CONSENTIMENTO NO DIREITO DA SAÚDE NO ÂMBITO DOS ATENDIMENTOS MÉDICOS E NO TRATAMENTO/DIVULGAÇÃO DOS DADOS DO PACIENTE NO CONTEXTO DA LGPD

Consent in health law within the scope of medical care and in the treatment/disclosure of patient's data within the context of the general personal data protection law

Cynthia Schultz de S. Thiago[1]

Resumo: Este artigo pretende abordar o conteúdo do consentimento do usuário dos serviços de saúde, na sua ramificação: no âmbito do atendimento médico e no tratamento dos dados dos pacientes. Trata-se de assunto atual e relevante, em foco pelas novidades trazidas com a vigência da LGPD e da necessidade da proteção de dados sensíveis que engloba a saúde do seu titular, diante da magnitude dos danos que podem ser gerados por eventuais usos indevidos, cuja consequência é provável que se repercuta no Judiciário, em ações indenizatórias ajuizadas por pacientes que tenham sido vítimas de erros no consentimento, tanto nos atendimentos, quanto no uso e tratamento de dados.

Palavras Chave: Direito da saúde, Consentimento no âmbito dos atendimentos médicos, Consentimento para dados de saúde, Pivacidade, Divulgação de dados sensíveis dos pacientes, LGPD.

Abstract: This article intends to outline the content of the health services user's consent, in its bifurcation: in the scope

[1] Graduada na Faculdade de Administração em Coburg/Bayern/Alemanha. Graduada em Direito na UNISOCIESC. Advogada. Área de atuação: Direito Previdenciário. O presente artigo refere-se ao trabalho de conclusão de curso da ESMAFESC/UNIVALI da Pós-graduação em nível de especialização em Direito da Seguridade Social com Enfoque na Reforma e no Processo Previdenciário. Coordenação do Curso: Desembargador Federal Dr. Paulo Afonso Brum Vaz. Professor Orientador: Juíz Federal Dr. Oscar Valente Cardoso.

of medical care and in the processing of patient data. This is a current and relevant theme, evidenced by the recent validity of the LGPD and the importance of protecting sensitive data that involves the health of its holder, given the severity of the damage that can be caused by possible misuse, the repercussion of which may still be felt in the Courts, in indemnity claims that maybe proposed by patients who have suffered damage due to failures in consent, on care, or in the data processing.

Keywords: Health law, informed consent, consent for health data, privacy, disclosure of sensitive patient data, LGPD.

SUMÁRIO: Introdução. **1.** O consentimento do paciente usuário dos serviços de saúde no âmbito da LGPD. **1.1.** Classificação dos dados no âmbito da LGPD. **2.** Proteção de dados na saúde digital: contextualização e desafios regulatórios. **3.** Compartilhamento e proteção de dados na era digital. **4.** As informações dos pacientes obtidas pelos serviços de saúde e os cuidados necessários no tratamento de dados sensíveis pós vigência da LGPD. **5.** Vulnerabilidade do paciente/autor. Conclusão. Referências.

Introdução

A Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), com vigência a partir de 18/09/2020, motivou a necessidade de adoção de medidas protetivas. Extrai-se da referida lei o consentimento do titular como uma das possibilidades de tratamento[2] de dados pessoais, sensíveis ou não, sendo determinante para conferir licitude à conduta de quem presta esta atividade.

O Direito da Saúde, mais precisamente o Direito Médico, já adota o consentimento do paciente ao tratamento ou ao atendimento especializado.

[2] Segundo o art. 5º, X, da LGPD, considera-se 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".

Entretanto, com a LGPD, faz-se necessário utilizar dois tipos de consentimento do paciente: o consentimento ao atendimento e o consentimento para o uso de informações pessoais.

Os problemas da pesquisa são os desafios regulatórios da saúde digital no Brasil; os cuidados que devem ser adotados ao empregar dados sensíveis em saúde; as informações dos pacientes obtidas pelos serviços de saúde e os cuidados necessários no tratamento de dados pós vigência da LGPD; bem como a vulnerabilidade do paciente/autor.

Estabelecem-se como hipóteses: A LGPD é um importante avanço para desenvolver e organizar um ambiente regulatório claro e coordenado para as tecnologias aplicadas à saúde; a fim de contornar as limitações de tratamento dos dados, uma possibilidade seria recorrer à técnicas de anonimização de dados, retirando o vínculo da informação ao seu titular, de forma que as informações possam compor o banco de dados a ser trabalhado sem identificar seus titulares.

Esclareça-se que este artigo abordará especificamente o consentimento na vigência da LGPD quanto aos dados sensíveis de saúde de pacientes, não anonimizados, cujo atendimento dependa de consentimento.

O objetivo é uma melhor compreensão dos desafios que estão impostos à sociedade contemporânea no que se refere à necessária regulação da saúde para sua plena efetivação.

Quanto à Metodologia utilizar-se-á o método dedutivo, e, na técnica de pesquisa, enfatiza-se a coleta doutrinária, com pesquisa bibliográfica e documental.

1. O consentimento do paciente usuário dos serviços de saúde no âmbito da LGPD

Nas palavras de (SOARES, 2021 apud BIONI, 2019), a LGPD foi instituída para atender a duas finalidades, quais sejam, a de proteger os direitos fundamentais de liberdade e de privacidade e a de preservar “o livre desenvolvimento da personalidade” do titular (art. 1º), pois os dados pessoais estão

inseridos no âmbito dos direitos de personalidade, por serem projeção, extensão ou dimensão do seu titular.

Soares (2021, p. 4) esclarece que a proteção de dados vem sendo reconhecida como um direito fundamental autônomo:

> Tanto na dimensão digital do mundo, quanto na não digital, dados podem ser tratados, e o âmbito de aplicação da LGPD reside no tratamento de dados: (a) coletados no território nacional; (b) realizado no território nacional; (c) de titulares localizados no território nacional ou (c) que almeje "a oferta ou o fornecimento de bens ou serviços", e essas atividades podem ser levadas a efeito por pessoa natural ou jurídica, de direito público ou privado com ou sem sede no país onde estejam os dados (art. 3º).

Observa-se que a palavra tratamento é a base para atrair a incidência da LGPD, cujo amplo significado está previsto no art. 5º, inc. X, segundo o qual este abrange qualquer 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", a ser realizada com transparência e retidão.

Exatamente por conta da proteção reconhecida aos dados pessoais é que a LGPD, em seu art. 2º, cita que o amparo legal está assentado nos direitos humanos do titular, especialmente na autodeterminação e na liberdade informativa, comunicativa e de opinião, além da inviolabilidade da intimidade, da honra e da imagem, também expressamente mencionado no texto do art. 5º, inc. X, da CF/88.

O consentimento é uma das bases legais à legitimação do tratamento de dados digitais ou tradicionais (físicos). O conceito de consentimento consta no art. 5º da LGPD, tido como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (inc. XII) e legítima.

O art. 11, I, da LGPD regula as bases legais sobre os dados sensíveis. Assim, o art. 11 da LGPD exige, em seu inciso I, a emissão do

consentimento do paciente de “forma específica e destacada para finalidades específicas”, ou, se o titular estiver incapacitado para consentir, será substituído pela autorização do responsável (terceiros) a qual, de igual modo, também deve ser específica.

O consentimento ou a autorização do responsável delimitará o tratamento dos dados sensíveis, quanto ao seu conteúdo e alcance, não podendo ultrapassar ao que fora consentido ou autorizado. O art. 11, II, da LGPD traz as exceções em que o consentimento é dispensado. Será admissível, por exemplo, a dispensa do consentimento em situações de emergência.

No que diz respeito aos dados sensíveis de crianças e adolescentes, deve-se associar ao disposto no art. 14 da LGPD, que dispõe como condição de tratamento que esta atividade se suceda no melhor interesse e proteção desse grupo. Conforme o texto da lei, o consentimento pode ser fornecido diretamente pelo adolescente, mas o tratamento de dados de crianças depende da autorização de um dos pais ou, na ausência destes, do responsável legal, cujo controle de autoria demanda o emprego de diligência por parte do tomador dos dados, que, para este fim, deve utilizar as tecnologias disponíveis (art. 14, § 5º LGPD).

Dispensar-se-á o consentimento de crianças “para a sua proteção” ou “quando a coleta for necessária para contatar os pais ou o responsável legal”, desde que ocorra uma única vez (por necessidade de contato) e sem que ocorra o armazenamento dos dados ou o repasse indevido a terceiros, assim como será dispensado o consentimento de adolescentes para a proteção da vida ou da incolumidade física destes ou de terceiro, na forma do art. 11, inc. II, alínea *e;* e do art. 14, § 3º, da LGPD.

Soares (2021) reforça que mesmo no tratamento de dados sensíveis nas hipóteses que dispensam o consentimento, permanece o dever de informar aos pacientes, usuários dos serviços de saúde, o qual decorre da incidência do princípio da boa-fé objetiva.

Quanto à forma do consentimento ou da autorização de terceiros, o art. 8º da LGPD dispõe que a mesma é livre, ou seja, permite tanto a sua tomada por escrito (em cláusula destacada) quanto “por outro meio que demonstre a manifestação de vontade do titular”, cabendo ao controlador o ônus da prova quanto à conformidade da sua obtenção.

Soares (2021) alerta que o tratamento se limitará ao que foi consentido, delimitado e anuído, sendo vedado, por exemplo, coletar um dado justificando para o paciente que a informação é necessária para identificação de doença e, em seguida, utilizar essa mesma informação para fins de publicidade direcionada, sob pena de violação ao princípio da finalidade; ou ainda, repassar às farmácias conveniadas os dados para que estas façam propaganda medicamentosa direcionada; ou o médico de uma determinada especialidade passar a sua lista de pacientes para que um laboratório farmacêutico faça propaganda dos seus produtos.

O consentimento jamais pode ser separado da licitude da conduta dos agentes de tratamento, com finalidade específica e transparente, além da efetiva possibilidade de escolha pessoal. Nesse sentido argumenta Soares (2021, p. 11):

> Não é possível afirmar que haja um consentimento válido se a decisão permissiva do titular não esteve baseada em informações corretas, completas e eficientes no mínimo quanto ao tipo de dado coletado, a finalidade, o tempo de uso e com quem esse dado será compartilhado, ou que não seja dado ao mesmo o direito de negar o emprego de determinadas ferramentas, condicionado ao consentimento de uso dos seus dados sensíveis, desde que isso não seja essencial ao próprio cumprimento da obrigação da outra parte. Diante desse contexto, afirma-se que o titular deve ter a real oportunidade de consentir ou de dissentir quando o tratamento dos seus dados depender da sua vontade (que não seja hipótese de tratamento independentemente de consentimento).

A par disso, há muitas condutas que são permitidas e outras não. Alguns exemplos de práticas não permitidas são a exposição do nome dos pacientes em painéis de chamadas, quando o correto é atribuir caracteres não identificáveis; circulação de documentação médica de pacientes em grupos de profissionais de saúde, exceto se estiverem anonimizadas e com o objetivo de abordar questões técnicas como o diagnóstico ou parecer, visto que aplicativos de mensagens não são seguros para a circulação de dados pessoais sensíveis,

sendo portanto desaconselhável pelo alto risco envolvido. Na pandemia do coronavírus, foi noticiada, por exemplo, a transação penal em processo crime contra um farmacêutico que divulgou, em grupo de Whatsapp, a receita médica (autoprescrição) de uma personalidade pública em tratamento para a COVID-19.[3] A circulação de imagens de exames de pacientes tampouco deve acontecer sem o devido consentimento.

Soares (2021) reforça a importância de salvaguardar os relatórios de atendimento que são documentos, como a ficha do paciente ou o prontuário, devendo ser arquivados com segurança máxima independentemente da anuência do paciente. A Lei nº 13.787/2018 prenuncia o dever de guarda do prontuário pelo prazo de vinte anos. O histórico clínico, embora não haja prazo legal de guarda, deve ser salvo enquanto existir a possibilidade de questionamento quanto à correção da conduta médica no âmbito administrativo ou judicial.

Soares (2021, p. 15) explica que:

> No consentimento, o paciente previamente admite que tolerará uma intervenção ou tratamento a ser efetivado em benefício dos seus interesses existenciais psicofísicos, delimita os seus contornos ou assentirá ao que lhe for proposto.

O consentimento é a legitimação, bem como a delimitação da atividade médica.

O termo de consentimento é de suma relevância para que o médico comprove (com presunção relativa) que repassou ao paciente as orientações e cuidados necessários sobre como proceder para o melhor resultado do procedimento, e serve para eximir o médico da responsabilidade pelo eventual não alcance desse resultado, caso alguma intercorrência tenha sido causada

---

[3] “Farmacêutico é condenado por vazar receita de cloroquina de David Uip. O magistrado fixou o profissional ao pagamento de pena crime em R$ 11 mil. O juiz Fabricio Reali Zia, do JEC da Barra Funda/SP, condenou o gerente de laboratório que vazou a receita de cloroquina do médico infectologista David Uip. O magistrado fixou o profissional ao pagamento de pena crime em R$ 11 mil”.
Migalhas.13 mar. 2021.Disponível em: https://www.migalhas.com.br/quentes/341731/farmaceutico-e-condenado-por-vazar-receita-de-cloroquina-dedavid-uip, acesso em 24 jun. 2023.

pela falta de cumprimento das recomendações que estejam no âmbito dos ônus que competem ao paciente cumprir ou que envolva risco relativo ao próprio procedimento ou tratamento.

O ônus probatório quanto ao consentimento recai sobre quem trata os dados, por isso, o risco da não comprovação pode ser um fator de desestímulo à adoção de outra modalidade de consentimento, que não seja de forma escrita.

1.1. Classificação dos dados no âmbito da LGPD

A classificação dos dados pela LGPD se divide em dados não sensíveis e dados sensíveis, sendo ambos afetados e resguardados pela lei, diferenciando apenas na medida da proteção, sendo que os dados sensíveis acarretam em maior proteção.

Os dados sensíveis referentes à saúde, que interessam ao presente estudo, estão contemplados no art. 5º da LGPD. Nas palavras de Soares (2021), os dados sensíveis vinculam à esfera nuclear da pessoa humana, sendo importantes e basilares ao livre desenvolvimento e exercício da personalidade do titular e, ao mesmo tempo, mais suscetíveis a elevados danos, se violados. Tratam-se de dados essenciais, pois como observa Soares (2021), caso sejam afrontados, atinge-se um dos mais altos graus de ofensa aos direitos fundamentais e aos direitos de personalidade a exemplo dos dados pessoais de uma pessoa com HIV, cujo vazamento indevido poderá trazer-lhe grandes danos, principalmente oriundos de discriminação em virtude do estigma social que engloba esse vírus. Ainda, os dados analisados podem levar a informações sensíveis, como a nota fiscal da farmácia que contenha o nome completo, endereço e CPF, bem como os medicamentos adquiridos, por intermédio do qual é possível identificar a doença que acomete esse indivíduo; aplicativos contadores de passos ou batimentos cardíacos e que controlam a pressão arterial, a indicar se o indivíduo sofre de alguma doença cardíaca, por exemplo; as buscas de um paciente em *sites* de marcações de consultas, notadamente quanto a especialidade médica agendada ou de tratamentos realizados.

Conforme analisa Soares (2021), na violação de dados sensíveis, há o agravamento da lesividade decorrente da ofensa, quando comparada àquela que afronta dados não sensíveis, agravado pela submissão relativamente inevitável do titular, tendo em vista a evolução tecnológica atual e a imprescindibilidade de uso de dados sensíveis em benefício próprio, notoriamente no setor da saúde, visto que não se faz um diagnóstico ou se emite um prognóstico da saúde de um paciente sem que sejam coletadas e analisadas informações e dados.

A tecnologia permite e cada vez mais possibilitará, a formação de uma gigantesca memória de atuação em rede, bem como a interconexão de dados e de informações, infinitamente maior que a capacidade humana. Além disso, viabilizará uma dependência cada vez mais intensa e extensa quanto ao uso de ferramentas eletrônicas pois, no futuro próximo, os dados de pacientes serão praticamente todos mantidos no ambiente digital conclui Soares (2021).

2. Proteção de dados na saúde digital: contextualização e desafios regulatórios

O século XXI é marcado cada vez mais pelas transformações trazidas pela tecnologia digital. A internet, o aumento das bases de dados, automatização, inteligência artificial, alta conectividade, redes sociais digitais globais, grandes corporações digitais, etc. Todas essas ferramentas da vida moderna digital estão revolucionando a sociedade e inclusive o setor de saúde. Uma quantidade crescente de serviços de saúde que se utilizam destes bancos de dados e tecnologias está sendo lançada nos sistemas de saúde do mundo todo.

> Para além dos benefícios enormes que estas inovações trazem, já está evidenciado que estes produtos, se não fiscalizados e desenvolvidos com ética e responsabilidade, podem produzir danos físicos, psicológicos e morais nos seus usuários.
>
> Compreender os desafios regulatórios impostos à sociedade nesse momento mostra-se estratégico para que possamos usufruir do que estas inovações podem trazer de melhor, sem, contudo, expor os indivíduos e a sociedade como um todo a riscos desnecessários e, até, letais.[4]

[4] AITH, Fernando; DALLARI, Analluza Bolivar. LGPD na Saúde Digital. São Paulo. Editora Thomson Reuters, 2022. P. 42.

A LGPD estabelece regras para o tratamento de dados por IA, como requisitos e procedimentos para categorias específicas de dados; autorizações ou vedações excepcionais para determinadas finalidades de uso; e padrões técnicos de coleta, armazenamento e compartilhamento, entre outras. O marco sugere, ainda, a adoção de boas práticas e governança por controladores e operadores de dados, para que estes estabeleçam seus próprios mecanismos internos de controle de riscos.[5]

Antes de mais nada, a lei determina níveis crescentes de restrições para o tratamento de dados, de acordo com o grau de exposição de seus titulares (dados anonimizados, pessoais e pessoais sensíveis). Dados são considerados pessoais quando seus titulares são identificados, ou identificáveis por meios técnicos razoáveis e disponíveis. Além disso, dados pessoais de saúde são qualificados como sensíveis, e, portanto, sujeitos às regras mais rígidas do art. 11 da LGPD.[6] Como esperado, diante dos algoritmos de aprendizagem de máquina em operação, valem essas mesmas regras para o tratamento de outros dados pessoais que possam revelar dados pessoais de saúde.[7]

No tocante às finalidades excepcionalmente autorizadas, a LGPD permite, mesmo sem consentimento do titular, o tratamento de dados pessoais para estudos científicos em saúde pública, respeitadas as condições do art. 13.[8] Por outro lado, o art. 11 da lei proíbe o tratamento de dados pessoais de saúde para a

---

[5] LGPD. “Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.”

[6] LGPD. “Art. 5º Para os fins desta Lei, condidera-se: (...) II – dado pessoal sensível: dado pessoal 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; (...).”

[7] LGPD. Art 11: “§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.”

[8] LGPD. “Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.”

obtenção de vantagem econômica em detrimento do paciente, ou a seleção de riscos na contratação de planos privados de assistência à saúde, estabelecendo barreiras expressas ao uso dessas informações para fins incompatíveis com os princípios e objetivos fundamentais da Constituição Federal.[9]

Ainda, à semelhança da legislação do *habeas data*, a LGPD garante ao titular o acesso facilitado a informações sobre o tratamento de seus dados,[10] a prerrogativa de exigir a revisão e correção de seus dados em posse de terceiro, e o direito de não se submeter a decisões tomadas unicamente com base em tratamento automatizado de dados, o que tem fortes implicações no âmbito da governança de IA, sobretudo as espécies com menor grau de controle humano.[11]

Quanto a padrões técnicos de coleta, armazenamento e compartilhamento, todo o capítulo IV da legislação se dedica ao tratamento de dados pelo poder público, impondo procedimentos aos agentes do Estado visando coibir abusos e incentivar a eficiência e produtividade. A esse respeito, é pertinente destacar que a administração pública dispõe de prerrogativas extraordinárias, e pode realizar o tratamento de dados pessoais em hipóteses mais amplas do que os particulares,[12] principalmente para a execução de políticas públicas.[13]

Verifica-se, portanto, que o ordenamento jurídico brasileiro, em especial com a LGPD, dispõe de um conjunto de normas que tratam da governança

---

[9] LGPD. Art. 11: "§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica (...). § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários."

[10] LGPD. "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: (...)."

[11] LGPD. "Art. 20. O titular dos dados tem direito a solicitar a revisão (,por pessoa natural,) de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade."

[12] A Lei 12.527/11 (Lei de Acesso à Informação) e o Decreto 7.724/12 possuem normas específicas voltadas para o tratamento de dados em bancos públicos de informação.

[13] LGPD. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; (...)."

digital de IA na saúde, direcionadas principalmente à proteção de dados pessoais. De fato, as normas aferem importantes direitos aos usuários, e maior segurança jurídica aos controladores e operadores.

Há um debate crescente sobre o direito individual à privacidade e como ele limita o interesse coletivo em pesquisar dados de saúde para fins de pesquisa e saúde pública. Podemos fazer a seguinte reflexão: a privacidade estaria atrapalhando a inovação ou seria o contrário, ou seja, a inovação é quem estaria ameaçando a autonomia individual?

A falta de informação e conscientização da sociedade sobre os usos potencialmente perigosos dos dados coletados para fins de medicina, assim como a conexão entre os dados de saúde e os próprios indivíduos, levaram a criação de leis de proteção de dados ao redor do mundo, incluindo a Lei Geral de Proteção de Dados no Brasil (Lei 13.709/2018, abreviada “LGPD”), a se concentrar em mecanismos de coleta de dados mediante consentimento, sobretudo para dados pessoais sensíveis definidos no Art. 5º, II, da LGPD, que incluem dados de saúde.

O desenvolvimento da saúde digital representa um desafio para a proteção dos dados pessoais de saúde. O uso de tecnologias de Inteligência Artificial (IA) para a saúde, mais que uma promessa, já contribui para avanços na descoberta de medicamentos, patologias e prevenção de doenças. O uso dessas tecnologias pode otimizar resultados assistenciais obtidos a partir de dados, entretanto os gestores devem ficar atentos a aspectos éticos e à segurança das informações e dados relacionados à saúde.

Um dos objetivos dessa área é a busca por conhecimento cada vez mais avançado que existe por trás do desenvolvimento de várias doenças, a fim de criar, melhorar e expandir medidas protetivas, estabelecer diagnósticos mais precisos e tratamentos mais adequados, com o desenvolvimento de novos medicamentos, terapias, equipamentos e aprimoramento de técnicas cirúrgicas.

A utilização de dados em saúde, pode prejudicar a privacidade e a autonomia. Como destacam Campos e Santana (2022, p. 155):

> O direito dos indivíduos aos seus próprios dados é baseado em conceitos relacionados aos direitos humanos, incluindo o direito à propriedade, à privacidade, à autonomia e à dignidade humana. O exercício do direito de controle de seus dados pode incluir várias abordagens de consentimento individual e também de mecanismos coletivos para garantir que os dados sejam usados de forma adequada por terceiros.

As legislações e políticas de proteção de dados devem se nortear em direitos humanos que protejam os direitos dos indivíduos e fixem obrigações para os controladores e processadores de dados, tanto privados como públicos, bem como aplicação de sanções na hipótese de quebra destes direitos.

3. Compartilhamento e proteção de dados na era digital

Machado (2022, p. 103) enfatiza que:

> Muitos desses serviços de controle de dietas e peso, monitoramento de sono e mesmo produtividade, operam sem adequação a regras rígidas, mas alimentam uma indústria que de fato produz pesquisa e serviços na área da saúde em um sentido amplo.

Machado (2022, p.106) traz também a seguinte problemática:

> A questão central em torno da coleta massiva de dados de saúde via dispositivos conectados, gira em torno do impacto que isso tem na autonomia individual. Esse é um dos princípios mais relevantes da LGPD, estabelecida no Art. 2º, inciso II, e é um dos elementos fundamentais de todo o campo. A autodeterminação informativa surge por se entender que a capacidade de controlar a exposição e a circulação da nossa informação é aspecto fundamental da autonomia individual. Assim, é imprescindível pensar em salvaguardas para que as pessoas protejam seus interesses e se protejam contra os danos potenciais da coleta e análise de dados, especialmente quando se trata de nível coletivo.

De um lado, os desafios relacionados ao consentimento, uso e manipulação de dados também estão inerentemente conectados à capacidade das pessoas de entender e interpretar para que e como seus dados estão sendo usados.

4. As informações dos pacientes obtidas pelos serviços de saúde e os cuidados necessários no tratamento de dados sensíveis pós vigência da LGPD

No Brasil, a LGPD estabelece diversas diretrizes importantes para a proteção dos dados pessoais, dispõe sobre a digitalização e a utilização de

sistemas informatizados para a guarda, o armazenamento e o manuseio de dados, como prontuário de paciente.

De acordo com a LGPD, todo e qualquer dado pessoal deve ser tratado protegendo a privacidade do titular, o que significa que todas as informações contidas no prontuário devem ser coletadas e armazenadas de forma segura.

Os cuidados, conforme bem coloca Soares (2021, p. 9) envolvem, dentre outros:

> O conhecimento dos envolvidos (titular ou o seu responsável) quanto a quais são dados tratados, por quem o são, para que o são, em quais meios digitais ou físicos circulam ou são depositados, por quanto tempo são ou serão utilizados e como proceder para exercer os direitos de acesso, retificação, exclusão, etc. (os propósitos devem ser claros, legítimos, específicos e devidamente informados previamente ao destinatário, que é o titular ou quem deva autorizar por ele ou assentir ao ato).

No âmbito da tramitação dos processos judiciais, um dos cuidados necessários é a tramitação dos processos sob segredo de justiça, sendo que muitos magistrados já estão se adequando as diretrizes da LGPD. Nesse sentido, seguem julgados do TRF4:

> DECISÃO: **Considerando a garantia legal da proteção à privacidade, inclusive nos meios digitais (Lei 13.709/2018**), e estando ausente quaisquer das hipóteses que justifiquem, para fins do processamento desta demanda, a **necessidade de "tratamento dos dados pessoais" (art. 7º da Lei Geral de Proteção de Dados Pessoais - LGPD), reconsidero o despacho do evento 4. Assim, defiro o pedido de sigilo**. Intime-se. Oportunamente, paute-se para julgamento. (**TRF4, AC 5000727-16.2020.4.04.7212, PRIMEIRA TURMA, Relator ANDREI PITTEN VELLOSO, juntado aos autos em 11/07/2022**)
>
> **EMENTA:** PREVIDENCIÁRIO. PROCESSUAL CIVIL. AGRAVO DE INSTRUMENTO. INICIAL. NECESSIDADE DE QUALIFICAÇÃO PESSOAL. MOMENTO DO PROTOCOLO. PERMISSÃO. **ATRIBUIÇÃO DE SIGILO AOS DOCUMENTOS. 1. A lei processual não é incompatível com a LGPD e estabelece que algumas informações devem constar da inicial (art. 319, II). 2. Ao procurador da parte interessada é permitido, no momento do protocolo, atribuir "sigilo nível 1" aos documentos que entender pertinentes, justificando a necessidade do sigilo na peça que os introduz.** 3. A fim de possibilitar o acesso às instâncias superiores, consideram-se prequestionadas as matérias constitucionais e legais suscitadas no recurso, nos termos dos fundamentos do voto, deixando de aplicar dispositivos constitucionais ou legais não expressamente mencionados e/ou havidos como aptos a fundamentar pronunciamento judicial em sentido diverso do que está declarado. (**TRF4, AG 5051407-73.2021.4.04.0000, SEXTA TURMA,**

> **Relator JOÃO BATISTA PINTO SILVEIRA, juntado aos autos em 11/03/2022**)

É cabível, portanto, a aplicação do segredo de justiça, tendo em vista que serão anexados aos autos dados sensíveis do paciente/cliente. Na medida do possível, o máximo de anonimização deverá ser aplicado de forma a evitar a exposição desnecessária dos dados sensíveis dos pacientes/clientes (art. 89 do CEM).

O art. 13 da LGPD esclarece que “na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a base de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas”.

Filho e Ferrari (2021) alertam que, mesmo as instituições que não coletem dados novos, mas sigam armazenando dados antigos, precisam se adaptar aos ditames da LGPD.

De acordo com Filho e Ferrari (2021, p. 227), é natural que, vez ou outra, informações pessoais utilizadas em pesquisas científicas sejam objeto de vazamento, haja vista que até o Pentágono já foi hackeado, todavia:

> O que a lei tenta garantir, portanto, é que as empresas, hospitais, instituições de pesquisa e controladores de dados pessoais em geral, atendam a comandos basilares de segurança, por meio do estabelecimento de deveres de cuidado e guarda que reduzam a ocorrência desses incidentes, além da estruturação de um plano de ação que permita reduzir as consequências deletérias dos incidentes.

Ainda de acordo com Filho e Ferrari (2021), a completude, os cuidados com o armazenamento, os fluxos estabelecidos, e a resposta aos incidentes influirão, portanto, nas sanções aplicadas que, no campo administrativo, podem chegar a cinquenta milhões de reais por infração (art. 52, II, LGPD).

5. Vulnerabilidade do paciente/autor

Machado (2022) enfatiza que um embate surge entre o interesse público do uso dos dados pessoais e dados pessoais sensíveis e as proteções individuais. Ainda de acordo com Machado (2022, p. 109): “A LGPD oferece bases legais que contemplam o interesse público e também mais especificamente a saúde pública, exigindo uma criteriosa avaliação de necessidade e proporcionalidade para legitimar o tratamento com essas bases”.

Uma fonte de dados altamente promissora, mas que exige uma análise extremamente cautelosa, são os registros eletrônicos de saúde, que contêm resumos das atividades dos pacientes.

Machado (2022) destaca que o potencial de uso desses dados para pesquisa beira o inimaginável e que estudos indicam que o consentimento tem efeitos inibidores significativos sobre as possibilidades de pesquisa. Ou seja, os pesquisadores têm constatado que a exigência de consentimento para pesquisas médicas traz uma queda no número de registros disponíveis para pesquisa.

Além disso, Machado (2022, p.110) traz um alerta:

> Os requisitos de consentimento também podem ter um impacto negativo na qualidade dos dados, bem como na quantidade, ao introduzir um viés de seleção, uma vez que as pessoas que aceitam e que recusam o uso de dados parecem ter perfis demográficos significativamente diferentes.

Por tais razões, parte da doutrina defende que os benefícios superam significativamente os pequenos inconvenientes individuais.

Machado (2022, p.110) entende que:

> Esse padrão ético precisa se infiltrar na regulamentação sobre o que o interesse público realmente significa, por exemplo, estabelecendo padrões de exclusividade ou abertura das descobertas e desenvolvimentos de pesquisa, e estabelecendo os limites para que tipo de pesquisa não está englobado no que é considerado de interesse geral. Essa discussão é necessária para que se tenha fundamentos para buscar bases legais para o tratamento de dados pessoais sensíveis que não sejam dependentes do consentimento.

Machado (2022) coloca ainda que os órgãos governamentais de saúde deveriam se concentrar na criação de mecanismos que tornem a doação e

o consentimento de dados um padrão universal, o que pressupõe que a contribuição com dados é uma obrigação moral em relação aos interesses coletivos.

Um grande desafio é a aparente divisão entre o uso de dados públicos para pesquisa médica, que normalmente é considerada como justificada e de interesse público, e o desenvolvimento de produtos e serviços para a comercialização privada.

O avanço das tecnologias também contribui para a exposição e vulnerabilidade do paciente. A telemedicina, por exemplo, é uma prática que aumentou muito após a pandemia do covid, devendo ser praticada com o uso de ferramentas tecnológicas seguras, sendo que o paciente deve ser advertido de eventuais falhas em seu uso.

Outro ponto de vulnerabilidade é a dependência de *softwares* (incluindo aplicativos) para arquivamento de dados, que garantam a segurança na guarda de dados sensíveis de saúde dos pacientes.

Em 01/06/2023 participei de visita técnica ao Hospital Municipal São José de Joinville/SC com a Comissão de Direito da Saúde, Médico e Sanitário da Subseção da OAB Joinville e questionei um dos diretores do hospital acerca do vazamento de dados sensíveis dos pacientes. A pergunta se deu em razão de alguns clientes do escritório terem relatado a abordagem por empresas de assessorias jurídicas colocando seus serviços à disposição buscando soluções e benefícios previdenciários. A resposta que obtive sobre os vazamentos de dados pessoais sensíveis a empresas de assessorias foi de que existe uma investigação em curso pelo Ministério Público e trata-se de algo complexo, pois os *softwares* do Hospital são antigos, desatualizados e não foram adequados à LGPD, sendo que manipulam centenas de dados sensíveis de pacientes diariamente.

Tivemos uma situação no escritório em que a cliente é acometida de patologia de ordem psicológica e no curso do processo acidentou-se e foi internada no Hospital Municipal de Joinville. Ainda na maca e debilitada passou a receber mensagens de assessorias para que dê entrada em benefícios

previdenciários. Outros clientes relataram que também foram abordados por pessoas se colocando à disposição para prestar seus serviços. Abaixo seguem colacionadas algumas mensagens recebidas por clientes do escritório a fim de exemplificar o quão vulnerável estão os pacientes usuários principalmente do SUS, pois certamente tiveram seus dados de saúde vazados:

> Oi doutora eu recebi umas mensagens hoje que mim deixou meio emcacucado. Essas são as mensagens:
>
> Olá, boa tarde. Tudo bem? Tentei entrar em contato por telefone, mas não tive sucesso.
>
> Eu sou o (xxx), sou assessor previdenciário da Assessoria (xxx), escritório especializado na área de acidente de trabalho do INSS. Eu gostaria de falar com (xxx) sobre um acidente de trabalho que ocorreu em (xxx). Agradeço desde já!
>
> • O que é o auxílio acidente?
>
> É um benefício dado pelo INSS, no valor da metade do que recebia no auxílio doença, para aqueles que sofreram acidente de trabalho e possuem sequela (pino, placa, parafuso, sofreram alguma amputação, perderam algum tipo de movimento, etc.) até a aposentadoria.
>
> •Quanto custa para dar entrada no processo?
>
> O processo só vai gerar custo caso seja ganho (99% de chance), e o pagamento são as 3 primeiras parcelas do benefício. Por exemplo: a pessoa começa a ganhar o benefício em janeiro - as parcelas de janeiro, fevereiro e março serão o pagamento do escritório. Após as 3 primeiras parcelas pagas, o benefício é todo da pessoa.
>
> • Envolve a empresa onde sofreu o acidente?
>
> Não. Esse benefício é dado pelo INSS, e o processo não envolve a empresa onde sofreu o acidente e nem seu trabalho atual.
>
> • Qual a diferença do auxílio-doença pro auxílio-acidente?
>
> Auxílio doença: benefício que a pessoa recebe do INSS enquanto está afastada do trabalho. Auxílio acidente: benefício que a pessoa que ficou com sequela do acidente recebe até a aposentadoria.
>
> • Quem tem direito?
>
> - Pessoas que possuem sequela: pino, placa, parafuso, haste, sofreu amputação. - Sofreu acidente no trabalho ou no percurso casa-trabalho ou trabalho-casa . NÃO tem direito: quem não possui nenhuma sequela.
>
> ----
>
> Oi, tudo bem? Estou entrando em contato pra saber se você está recebendo o Auxílio-Acidente do INSS. E se por conta do seu acidente de trabalho ficou algum tipo de lesão permanente, algum tipo de sequela,

> ocorreu alguma amputação, ou se você passou por cirurgia que teve que colocar placa, pino, haste, alguma coisa do tipo.
>
> ---
>
> Bom dia Sra. (xxx), Tudo bem? Me chamo (xxx) sou assistente jurídica do advogado especialista em previdenciário Dr. (xxx)
>
> Estou entrando em contato com você referente ao auxílio doença que foi negado pelo INSS. Posso agendar um horário para vir até nosso escritório?
>
> ----
>
> BOM dia Dra Cíntia é a (xxx) ontem recebi uma ligação não atendi depois mandaram um mensagem perguntando se eu era (xxx) falei sim Uma moça se chama (xxx) era do diário oficial do INSS perguntando se eu tinha advogado Ela é secretaria do advogado Dr (xxx). Não respondi nada
>
> ----
>
> Olá, tudo bem? Me chamo (xxx), falo em nome da (xxx) Assessoria.
>
> Trabalhamos com INDENIZAÇÕES E BENEFICIOS. Você teve alguma FRATURA, LESÃO LIGAMENTAR OU LUXAÇÃO?
>
> Podemos estar te ajudando a receber algum valor referente a isso.
>
> Me dê um OI para darmos continuidade na conversa! Ótimo dia ☺ (Grifou-se)

Depreende-se das mensagens acima que não há respeito à privacidade e ao sigilo dos dados pessoais sensíveis. Não bastasse, muitas vezes estas pessoas vão pessoalmente na casa dos pacientes/clientes oferecerem serviços. Já teve cliente que me ligou por chamada de vídeo, pois tinha uma pessoa em sua casa, a par de sua enfermidade e colocando-se à disposição para “ajudar”. Sentindo-se constrangida e com a privacidade invadida disse que iria ligar para a sua advogada de confiança. Ou seja, situações como essa são muito frequentes e tais práticas precisam ser abolidas. Foi justamente motivada por estas questões que me deixaram indignada é que decidi dedicar a pesquisa do artigo à LGPD.

Extrai-se do informativo Migalhas[14] um caso de vazamento de informações hospitalares:

---

[14] Vazamento de informações hospitalares. Tratamento de dados e inobservância da LGPD pode causar indenizações milionárias. Migalhas. 12 jul. 2022. Disponível em:

> (...) **Em uma pesquisa foi descoberto que somente 8,7% das empresas do setor de saúde e hospitais estão em conformidade com os requisitos da lei de proteção de dados.** Este número assusta, pois, as sanções são graves para aqueles que não estão seguindo todos os parâmetros de tratamento, gestão e transmissão dos dados.
>
> Uma paciente, em Brasília, teve seus dados vazados, no qual, seu filho recebeu uma ligação, falando sobre um procedimento, no valor de R$ 3.000 mil. O filho da paciente efetuou a transferência desse valor, logo após, descobriu que nada mais era, que um golpe de um estelionatário. O órgão julgador condenou o hospital a pagar danos morais e a restituir o valor pago. Cabe ressaltar que a LGPD não estava sob vigência no momento em que aconteceu o caso.
>
> **Pois bem, os dados contidos em exames, diagnósticos, procedimentos e afins, são dados confidenciais e ultraprivativos, que não deve ser repassado, nem mesmo para parentes do paciente, ainda mais para terceiros. O tratamento e gestão desses dados devem ser restritos à equipe que efetua o tratamento, proibindo acessos de terceiros.**
>
> **Em caso de prontuário digital, o acesso deve ser registrado, com a identificação dos usuários que acessaram aquela informação**. No caso da atriz, o vazamento das informações causou danos maiores, do que uma pessoa anônima, e não só isso, o procedimento realizado é de cunho extremamente pessoal e íntimo.
>
> A responsabilidade civil do hospital, em relação ao vazamento, atinge a esfera extrapatrimonial e patrimonial da atriz, visto que, por ser artista, a matéria jornalística expõe de maneira cruel e negativa um trauma que a mesma vinha tentando lidar na esfera particular e na judicial onde todos os seus direitos e deveres estavam corretamente assistidos.
>
> A LGPD não é, como costumeiramente se fala, uma lei de enfeite, "ela pegou", de toda forma, os locais que não estiverem em conformidade com as diretrizes, no que diz respeito a todas as etapas de gestão dos dados, estarão sob a possibilidade de sanções judiciais severas. (...) (Grifou-se)

O vazamento de dados sensíveis à saúde e a fragilidade na guarda de tais dados é um grande problema nos dias atuais, sendo que se adequar é o melhor caminho. Sendo assim, a necessidade de um projeto bem elaborado de tratamento e manuseio dos dados é fundamental.

Deve-se ter um cuidado muito grande para se evitar que as informações dos pacientes cheguem indevidamente a terceiros. Para evitar

---

https://www.migalhas.com.br/depeso/369617/vazamento-de-informacoes-hospitalares, acesso em 24 jun. 2023.

inconvenientes é indicado que, na alta hospitalar, o próprio paciente indique quem poderá receber informações.

Instituições financeiras também são conhecidas por entrarem em contato com as pessoas assim que algum benefício previdenciário é implantado no intuito de oferecer empréstimos consignados. Esta é outra questão que merece debate específico.

Além disso, outra ilicitude que vem crescendo é o oferecimento de "listas do INSS" de segurados que tiveram o benefício indeferido. Auditorias deveriam ser feitas, assim como maior fiscalização para coibir esse tipo de prática que se mostra na contramão das diretrizes da LGPD, da moral, ética e transparência no tratamento de dados. É uma verdadeira aberração que tais condutas ainda sejam corriqueiras nos dias de hoje.

Outro desafio a ser enfrentado é a invasão de *hackers* nos bancos de dados colocando em risco informações de trato confidencial[15], conforme publicado em matéria no Conjur:

> Os *hackers* se utilizam de falhas na criptografia dos sistemas para impedir que os proprietários dos sites os acessem e, para a devolução dos endereços eletrônicos e dados, solicitam que seja feito o pagamento de uma quantia, ação semelhante a sequestros. O mesmo ocorreu neste ano com o site do Superior Tribunal de Justiça.
>
> Desde o início da pandemia, o Ministério da Saúde já esteve envolvido em ao menos um outro acidente de segurança que resultou no vazamento de dados pessoais sensíveis de diversos cidadãos. Em novembro de 2020, foi apurado que um funcionário do Hospital Albert Einstein que participa do Projeto Proadi-SUS, em que são realizadas trocas de informações entre o sistema de saúde público e hospitais privados para aprimoramento do sistema, teria exposto dados de cerca de 16 milhões de pacientes que teriam passado por algum tratamento ou teste relacionado com a Covid-19.
>
> Os dois incidentes citados colocam em foco a dificuldade e a ausência de sistemas de segurança fortes no Ministério da Saúde. Os dados tratados são todos caracterizados como sensíveis, nos termos do artigo 5º, II, da LGPD, por envolverem informações sobre a saúde dos titulares. Desse modo, os agentes de tratamento deveriam, ao menos, fornecer um sigilo

[15] Consultou Jurídico Conjur. Vazamento em ministério: instituições públicas sabem lidar com dados sensíveis? 17 dez. 2021. Disponível em: https://www.conjur.com.br/2021-dez-17/opiniao-instituicoes-publicas-sabem-lidar-dados-sensiveis. Acesso em 25 jun. 2023.

> e segurança desses dados de uma forma mais abrangente, diante do caráter das informações, o que não se observa na prática.
>
> Incabível dizer que o Ministério da Saúde não pode realizar o tratamento dessas informações, pois pautada em efetivo embasamento legal, inclusive para fins de execução de políticas públicas. Porém, questiona-se sobre quais são os riscos em que os cidadãos estão expostos e como a ANPD deve passar a atuar para impedir que esses incidentes sejam tão recorrentes e que o Ministério da Saúde, assim como qualquer outro agente que realiza tratamento de dados, seja responsável pela restauração dos danos causados. Para tanto, é imprescindível que a ANPD atue de forma a conscientizar os agentes de tratamento sobre métodos para evitar os riscos e danos à privacidade dos titulares.
>
> Cada vez mais, as autoridades públicas recebem ataques direcionados em relação aos seus *sites*, o que coloca em risco a segurança da informação. Caberá à ANPD, agora estabelecida e com capacidade de aplicação de multas e determinação de ações, utilizar esse vazamento como exemplo de prática indevida e impor as consequências cabíveis.
>
> A proteção aos dados pessoais é medida prioritária e envolve, justamente, a privacidade dos cidadãos. Independentemente de estarmos lidando com órgãos públicos ou organizações privadas, o tratamento pela ANPD deve ser igualitário e as práticas adotadas pelo Ministério da Saúde devem ser apuradas. Não há como os cidadãos lidarem recorrentemente com essas falhas na segurança, observando o vazamento dos seus dados, sem qualquer atitude devida.
>
> Informações sobre os incidentes de segurança também devem ser divulgadas, inclusive de acordo com as possíveis sanções previstas no artigo 52 da LGPD, a fim de que outras entidades que realizam o tratamento de dados possam melhor se proteger.

De acordo com Rivelli (2021), o setor de saúde é um dos mais visados pelos ataques cibernéticos do tipo *ransomware* – que criptografa arquivos e exige resgate para desbloquear os dados, principalmente por possuir dados confidenciais sobre pacientes.

Para Moreira e Santos (2021), pode-se apontar alguns desafios na implantação e operacionalização da plataforma digital na saúde, em conformidade com a LGPD, como o desconhecimento da LGPD por uma parcela considerável dos gestores da saúde; a complexidade na sua aplicabilidade; as dificuldades financeiras quanto a segurança de dados, que tem elevado custo; a veracidade dos dados; a ausência de dados essenciais e dados falsos; as falhas no funcionamento do sistema e no tratamento de dados; o descarte de dados sensíveis; a responsabilização por vazamentos num sistema interfederativo de dados sensíveis; a segurança de dados colhidos por agentes comunitários de saúde em seus *tablets*; a necessária coordenação nacional do sistema nacional e a sua governança

interfederativa; o vazamento de dados de milhões de pessoas que não pode ser reparado; o uso indevido de dados e a captura do cidadão em uma sociedade tecnológica. Ou seja, há muitos pontos vulneráveis que precisam ser resolvidos.

Os conselhos de fiscalização devem monitorar, com mais intensidade o cumprimento da ética profissional, a fim de que se crie um ambiente de permanente vigilância quanto à segurança dos dados em saúde e reforço da conduta ética no uso dos sistemas informatizados.

Nesse contexto, o vazamento de dados pessoais, dentro dos aspectos da LGPD fez com que crescesse o número de ações judiciais em busca de indenizações.[16]

Considerações Finais

O tratamento de dados sensíveis em saúde demanda adequação de toda a operação à Lei Geral de Proteção de Dados. Não é tarefa simples o procedimento de implantação e adequação à LGPD. Avanços na área de coleta, armazenamento e análise de dados possibilitam o progresso na área da saúde, no entanto, alguns desafios técnicos e éticos perduram.

Verifica-se que há muitos desafios e que os pacientes encontram-se em situação de grande vulnerabilidade. Os obstáculos são grandes e vão desde a invasão de *hackers*, sistemas/*softwares* precários e não preparados para o tratamento de dados de forma segura, vazamento de dados a terceiros para obtenção de vantagens econômicas, etc.

Portanto, é de extrema importância que a LGPD seja cumprida, mesmo ante todos os desafios apresentados e que sanções sejam aplicadas pela não observância do correto tratamento de dados dos pacientes.

É necessário que treinamentos e medidas preventivas mitigadoras de danos sejam adotados; que sejam adotados planos de governança e gestão de

[16] Ações judiciais sobre LGPD aumentam em mais de 500% em dois anos. São Paulo. Disponível em: https://www.jota.info/justica/acoes-judiciais-sobre-lgpd-aumentam-em-mais-de-500-em-dois-anos-09032023. Acesso em 25 jun. 2023.

riscos. O controle de acessos deve ser eficiente e várias medidas de segurança implementadas de forma a superar a vulnerabilidade dos pacientes, a fim de que sejam cumpridas e respeitadas as diretrizes legais.

Uma das consequências da vigência da LGPD é o aumento do conhecimento do cidadão sobre seus direitos e quando se sente lesado, o brasileiro tem a cultura de judicializar. Consequentemente, observou-se um aumento exponencial de ações judiciais que discutem a aplicação da LGPD.

Se antes uma prática ilegal causava incômodo e aborrecimento ao paciente, após a vigência da LGPD ela causa incômodo e aborrecimento, mas também o leva a agir e buscar seus direitos.

Referências das fontes citadas

CAMPOS, Roberta de Freitas; SANTANA, José Paranaguá de. LGPD na Saúde Digital: **Saúde global e proteção de dados na era digital**. São Paulo: Thomson Reuters Brasil, 2022.

FILHO, Alexandre Dias Porto Chiavegatto; FERRARI, Isabela. LGPD na Saúde Digital: **Uso d Big Data em saúde no Brasil: perspectivas e desafios de conformidade com a LGPD**. São Paulo: Thomson Reuters Brasil, 2022.

MACHADO, Vieira. LGPD na Saúde Digital: **Implicações éticas e jurídica do desenvolvimento de uma saúde a partir de dispositivos conectados: O desafio dos dados de saúde**. São Paulo: Thomson Reuters Brasil, 2022.

MOREIRA, Marizelia Leão; SANTOS, Lenir. LGPD na Saúde Digital: **A digitalização do prontuário de pacientes do sistema único de saúde e a criação de uma plataforma única de armazenamento de dados: vulnerabilidades e adequação com a LGPD**. São Paulo: Thomson Reuters Brasil, 2022.

RIVELLI, Fabio. LGPD na Saúde Digital: **Aplicação e conformidade dos dados sensíveis na saúde digital e os preceitos da LGPD**. São Paulo: Thomson Reuters Brasil, 2022.

SOARES, Flaviana Rampazzo. Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. **Revista IBERC**, Belo Horizonte, v. 4, n. 2, p. 18-46, maio/ago. 2021.