrizes erige-se como fundamental para que os planos de saúde alcancem a conformidade com a LGPD, resguardando a privacidade e a segurança das informações pessoais sob sua custódia.

3.3.3 Potencial da LGPD para Estimular Inovações Éticas no Uso de Dados Médicos

Muito além de representar um conjunto de obrigações e adequações necessárias para evitar penalidades dos órgãos fiscalizadores, a Lei Geral de Proteção de Dados (LGPD) carrega consigo valiosas oportunidades para fomentar inovações éticas no uso dos dados médicos dos pacientes. Isso porque, ao estabelecer balizas rígidas para o tratamento consentido dessas informações sensíveis, a legislação termina por estimular os players da saúde a buscarem alternativas criativas e seguras de manuseio dos dados que estejam alinhadas aos preceitos éticos.

Nesse contexto, abre-se espaço para um prolífico campo de pesquisa e desenvolvimento voltado à concepção de políticas, processos e soluções tecnológicas que maximizem o aproveitamento dos dados médicos ao mesmo tempo em que salvaguardam sua proteção integral, em consonância com os princípios e objetivos trazidos pelo normativo.

Assim, a LGPD fortalece sua posição como vetor de transformação cultural e operacional, podendo estimular ideias disruptivas para o setor. Um exemplo é o uso de técnicas de inteligência artificial tanto para acelerar diagnósticos e tratamentos quanto para aprimorar a qualidade da anonimização dos dados sensíveis. Outra possibilidade é a adoção em larga escala de blockchain e registros distribuídos para evitar a centralização excessiva das informações médicas por um único agente controlador.

Até medidas aparentemente simples, como a implementação de interfaces amigáveis para gerenciamento do consentimento dos pacientes ou a disponibilização de painéis individuais de controle de dados, podem ser valiosos desdobramentos das obrigações trazidas pela LGPD no sentido de viabilizar os direitos dos titulares.

Portanto, mais do que um conjunto de despesas e restrições, a conformidade legal sob a LGPD pode ser encarada pelo setor da saúde como uma oportunidade de revisão ética dos atuais modelos de uso de dados pessoais. Isso permitirá trilhar caminho em direção a um ecossistema verdadeiramente responsável e inovador no tratamento das informações sensíveis dos pacientes.

4 OS DESAFIOS DA IMPLEMENTAÇÃO DA LGPD NAS INSTITUIÇÕES DE SAÚDE

A aplicação da Lei Geral de Proteção de Dados (LGPD) em Instituições de Saúde traz consigo uma série de desafios, levando em conta o ambiente delicado e complexo em que essas entidades atuam. Um dos principais obstáculos é a necessidade de ajustar os processos internos para assegurar a conformidade com as normas legais.

Um dos principais entraves é a coleta e o manuseio de dados pessoais sensíveis, que são intrínsecos às atividades das Instituições de Saúde. A LGPD requer uma atenção especial na gestão desses dados, impondo medidas de segurança robustas e a definição de protocolos transparentes para o acesso e a troca de informações entre os profissionais de saúde e os departamentos administrativos.

Adicionalmente, a sensibilização e a formação dos colaboradores são desafios importantes. É essencial que todos os membros da equipe estejam informados sobre as regras da LGPD e estejam preparados para tratar as informações pessoais de forma ética e legal. A transformação cultural e a instauração de uma cultura organizacional focada na privacidade e segurança dos dados são processos que exigem tempo e investimento.

A LGPD também ressalta a importância da transparência no manuseio dos dados, incluindo a comunicação efetiva com os pacientes sobre como suas informações serão usadas. Este aspecto implica a revisão e atualização de contratos e termos de consentimento, bem como a implementação de mecanismos que permitam aos indivíduos exercerem seus direitos, como o acesso, correção e exclusão de dados.

Um desafio adicional está ligado à conformidade com padrões técnicos e regulatórios específicos da área de saúde. A harmonização da LGPD com normas já existentes, como as que se referem à segurança da informação em saúde, requer uma estratégia metódica e a cooperação entre os departamentos jurídico e de tecnologia da informação.

Em suma, a aplicação da LGPD nas Instituições de Saúde exige uma estratégia completa, que inclui revisão de processos, treinamento de pessoal, ajuste de tecnologias e a formação de uma cultura organizacional que priorize a privacidade e a segurança dos dados. O êxito nessa tarefa dependerá da capacidade das instituições em superar esses desafios de forma eficaz e ética.

5 A LGPD COMO INDUTORA DE UM NOVO MODELO DE NEGÓCIOS NA SAÚDE

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) provoca um ponto de inflexão no setor da saúde, demandando uma profunda revisão dos modelos de negócios vigentes. Mais do que simples conformidade legal, a nova legislação sobre privacidade impõe uma mudança de mentalidade e de cultura dentro das organizações de saúde.

Isso porque a LGPD eleva o cuidado com os dados do paciente a um patamar muito mais estratégico para qualquer player que deseje se estabelecer no setor da saúde atual. Não basta apenas oferecer um bom serviço ou ter tecnologia de ponta. É preciso construir uma

proposta de valor orientada também aos legítimos interesses dos usuários em resguardar sua privacidade e exercer controle sobre as informações mais sensíveis.

Portanto, a adequação à LGPD passa a funcionar como um catalisador para acelerar a incorporação de atributos como transparência, segurança e controle do paciente nos modelos de negócios das healthtechs, startups e demais agentes. Essas características deixam de ser meros diferenciais para se tornarem condições indispensáveis à sobrevivência e crescimento.

Um exemplo são os aplicativos e dispositivos vestíveis focados em saúde e bem-estar, que coletam enormes volumes de dados pessoais. A conformidade com a LGPD obriga essas soluções a serem desenhadas já com privacidade desde a concepção, viabilizando aos usuários facilidades como gerenciamento granular de consentimento, além de garantir a portabilidade, eliminação e segurança.

Portanto, a LGPD impulsiona mudanças culturais e estratégicas profundas, reposicionando a privacidade do paciente como elemento central na construção e entrega de valor neste novo ciclo do mercado da saúde. Mais que um ônus, a proteção ética de dados surge como uma oportunidade de inovar com soluções legítimas e socialmente responsáveis.

6 DISCUSSÃO

6.1 IMPACTO DA LGPD NOS PLANOS DE SAÚDE E O USO DE DADOS

A implementação da LGPD provoca uma redefinição significativa na operação dos planos de saúde, influenciando diretamente as práticas de coleta, processamento e utilização de dados pessoais. O enfoque em princípios como transparência e consentimento explícito traz à tona a necessidade de rever políticas, termos contratuais e maneiras de se relacionar com o beneficiário.

Essa reconfiguração implica investir em governança sólida, ferramentas seguras de gestão de consentimento, anonimização efetiva de dados quando aplicável e controles rígidos de acesso à informação. O estabelecimento de canais éticos e lícitos de obtenção e

compartilhamento de dados pessoais passa a ser crucial para construir vínculos de confiança e sustentar as operações.

Portanto, uma relação transparente e alinhada aos padrões da LGPD não é opcional para os planos de saúde, configurando-se como requisito legal e essencial sob a perspectiva da legitimidade social de longo prazo. A conformidade plena amplia a segurança jurídica e opera como diferencial competitivo para as empresas comprometidas.

Assim, independentemente dos obstáculos, é incontestável que a LGPD produz efeitos profundos no setor de saúde suplementar. Mais do que simples adequação normativa, a lei fomenta e acelera uma transformação cultural com foco na integridade e ética no tratamento dos dados dos beneficiários

6.2 DESAFIOS E OPORTUNIDADES PARA APRIMORAR A PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

A implementação da LGPD nos planos de saúde não está isenta de desafios. Um dos principais obstáculos diz respeito à complexidade dos dados de saúde, que envolvem informações sensíveis e interconectadas entre diversos atores do setor. Isso demanda uma abordagem cautelosa e estratégias customizadas de governança e segurança da informação.

Outra questão central está relacionada aos altos investimentos necessários para adequação tecnológica, considerando a necessidade de revisar arquiteturas de TI, adquirir novas ferramentas de controle de acesso e proteção de dados, além de lidar com legados e sistemas ultrapassados.

Soma-se a isso o desafio cultural representado pela resistência organizacional e falta de experiência com requisitos mais rígidos de conformidade. A mudança de mentalidade quanto à privacidade como um valor fundamental não é algo trivial e pode enfrentar barreiras.

Por outro lado, a conformidade com a LGPD também apresenta oportunidades relevantes para os planos de saúde. A chance de construir relações de confiança mais sólidas com os beneficiários, por meio de práticas transparentes e éticas de gestão de dados, é um potencial significativo.

Além disso, a maior segurança proporcionada pelos controles técnicos aprimorados contribui para mitigação de uma variedade crescente de ameaças cibernéticas. O estímulo para adoção de tecnologias inovadoras relacionadas à proteção da privacidade, como inteligência artificial e blockchain, pode impulsionar a eficiência.

As inovações tecnológicas como inteligência artificial (IA) e blockchain têm o potencial de melhorar significativamente a eficiência dos processos em planos de saúde e operadoras do setor.

A IA pode ser aplicada na análise preditiva de grandes conjuntos de dados dos beneficiários, identificando padrões de utilização e perfis de risco. Isso permite que a operadora personalize melhor a experiência do usuário, antecipe a necessidade de intervenções preventivas e gerencie de forma proativa os custos assistenciais.

Já o blockchain propicia automatizar processos internos antes complexos, como a conferência de faturas hospitalares, a auditoria de contas médicas e o cruzamento de informações entre prestadores. A descentralização e imutabilidade dos registros trazem mais transparência e controle.

Além disso, essa tecnologia viabiliza compartilhar dados entre operadoras e prestadores de forma segura, facilitando interoperações. Isso melhora o atendimento ao permitir ao médico acessar o histórico completo do paciente com rapidez e com as permissões corretas.

Portanto, essas inovações podem gerar ganhos de produtividade nos planos de saúde, reduzindo burocracias, aprimorando análises, potencializando a prevenção e fornecendo ferramentas avançadas de segurança da informação. A inteligência artificial e o blockchain mostram-se como aliados valiosos na busca por mais eficiência.

Por conseguinte, apesar dos obstáculos, o alinhamento com a LGPD fortalece o compromisso dos planos de saúde com seus usuários, trazendo benefícios mútuos por meio de práticas lícitas, éticas e socialmente responsáveis de uso de dados.

6.3 RECOMENDAÇÕES PARA A CONFORMIDADE COM A LGPD NOS PLANOS DE SAÚDE

Tendo como pano de fundo os desafios e oportunidades analisados, são propostas algumas recomendações práticas para que os planos de saúde garantam sua conformidade com a LGPD:

Inicialmente, é essencial a formalização e divulgação ampla de políticas claras e detalhadas de privacidade e proteção de dados pessoais. Tais documentos devem informar, em linguagem simples e acessível, quais dados são coletados, suas finalidades, tempo de retenção, formas de compartilhamento, direitos dos titulares e medidas técnicas implementadas.

Além disso, mostra-se imprescindível investir na realização contínua de treinamentos e capacitações sobre segurança da informação e privacidade para os colaboradores. A conscientização quanto às responsabilidades e boas práticas no tratamento de dados deve se tornar parte indivisível da cultura organizacional.

Outro ponto relevante refere-se à incorporação de avaliações regulares de impacto à proteção de dados pessoais. Tais análises permitem mapear riscos concretos, verificar a efetividade dos controles atuais e identificar necessidades de adaptação.

Por fim, ressalta-se a importância da cooperação próxima da alta direção com profissionais especializados nas áreas jurídica e de segurança da informação. Essa interação qualificada fortalece a infraestrutura de governança em privacidade e viabiliza respostas ágeis aos desafios e incidentes.

A observância dedicada e proativa de tais recomendações eleva as chances de sucesso dos planos de saúde em alcançar os requisitos da LGPD. Mais que uma resposta pontual, a privacidade deve ser encarada como um compromisso contínuo.

7 CONSIDERAÇÕES FINAIS

O objetivo do presente trabalho de analisar os impactos, obstáculos, oportunidades e recomendações relacionados à implementação da LGPD na área da saúde, sobretudo nos planos de saúde, foi plenamente alcançado.

Através da revisão bibliográfica, foi possível identificar os principais desafios enfrentados pelas organizações de saúde, assim como perspectivas positivas e caminhos para uma adequação efetiva à legislação.

Além disso, a pergunta sobre quais são os obstáculos e potenciais benefícios da aplicação da LGPD no contexto da saúde foi respondida de forma abrangente. As análises evidenciaram questões gerenciais, éticas e tecnológicas envolvidas nesse processo de adequação.

A metodologia de pesquisa baseada em fontes secundárias mostrou-se apropriada e viável para coletar visões diversas de especialistas sobre o estado da arte do tema. As referências consultadas, bem como a análise crítica do material, permitiram conclusões consistentes.

Dentre as dificuldades para realização do estudo, destaca-se a ainda limitada literatura científica específica tratando da intersecção entre a proteção de dados e o setor da saúde. Isso restringiu em certa medida avaliações quantitativas dos impactos.

Como sugestões para trabalhos futuros, sugere-se a realização de pesquisas de campo, como entrevistas com gestores de saúde, para quantificar os desafios e benefícios observados na prática com a implementação da LGPD. Além disso, é necessário que haja estudos que possam analisar a evolução desse cenário.

8 REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm Acesso em: 1 set. 2023.

BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. Acesso em: 22 nov. 2023.

Blog-HDPO. Os 5 maiores desafios para implantar a LGPD nas instituições de saúde. Disponível em: <https://hdpo.com.br/os-5-maiores-desafios-para-implantar-a-lgpd-nas-instituicoes-de-saude/>. Acesso em: 20 nov. 2023.

BOTELHO M. C., CAMARGO E. P. A. A aplicação da lei geral de proteção de dados na saúde. R. Dir. sanit., São Paulo v.21, e-0021, 2021. Disponível em: <https://www.revistas.usp.br/rdisan/article/view/168023/178494>. Acesso em 22 de nov. 2023.

CAMPOS, L. V. O que são Fake News? Brasil Escola. Disponível em: <https://brasilecola.uol.com.br/curiosidades/o-que-sao-fake-news.htm>. Acesso em: 17 nov. 2023.

CUNHA, C. Tecnologia: o que é a 4ª revolução industrial? UOL Vestibular. Disponível em: <https://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/tecnologia-o-que-e-a-4-revolucao-industrial.html>. Acesso em: 17 nov. 2023.

FEIGELSON, B.; SIQUEIRA, A. H. A. (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019. Acesso em: 21 nov. 2023.

FRANCO, P. A. Lei Geral de Proteção de Dados Pessoais comentada. Leme: Imperium Comunicação e Editora, 2020. Acesso em: 20 nov. 2023.

LGPD na saúde: como deve ser o consentimento para uso dos dados. Blog Aurum. Disponível em: <https://www.aurum.com.br/blog/lgpd-na-saude/#como-deve-ser-o-consentimento-para-uso-dos-dados>. Acesso em: 21 nov. 2023.

MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Acesso em: 22 nov. 2023.

PERASSO, V. O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas. BBC News. Disponível em:
<https://www.bbc.com/portuguese/geral-37658309>. Acesso em: 20 nov. 2023

Revolução Industrial: Terceira Revolução Industrial. Brasil Escola. Disponível em:
<https://brasilescola.uol.com.br/geografia/terceira-revolucao-industrial.htm>. Acesso em 20 nov. 2023.

SARNICK, Stefanie. Medicina - Os desafios da implementação da LGPD na área da Saúde. Disponível em: <https://medicinasa.com.br/desafios-implementacao-lgpd/>. Acesso em: 23 nov. 2023.

SOUZA, Carlos. LGPD - LGPD e os desafios no setor da saúde. Disponível em:
<https://fbh.com.br/lgpd-e-os-desafios-no-setor-da-saude/>.
Acesso em: 22 nov. 2023.