XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO E SAÚDE

JANAÍNA MACHADO STURZA

LITON LANES PILAU SOBRINHO

JURACI MOURÃO LOPES FILHO

D597

Direito e saúde [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Janaína Machado Sturza; Juraci Mourão Lopes Filho; Liton Lanes Pilau Sobrinho. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-851-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Saúde. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34

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

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO E SAÚDE

Apresentação

Nos dias 15, 16 e 17 de novembro, aconteceu o XXX Congresso Nacional do CONPEDI, na cidade de Fortaleza, no Ceará, mais especificamente no Centro Universitário Christus – Unichristus.

No dia 17 aconteceu o GT Direito e Saúde, no qual foram apresentados trabalhos que versaram sobre diferentes perspectivas e possibilidades de diálogos com a saúde enquanto direito social, fundamental e humano, salientando-se pautas como estudos conceituais e/ou relatos de experiências no contexto brasileiro e/ ou internacional, focalizando a concretização da saúde e suas demandas, com alicerces na Constituição Federal. Foram abordados temas como a judicialização da saúde, especialmente no que refere-se a medicamentos, internações hospitalares e tratamentos de alto custo; a saúde digital e suas interlocuções com as tecnologias; questões de gênero vinculadas ao direito à saúde; medicamentos e experimentos em saúde; autonomia da vontade e prospecções da saúde com a bioética; entre outros.

Sem dúvida alguma foram belos e interessantes trabalhos que contribuíram não somente para amplas reflexões, mas também, e certamente, são grandes contribuições para a pesquisa jurídica e social na academia brasileira e internacional, notadamente com destaque ao direito à saúde.

Janaína Machado Sturza – UNIJUI

Liton Lanes Pilau Sobrinho – Universidade do Vale do Itajaí / UPF

Juraci Mourão Lopes Filho – Centro Universitário Christus

AS BOAS PRÁTICAS DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NA TELESSAÚDE

GOOD PRACTICES FOR PROCESSING SENSITIVE PERSONAL DATA IN TELEHEALTH

João Araújo Monteiro Neto
Larissa Rocha de Paula Pessoa
Regina Célia do Nascimento Neves

Resumo

A saúde é essencial para a vida do ser humano, por esse motivo a Constituição Federal de 1988 buscou garantir o acesso à saúde como um direito fundamental. Atualmente, o debate e reflexões sobre as boas práticas de tratamento de dados pessoais sensíveis no sistema de telessaúde se fazem necessárias, não somente pela relevância legal e social do tema, mas pela própria forma de "aceleração" da telemedicina em razão da Covid-19. Por isso, esta pesquisa visa analisar as boas práticas no tratamento de dados pessoais sensíveis na telessaúde. Para isso, foi adotada uma abordagem metodológica bibliográfica e documental por meio da análise de legislação, regulamentos, recomendações técnicas e outros documentos necessários. Trata-se, portanto, de uma pesquisa qualitativa que visa levantar o debate sobre a importância de boas práticas de proteção de dados na telessaúde. Por fim, conclui-se que existem boas práticas em proteção de dados relativas ao setor da saúde, mas que ainda precisa ser aprimorada e desenvolvida para o cenário brasileiro e que sejam elaborados protocolos juntamente com a Autoridade Nacional de Proteção de Dados e minimizar riscos, vulnerabilidades e inconsistências na privacidade e proteção dos dados na telessaúde.

Palavras-chave: Saúde, Telessaúde, Dados pessoais, Proteção de dados, Boas práticas

Abstract/Resumen/Résumé

Health is essential for human life, for this reason the Federal Constitution of 1988 sought to guarantee access to health as a fundamental right. Currently, the debate and reflections on good practices for handling sensitive personal data in the telehealth system are necessary, not only due to the legal and social relevance of the subject, but also due to the very form of "acceleration" of telemedicine due to Covid-19. Therefore, this research aims to analyze good practices in the treatment of sensitive personal data in telehealth. For this, a bibliographical and documental methodological approach was adopted through the analysis of legislation, regulations, technical recommendations and other necessary documents. It is, therefore, a qualitative research that aims to raise the debate on the importance of good data protection practices in telehealth. Finally, it is concluded that there are good practices in data protection related to the health sector, but that it still needs to be improved and developed for the Brazilian scenario and that protocols are developed together with the National Authority

for Data Protection and minimize risks, vulnerabilities and inconsistencies in privacy and data protection in telehealth.

Keywords/Palabras-claves/Mots-clés: Health, Telehealth, Personal data, Data protection, Good habits

Introdução

Atualmente, pode-se afirmar que não há sociedade sem o uso de dados pessoais, essa percepção é também verdadeira nas atividades relacionadas a saúde, pois a ciência e a medicina estão evoluindo com força no campo digital visando melhorias e também buscando acompanhar a própria evolução tecnológica. Vale ressaltar que essa relação entre saúde e tecnologia possui dualidade constitucional pois além da garantia à proteção de dados pessoais nossa constituição federal garante o acesso à saúde, tanto no aspecto preventivo como assistencial como um direito fundamental.

Nesse contexto o uso de dados pessoais na execução de ações de saúde reveste-se de um nível de complexidade elevado posto que o constante embate entre o interesse público materializado na execução de políticas públicas de saúde, onde dados pessoais possuem valor fundamental, contrastam diretamente com os interesses dos titulares de dados pessoais de manterem suas informações privadas e seguras.

Desse modo, o debate e reflexões sobre as boas práticas de tratamento de dados pessoais sensíveis no sistema de telessaúde se fazem necessárias, não somente pela relevância legal e social do tema, mas pelo avassalador avanço de novas tecnologias associadas a medicina, dentre as quais destacamos a telemedicina, em virtude do crescente desenvolvimento tecnológico e da pandemia da Covid-19.

Isso porque o contexto da pandemia foi um período que gerou debate sobre a utilização de dados de georreferenciamento para o combate à Covid-19 e que também se destacaram algumas alternativas para evitar o aglomeramento das pessoas, tais como: a implementação do lockdown e a telemedicina (BRASIL, 2020). Nesse aspecto, é importante entender que isso aconteceu no mesmo cenário da entrada em vigor da Lei Geral de Proteção de Dados.

Dessa forma, considerando os parâmetros regulatórios existentes no Brasil sobre a telessaúde e o que preconiza o art. 5º, II e 11, ambos da LGPD, esta pesquisa tem como problema central: quais as boas práticas viáveis e eficazes para o tratamento de dados pessoais sensíveis na telessaúde?

Em relação ao objetivo geral, esta pesquisa visa investigar as boas práticas no tratamento de dados pessoais sensíveis na telessaúde. Já os objetivos específicos buscam descrever o panorama da proteção de dados e analisar os artigos 5º, II e art. 11, ambos da LGPD, que tratam sobre dados pessoais sensíveis, analisar as normas correlatas e resoluções, principalmente de órgãos relativos ao setor da saúde, como ANS, CFM e a lei de telessaúde, e

por último, identificar as boas práticas relacionadas ao tratamento de dados pessoais sensíveis na telessaúde.

A abordagem metodológica utilizada nesta pesquisa foi bibliográfica e documental por meio da análise de legislação, regulamentos, recomendações técnicas e outros documentos necessários para o desenvolvimento deste artigo. Trata-se, portanto, de uma pesquisa qualitativa que visa levantar o debate sobre a importância de boas práticas de proteção de dados na telessaúde.

Para isso, este artigo teve o seu desenvolvimento dividido em três partes. A primeira parte refere-se ao estado da arte sobre a proteção de dados, antes mesmo da Lei Geral de Proteção de Dados, apresentando a complexidade e dinamicidade relacionada à proteção de dados em perspectiva histórica para, em seguida, abordar a tutela dos dados de saúde na LGPD e na CF/88.

Já a segunda parte visa analisar as normas setoriais e recomendações de órgãos como ANS e CFM, que apresentam uma lógica de corregulação, assim como também estudar a Lei da Telessaúde, extraindo uma perspectiva de proteção de dados e de compatibilidade com a Lei Geral de Proteção de Dados e o Marco Civil da Internet.

A terceira parte busca apresentar boas práticas no tratamento de dados pessoais sensíveis na telessaúde, considerando as particularidades regulatórias da proteção de dados no Brasil para dados pessoais sensíveis e os estudos com recomendações já existentes.

Por fim, conclui-se que existem boas práticas em proteção de dados relativas ao setor da saúde, mas que ainda precisa ser aprimorada e desenvolvida para o cenário brasileiro e que sejam elaborados protocolos juntamente com a Autoridade Nacional de Proteção de Dados e minimizar riscos, vulnerabilidades e inconsistências na privacidade e proteção dos dados na telessaúde.

1- Panorama da Proteção de Dados Pessoais e o Tratamento de Dados de Saúde

Inicialmente, é necessário fazer um panorama do histórico da proteção de dados pessoais para que posteriormente se possa avançar em relação às boas práticas na área da saúde. A proteção de dados e a privacidade não são assuntos recentes, são temas relevantes que já são discutidos há muitas décadas, o que ocorre é que na atualidade ganharam maior visibilidade por causa do Regulamento Geral da União Europeia e a sua inegável influência na Lei Geral de Proteção de Dados do Brasil.

O direito à privacidade surgiu nos Estados Unidos, sendo destaque o artigo "The right of privacy" de Samuel Warren e Louis Brandeis, mas as primeiras leis referentes ao tema proteção de dados surgiram nos nas décadas de 70 na Europa, sendo a primeira legislação oficialmente estruturada e direcionada a temática surgiu na Alemanha, intitulada a Lei de Proteção de Dados pessoais do Land de Hesse. E, ao longo das décadas, foram surgindo diversas regulações específicas, como a sueca, a francesa, a dinamarquesa e entre outras (DONEDA, 2021).

Em 1981, o Conselho da Europa cria a Convenção 108, incitando a adoção de normas específicas para o tratamento desses elementos sob seus próprios parâmetros. Já em 1995, surge a Diretiva 95/46/CE, estabelecendo uma definição básica de dados pessoais e outras delimitações importantes para a discussão do tema, além do incentivo ao comércio, mas foi revogado pelo Regulamento Geral de Proteção de Dados (RGPD) em 2018, sendo diretamente aplicada a todos os países-membros da União Europeia.

No cenário brasileiro, antes do surgimento da Lei Geral de Proteção de Dados, a Constituição Federal de 1988 já resguardava a privacidade no seu art. 5º, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988) .

Além disso, outros códigos já desenhavam de forma esparsa uma "proteção dos dados pessoais", como por exemplo, o Código do Consumidor, a Lei de Acesso à Informação, a Lei Carolina Dieckmann e o Marco Civil da Internet (MCI).

Sendo o Marco Civil da Internet o primeiro a estabelecer de forma direta os "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014), apresentando conceitos sobre a neutralidade de rede e a liberdade de expressão e definindo quais são as obrigações dos órgãos públicos e privados no fornecimento de internet e a responsabilidade dos provedores da internet.

Apesar do MCI estabelecer algumas proteções a privacidade e aos dados dos atores que acessam os serviços dos entes por ele regido, nota-se que ele apresenta a proteção de dados pessoais de forma genérica, não sendo uma regulamentação sobre esse tema, sendo necessário uma legislação que tratasse da proteção de dados no Brasil.

É a partir do surgimento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, influenciada pelo contexto internacional, sobretudo, pelo Regulamento Geral de Proteção de Dados da União Europeia, que se passou a regulamentar a proteção de dados para todas as empresas e setor público que realizam o tratamento de dados.

Após a vigência da LGPD, a proteção de dados pessoais ganhou amparo na Constituição Federal de 1988, sendo inserida expressamente pela Emenda Constitucional n. 115/2022 (BRASIL, 2022), que assegura a proteção de dados pessoais como direito fundamental previsto no art. 5º, inciso LXXVIII da CF (BRASIL, 1988).

Dito isso, pode-se mencionar que os principais pontos da proteção de dados na LGPD são: a garantia de direito para os titulares de dados; maior transparência sobre o tratamento de dados realizados pelo setor privado e setor público, permitindo a redução da assimetria informacional; estabelecer deveres para os agentes tratamentos e maior segurança jurídica; portabilidade de dados; proteção especial para os dados sensíveis; e sanções administrativas, se houver descumprimento da lei.

Isso implica em uma série de mudanças estruturais que demandam tempo e investimento das empresas que tratam dados no Brasil, necessitando o desenvolvimento e implementação de boas práticas vinculadas à proteção e segurança dos dados pessoais, especialmente, as empresas que tratam dados pessoais sensíveis no setor da saúde.

A Lei Geral de Proteção de Dados resguarda os dados pessoais e dados pessoais sensíveis, sendo conceitos definidos no art. 5º, inciso I e II da LGPD, o que se pretende analisar neste estudo são os dados de saúde, considerados dados pessoais sensíveis e tratados por empresas do setor da saúde, confira:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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. (BRASIL, 2018)

O tratamento de dados pessoais sensíveis somente poderá ocorrer nas hipóteses estabelecidas no art. 11 da LGPD, que pode ser pelo consentimento de forma específica, destacada e para finalidades específicas (BRASIL, 2018), e sem o consentimento do titular, nas hipóteses em que for indispensável para o "cumprimento de obrigação legal ou regulatória pelo controlador" previsto no inciso II, alínea "a" (BRASIL, 2018) e a "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" estabelecido no inciso II, alínea "f" do mesmo dispositivo (BRASIL, 2028) em se tratando de dados de saúde e sem prejuízo de outra base legal no caso concreto.

Observa-se que o art. 11 da LGPD, estabelece uma vedação para a comunicação ou uso compartilhado entre controladores sobre os dados de saúde com o objetivo de obter

vantagem econômica, com algumas exceções que sejam "[...]relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados" em seu §4º, sendo permitido para portabilidade solicitada pelo titular e para fins de transações financeiras e administrativas decorrentes do uso e da prestação dos serviços (BRASIL, 2018).

Ressalta-se que as operadoras de planos privados de assistência à saúde não podem realizar tratamento de dados para fins de seleção de riscos em contratação e exclusão de beneficiários com base no art. 11, §5º da LGPD (BRASIL, 2018), pois essa prática é expressamente vedada pela lei, uma vez que poderia ocasionar práticas discriminatórias e outros danos à vida dos titulares de dados.

Além disso, não há o que se falar em utilização do legítimo interesse para tratamento de dados pessoais sensíveis, a própria legislação afastou a sua aplicação quando não colocou como uma das bases legais de tratamento de dados pessoais sensíveis, confira:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. (BRASIL, 2018)

Verifica-se que é possível a realização de tratamento de dados sem o consentimento do titular é possível quando for adequadamente utilizada a base legal de tutela de saúde ou a de cumprimento de obrigação legal ou regulatória pelo controlador, sem prejuízo de outra base legal conforme o caso concreto, uma vez que:

> Art. 5º, X da LGPD: 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. (BRASIL, 2018)

Ressalta-se que, além da LGPD, os serviços de saúde e os profissionais da saúde precisam observar outras legislações e regulações aplicáveis na área da saúde, inclusive, em relação à telemedicina, que é esse exercício ou acesso à saúde no ambiente digital, sendo regulamentada na recente Lei de Telessaúde.

Os desafios relacionados aos avanços da telessaúde estão relacionados à garantia da confidencialidade dos dados no ambiente digital, portabilidade dos dados, a forma de transmissão e armazenamento dessas informações de saúde.

Ressalta-se ainda a necessidade de uma segurança da informação e providências adequadas na interoperabilidade da informação que sejam capazes de resguardar os dados de saúde, que se enquadram nos dados pessoais sensíveis e que recebem uma proteção especial na LGPD.

Desse modo, após ser apresentado o cenário de proteção de dados de saúde na LGPD, será abordado na próxima seção as principais regulamentações que permeiam o contexto de corregulação dos dados de saúde no Brasil, especialmente, sobre a telessaúde.

2- Análise das Normas e Recomendações do Setor da Saúde relacionadas a Proteção De Dados e da Lei de Telessaúde

Não há dúvidas da relevância da proteção de dados no âmbito da saúde, principalmente, considerando que os dados tratados são os sensíveis e definidos na LGPD como dados "relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a um indivíduo"(BRASIL, 2018).

Desse modo, os órgãos reguladores da área de saúde se manifestaram para normatizar as práticas desejáveis e/ou esperadas pelos entes da saúde envolvidos, assim como também para orientar em relação às boas práticas para o tratamento dos dados pessoais utilizados para a efetiva prestação do serviço de saúde aos titulares de dados.

Entende-se que os impactos da LGPD na saúde estão diretamente relacionados ao aumento da responsabilidade e cautela na gestão das informações, de modo a evitar vazamentos e o uso inadequado dos dados, passando a ser uma preocupação geral das entidades envolvidas (Icict/Fiocruz, 2023).

Nesse sentido, tem-se uma recente pesquisa realizada e publicada pelo Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), Intervozes – Coletivo Brasil de Comunicação Social e Instituto Brasileiro de Defesa do Consumidor (Idec), que mostra o posicionamento da Abramge – Associação Brasileira de Planos de Saúde:

> Obviamente uma preocupação que eu acho que não é só o setor de saúde, mas uma maneira geral em todos os setores, o vazamento. A segurança e as camadas de segurança aplicáveis e como fazer isso funcionar sem travar a operação, e preservando o dado do paciente, acho que será sempre a preocupação número 1 (um) das operadoras. Em termo de consentimento e base legal aplicável, eu vejo que as operadoras têm as suas próprias assessorias jurídicas, seus mapeamentos internos estão sendo realizados, seja da pequena para a grande operadora, todas de acordo com sua possibilidade financeira e sua operação, estão fazendo o dever de casa no sentido de construir tudo muito alinhado dentro da operação (Icict/Fiocruz, 2023).

Na mesma pesquisa, observa-se o representante do CFM – Conselho Federal de Medicina, se posicionou de forma centrada na existência de normas regulamentares do conselho sobre a relação médico-paciente e fez diversas afirmações de que essas normas "estão adequadas à Lei Geral de Proteção de Dados Pessoais", destaca-se:

> Então, assim, nós acreditamos [...] que as nossas resoluções, o nosso arcabouço regulamentar tem uma certa adequação razoável já com a LGPD. Ele não se baseou obviamente na Lei Geral de Proteção de Dados porque ele é anterior a ela. Nós trazemos esse tipo de interação com a lei baseado em princípios que vêm da própria Constituição. Sobretudo na questão do respeito à privacidade e à intimidade. Assim, a atividade médica em si, ela é uma atividade que envolve dados sensíveis tanto que uma das hipóteses específicas que a lei determina quanto a dados sensíveis é exatamente aquelas que envolvem a saúde do paciente (Icict/Fiocruz, 2023).

A partir da crescente preocupação social e setorial sobre o tema, surgiram resoluções, normas e regulamentos que visam essa adaptação e harmonia com a Lei Geral de Proteção de Dados, na busca de eficiência na proteção e segurança de dados pessoais sensíveis dos titulares.

Dessa forma, desenvolve-se no Brasil, um contexto de corregulação na matéria de proteção de dados na área da saúde e que segundo Frazão, Oliva e Abilio a corregulação "combinaria diferentes categorias de práticas regulatórias e exigiria o envolvimento central dos agentes privados e dos governos, a fim de propiciar muitas vantagens da autorregulação sem as mesmas desvantagens" (FRAZÃO; OLIVA; ABILIO, 2019, p. 685).

Nesse sentido, a Resolução Administrativa nº 80 da Agência Nacional de Saúde – ANS de 28 de junho de 2022, que dispõe sobre a Política de Proteção de Dados Pessoais no âmbito da Agência Nacional de Saúde Suplementar, relacionando-se diretamente com a LGPD, quando determina que os dados pessoais deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado em cumprimento ao disposto no art. 25 da Lei nº 13.709/2018 e no art. 8º § 3º, da Lei nº 12.527/2011, de forma a facilitar seu uso quando necessário (BRASIL, 2022). Sendo toda essa política aplicável aos servidores, colaboradores, terceirizados, estagiários, fornecedores e todos que realizem atividades que envolvam, de

forma direta ou indireta, tratamento de dados pessoais custodiados pela própria ANS (BRASIL, 2022).

Além disso, deve-se considerar que o sistema de saúde brasileiro é híbrido, pois existe uma interação entre os serviços públicos e privados na prestação dos serviços de assistência à saúde, em que de um lado está o poder público, com rede própria e a conveniada do SUS, e de outro, o setor privado, que conta com a rede privada de serviços de assistência à saúde, inclusive, a prestação direta dos serviços por profissionais e outros estabelecimentos de saúde e a cobertura dos riscos de assistência à saúde pelas operadoras de planos de assistência à saúde (GREGORI, 2020).

Ressalta-se que a relação jurídica nos serviços de assistência à saúde, realizados por operadoras de planos de assistência à saúde e por prestadores de serviços de assistência à saúde, que prestam os serviços de saúde aos consumidores, é civil e comercial, sendo assim, essa relação deve observar às normas do Código Civil e da Lei 9.656/1998, no que couber (GREGORI, 2020).

Sobre os serviços de assistência à saúde suplementar, compreende-se que consumidores são os titulares de planos de saúde, seus dependentes, agregados, beneficiários, usuários, isso significa que são todos os que utilizam ou adquirem serviços de saúde, e o fornecedor, no caso as operadoras de planos de assistência à saúde, são as seguradoras e administradoras de benefícios de saúde, assim como outros estabelecimentos da rede de saúde (GREGORI, 2020). Desse modo, esta relação encontra-se amparada no Código de Defesa do Consumidor.

Já a Lei dos Planos de Saúde disciplina de forma específica as relações de consumo na saúde suplementar, sobre a cobertura assistencial, abrangência dos planos, rede credenciada, procedimentos e eventos cobertos e não cobertos, carências, doenças e lesões preexistentes, cláusulas contratuais, além de outras normas para as operadoras nesse mercado (GREGORI, 2020).

Nesse cenário, é preciso destacar que a ANS apresenta as funções de fiscalizar, regulamentar e monitorar o mercado de saúde suplementar no país, visando coibir práticas lesivas ao consumidor, incentivar comportamentos que reduzam os conflitos e promover a efetividade na prestação de serviços de saúde, é por essas funções que é possível existir um contexto de corregulação no país.

Um assunto que se tornou imprescindível no setor da saúde, é a proteção de dados, isso implica repensar as formas de acesso, tratamento, integração, portabilidade e segurança dos dados pessoais sensíveis dos titulares.

Isso deverá ser observado no mercado da saúde suplementar, para fins de elaboração de políticas públicas eficazes, para a adequada e eficaz prestação do serviço oferecido, tanto pela ANS, como pelas empresas que atuam neste setor, para que se permaneça prestando serviço de qualidade e adequados à legislação (GREGORI, 2020).

Recentemente, o Brasil enfrentou uma pandemia do Covid-19 e necessitou debater sobre a utilização de dados de georreferenciamento para o combate à pandemia da Covid-19 (BIONI; ZANATTA; MONTEIRO; RIELLI, 2020), assim como também a possibilidade de utilização de entes privados ou estatais sobre os dados pessoais, sem consentimento prévio dos titulares, para fins de políticas de combate à pandemia, sem colocar em risco a segurança, a coleta e o armazenamento dos dados. Isso demonstra que a Lei Geral de Proteção de Dados (LGPD) é importante no contexto de tratamento de dados pessoais relacionados à saúde pública e combate à pandemia.

O avanço tecnológico e a digitalização no setor da saúde promoveram transformações na prestação de serviços de saúde em clínicas, hospitais, laboratórios e outros do sistema de saúde no Brasil, principalmente, no período da pandemia de Covid-19 pela utilização da telemedicina.

Em meio às dificuldades no enfrentamento da pandemia do coronavírus, a telemedicina foi uma oportuna alternativa para atendimento de pacientes sem que houvesse a necessidade de locomoção, evitando-se a aglomeração em hospitais, clínicas e outros estabelecimentos de rede de saúde.

Isso porque as atividades da telemedicina "são muito similares às da medicina tradicional, tendo como diferença o fato de o profissional de saúde e o paciente estarem fisicamente distantes" (CNSAÚDE, 2021).

A Lei n. 13.989/20 que trata sobre a telemedicina durante o período da pandemia de Covid-19, também proporcionou o uso de receitas médicas digitais regulamentadas pela Resolução n. 2.299/21, que estabelece os requisitos mínimos de validade da receita e o uso de plataforma digital. Em 2022, a Lei n. 14.510/22 revogou a lei de telemedicina da pandemia (Lei n. 13.989/20) e passou a autorizar e disciplinar a prática de telessaúde no país.

A lei de telessaúde (Lei n. 14.510/22) em seu art. 26-A (BRASIL, 2022), permite a prestação remota de serviços a todas as profissões da área da saúde que são regulamentadas pelos órgãos competentes e estabelece alguns princípios, entre os quais podemos destacar, o consentimento livre e informado do paciente, a confidencialidade dos dados e a responsabilidade digital.

A telessaúde é definida como uma modalidade de prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação, utilizando uma transmissão segura de dados e informações de saúde, nos termos do art. 26-B da Lei de Telessaúde (BRASIL, 2022).

Deve-se ressaltar que a Lei da telessaúde determina que a sua prática seja realizada por meio de consentimento livre e esclarecido do paciente ou de seu representante legal, sob responsabilidade do profissional de saúde, assim como também em conformidade com o Marco Civil da Internet, Lei do Ato Médico, Lei Geral de Proteção de Dados, Código de Defesa do Consumidor e Lei do Prontuário Eletrônico.

Em relação ao consentimento do paciente no âmbito da telemedicina, Sanches e Giovanini ressaltam que:

> Sem prejuízo, cabe dizer que a lei da Telessaúde possui natureza de legislação geral, não excluindo, portanto, regulamentações emitidas por órgãos competentes, a exemplo da Resolução 2.314/22 do Conselho Federal de Medicina "CFM", que define como obrigatória a coleta de consentimento explícito do paciente para compartilhamento de informações de natureza pessoal no âmbito da telemedicina, salvo em caso de emergências médicas (art. 15 caput e parágrafo único da Resolução CFM 2.314/22) (SANCHES; GIOVANNI, 2023).

É necessário esclarecer que esse entendimento sobre a obrigatoriedade do consentimento do paciente no âmbito da telemedicina é controverso, uma vez que existem outras interpretações sobre esse aspecto e que merecem uma atenção na elaboração de boas práticas.

Essa dinamicidade da relação entre meio físico e o meio digital de dados de saúde é algo mais complexo e deve ser analisada de forma sistemática, isso significa que a interpretação da Lei da Telessaúde e demais regulamentações setoriais da saúde não devem ser feitas de forma isoladas, mas de modo coerente com todo ordenamento jurídico brasileiro.

Nota-se o esforço do legislador em dizer expressamente a Lei Geral de Proteção de Dados deverá ser observada, assim como também a Lei do Marco Civil da Internet, é inegável que essa disposição fortalece a aplicabilidade e o desenvolvimento de uma cultura de proteção de dados, mas mesmo que não fosse previsto na Lei de Telessaúde, não há dúvidas que ambas as legislações são aplicáveis nesses casos de dados relativos à saúde digital por meio da telessaúde.

Dentro desse contexto, a utilização dos Prontuários Eletrônicos do Paciente está definido e regulamentado na Resolução 1.821/2007 (BRASIL, 2007) que trata sobre a

digitalização e uso de sistemas informatizados para fins de guarda e manuseio dos documentos dos prontuários dos pacientes e os níveis de segurança que devem ser adotados.

Sendo assim, existe uma regulamentação sobre a telessaúde no Brasil, que deverá ser interpretada em consonância com outras leis e regulamentações do ordenamento jurídico, mas em relação às recomendações e boas práticas empresariais acerca do tratamento de dados pessoais sensíveis na telemedicina será objeto do próximo tópico.

3- Análise das Boas Práticas no Tratamento de Dados Pessoais Sensíveis no Setor de Saúde no Uso da Telessaúde

No setor da saúde já existiam práticas de sigilo na relação de médico-paciente, em relação a resultados e análise de exames e outras atividades relativas à saúde do paciente. A partir da entrada em vigor da LGPD, o crescimento tecnológico e o avanço na telemedicina na pandemia ficaram evidente a necessidade de novas boas práticas que sejam condizentes com essa realidade e com a própria LGPD.

Essas orientações e *guidelines* precisam levar em consideração as particularidades regulatórias da proteção de dados no Brasil para dados pessoais sensíveis. Isso porque é necessário prevenir situações de acessos não autorizados aos dados, acidentes e/ou vazamentos de dados, assim como também a perda, alteração ou qualquer incidente ou tratamento de dados em desacordo com a LGPD.

Além disso, o desenvolvimento de boas práticas precisa observar os princípios elencados na LGPD, pois a dinâmica e a operacionalização efetiva da proteção de dados passa pelos princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018).

Apesar deste tópico buscar as boas práticas relacionadas a telessaúde, observa-se um cenário ainda muito incipiente, ou seja, ainda não possui práticas de proteção de dados específicas e exclusivas para a telessaúde após o surgimento da lei que fez a sua regulamentação. Isso significa que ainda é necessária uma construção de boas práticas específicas para a telessaúde, mas que por enquanto é importante considerar as boas práticas já existentes para a área da saúde em sentido amplo.

Existem algumas recomendações de boas práticas feitas sobre a telemedicina, mas que não foram feitas com base na lei de telessaúde. Na relação entre o médico, rede de saúde e as empresas de tecnologia, pode-se destacar as seguintes práticas:

> O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados.
> [...]recomenda-se que sejam implementadas medidas de controle de acesso aos documentos, para garantir que apenas pessoas autorizadas possam acessar as informações. Além disso, sugere-se que sejam adotados sistemas de rastreamento das atividades realizadas com os dados (modificações, cópia, compartilhamento, etc...) e a implementação de um sistema de validação de transferência de arquivos.
> [...]Lidar com dados de saúde que requerem proteção especial requer uma infraestrutura segura que deve impedir o acesso de terceiros. [...] Além disso, ao transmitir resultados de exames ou quadros clínicos ao interessado, deve-se garantir que a pessoa que recebe as informações é realmente o paciente ou o seu representante e, portanto, tem o direito de receber tais informações (CNSAÚDE, 2021, p.68-71).

Além disso, algumas recomendações de boas práticas foram feitas por Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), Intervozes – Coletivo Brasil de Comunicação Social e Instituto Brasileiro de Defesa do Consumidor (Idec) que estudaram, elencaram e publicaram:

> • Apresentar a informação sobre coleta, uso e tratamento dos dados pessoais dos/as usuários/as de forma amigável.
> • "Resumir" a política de privacidade ou apresentar informações sobre tratamento de dados de forma facilitada.
> • Disponibilizar informações em linguagem simples e acessível.
> • Ser transparente quanto à possibilidade de realizar inferências a partir dos dados, mesmo que as inferências em si não sejam divulgadas em sua integridade.
> • Quando houver diferentes formas de usabilidade listar todas as políticas em um mesmo lugar e oferecer hyperlinks para que sejam acessadas.
> • Embora não seja uma obrigação explícita da LGPD, considera-se uma boa prática divulgar informações sobre as bases legais utilizadas para uso dos dados, especialmente quando há dados sensíveis envolvidos.
> • Explicitar para as finalidades listadas se há diferenciação do que se aplica a dados sensíveis e a dados pessoais triviais.
> • Informar sobre possíveis usos posteriores dos dados para pesquisa (mesmo quando agregados).
> • Seria importante que órgãos públicos procurassem demonstrar com maior nitidez seus processos internos quanto à seleção de dados para pesquisas e seus testes de necessidade dos dados (Icict/Fiocruz, 2022, p.37).

O Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), Intervozes – Coletivo Brasil de Comunicação Social e Instituto Brasileiro de Defesa do Consumidor (Idec) fizeram mais algumas recomendações:

> • Fornecer mais informações, mesmo que não seja na política de privacidade, sobre as possibilidades de marketing e quais tipos de dados são tratados para o direcionamento de anúncios e/ou outras formas de propaganda e/ou comunicação com o/a usuário/a que não tenha relação direta com a prestação do serviço.
> • No caso de empresas e agentes públicos que utilizam serviços de nuvem de terceiro, é importante que indiquem qual é o provedor, já que diferentes provedores de nuvem terão especificações de seguranças distintas, de maneira que é possível ter uma ideia mais detalhada das condições de segurança.

> • Explicitar como o titular dos dados poderia não mais compartilhar os seus dados e revogar seu consentimento e oferecer processos simplificados para que isso ocorra.
> • Informar sobre o tempo de guarda dos dados, por quem e como. (Icict/Fiocruz, 2022, p.37)

Essas boas práticas sintetizam um estudo complexo e aplicável ao âmbito da saúde, inclusive, aplicável a própria telemedicina, em que se pode destacar:

> Nesse sentido, como destacado no Inventário de Tecnologias Digitais da Informação e da Comunicação que coletam dados pessoais sensíveis em serviços de Saúde Digital, os serviços de saúde digitais oferecem mecanismos considerados pouco transparentes para os/as usuários/ as e, sobretudo, baseados em noções de consentimento bastante frágeis tendo em vista a complexidade do mercado de dados e das interações existentes entre tecnologias, governos e grandes corporações. Icict/Fiocruz, 2022, p.41)

As mesmas instituições mencionaram no estudo algumas boas práticas para a Autoridade Nacional de Proteção de Dados:

> • Que a Autoridade Nacional de Proteção de Dados, instituições de pesquisa, órgãos públicos e demais envolvidos possam discutir parâmetros eficientes para a anonimização em casos diversos.
> • Que a ANPD, em diálogo com entidades reguladoras de saúde, defina de forma explícita o que é serviço de saúde, uma vez que ser serviço de saúde ou não pode determinar mais ou menos liberdade ou possibilidade de tratamento de dados. Icict/Fiocruz, 2022, p.41)

Ao nível internacional, Oliveira (2022) destaca que a *Health Insurance Portability and Accountability Act (HIPAA)* tem o objetivo a redução de fraudes ou abusos na assistência à saúde, estabelecendo requisitos para garantias de portabilidade, confidencialidade, segurança, transferência, manuseio e compartilhamento de dados, dividindo-se em aspectos de segurança (confidencialidade, integridade e disponibilidade) e de privacidade para fins de limites de uso e acesso aos dados.

Além disso, é importante observar os oito princípios de Caldicott da Inglaterra de 2020, pois visam garantir que as informações das pessoas sejam utilizadas em sigilo e adequadamente, contribuindo com a prestação de saúde, são eles:

> Princípio 1: Justifique o(s) propósito(s) para usar informações confidenciais"; Princípio 2: Use informações confidenciais somente quando necessário; Princípio 3: Use o mínimo necessário de informações confidenciais; Princípio 4: O acesso a informações confidenciais deve ser estritamente necessário; Princípio 5: Todos com acesso a informações confidenciais devem estar cientes de suas responsabilidades; Princípio 6: Cumprir a lei; Princípio 7: O dever de compartilhar informações para atendimento individual é tão importante quanto o dever de proteger a confidencialidade do paciente; Princípio 8: Informar pacientes e usuários de serviços sobre como suas informações confidenciais são usadas (GUARDIAN, 2020).

Desse modo, observa-se que a telessaúde é uma regulamentação recente e que precisa de um aprofundamento sobre boas práticas mais robustas, de forma positiva nota-se que já é pauta de estudos para fins de desenvolvimento de boas práticas de proteção de dados que possibilitem efetividade aos direitos e deveres estabelecidos na LGPD e o avanço da telessaúde de forma segura no país.

Por fim, a proteção de dados ainda é desafiadora para o setor da saúde, pois ainda necessita de estudo para ser desenvolvida para a realidade brasileira, para minimizar riscos, vulnerabilidades e inconsistências na privacidade e proteção dos dados na telessaúde.

Considerações finais

A partir do que foi exposto percebe-se a a complexidade do processo de adequação à Lei Geral de Proteção de Dados de agentes de tratamentos de dados pessoais na área da saúde, inclusive, especialmente no que tange as atividades de telessaúde no país.

É importante que haja um diálogo entre os órgãos responsáveis pelo setor da saúde com a Autoridade Nacional de Proteção de Dados, para fins de definição de parâmetros compatíveis com a realidade brasileira e a LGPD, evitando-se distorções e inconsistências nas regulamentações e definições de boas práticas.

É dever de todos os envolvidos com o tratamento de dados pessoais, em especial o tratamento de dados pessoais sensíveis na telessaúde garantir a proteção e segurança dos dados aos quais dão tratamento em meio digital. Ressaltando que a junção de medidas técnicas, processo definidos e pessoas orientadas e educadas em relação a proteção de dados, são capazes de predizer comportamentos fundamentais para a construção de uma Cultura de Proteção de Dados baseada em aspectos reais e que coloquem os/as cidadãos/ãs em condição de garantir a proteção dos seus dados no campo da saúde, preservando assim, de forma concreta, seus direitos fundamentais.

Para atingir a excelência em relação aos cuidados e segurança com referidos dados de saúde, necessário se faz estabelecer boas práticas, bem como a fiscalização do compartilhamento entre empresas parceiras (*due diligence*), prestadores de serviços, para que estas também estabeleçam o mesmo rigor.

Por fim, a pesquisa conclui que existem boas práticas em proteção de dados relativas ao setor da saúde, mas que ainda precisa ser aprimorada e desenvolvida para o cenário brasileiro e que sejam elaborados protocolos juntamente com a Autoridade Nacional de Proteção de

Dados, com o fim de minimizar riscos, vulnerabilidades e inconsistências na privacidade e proteção dos dados na telessaúde.

Assim, considerando a complexidade do sistema de saúde no Brasil, é importante ter um olhar reflexivo sobre as boas práticas, no âmbito internacional, que orientam o uso adequado de dados relativos a prestação de saúde, como os oitos princípios de Caldicott, e que podem contribuir no desenvolvimento destas práticas no país.

Referências Bibliográficas

BRASIL. Constituição (1988). **Constituição Federal de 1988**. Brasil, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2023.

BRASIL. **Lei do Marco Civil da Internet nº 12.965, de 23 de abril de 2014**. Brasil, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 maio 2023.

BRASIL. **Lei Geral de Proteção de Dados nº 13.709**, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 abr. 2023.

BRASIL. **Lei da Telessaúde nº 14.510**, de 27 de dezembro de 2022. . Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm#:~:text=LEI%20N%C2%BA%2014.510%2C%20DE%2027,15%20de%20abril%20de%202020.. Acesso em: 22 abr. 2023.

BRASIL. **Lei nº 13.989**, de 15 de abril de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13989.htm#:~:text=Art.,emergencial%2C%20o%20uso%20da%20telemedicina. Acesso em: 15 maio 2023.

BRASIL. Resolução Administrativa nº 80, de 28 de junho de 2022. **ANS**. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2022/res0080_30_06_2022.html. Acesso em: 15 abr. 2023.

BRASIL. **Resolução CFM nº 1.821**, de 11 de julho de 2007. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-cfm-no-1-821-de-11-de-julho-de-2007#:~:text=Aprova%20as%20normas%20t%C3%A9cnicas%20concernentes,de%20informa%C3%A7%C3%A3o%20identificada%20em%20sa%C3%BAde.. Acesso em: 15 maio 2023.

BIONI, B.; ZANATTA, R.; MONTEIRO, R.; RIELLI, M. **Privacidade e pandemia**: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020. Disponível em https://www.dataprivacybr.org/wp-content/uploads/2020/04/Relatorio-Privacidade-e-Pandemi-a-Data-Privacy-Brasil-2.pdf. Acesso em: 10 maio 2023.

CNSAÚDE. **Código de Boas Práticas**: proteção de dados para prestadores privados em saúde. Proteção de Dados para Prestadores Privados em Saúde. 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 22 abr. 2023.

DONEDA, Danilo. Panorama histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021.

Emenda Constitucional 115/2022. **Constituição Federal de 1988**. Brasil, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2023.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de Dados. In: **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coordenadores). São Paulo: Thomson Reuters Brasil, 2019.

GUARDIAN, National Data. **The Eight Caldicott Principles**. 2020. Disponível em: https://www.gov.uk/government/publications/the-caldicott-principles. Acesso em: 04 jun. 2023.

GREGORI, Maria Stella. OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA SAÚDE SUPLEMENTAR. **Thomson Reuters,** [s. l], p. 171-196, 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/rdc-maria-stella.pdf. Acesso em: 23 abr. 2023.

Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), Intervozes – Coletivo Brasil de Comunicação Social e Instituto Brasileiro de Defesa do Consumidor (Idec). **RESUMO EXECUTIVO Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil**. Outubro de 2022. Disponível em: https://intervozes.org.br/wp-content/uploads/2022/11/resumo_executivo_protecao_de_dados_pessoais.pdf . Acesso em: 04.maio.2023

Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), Intervozes – Coletivo Brasil de Comunicação Social e Instituto Brasileiro de Defesa do Consumidor (Idec). **RESUMO EXECUTIVO Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil**. Março de 2023. Disponível em: https://intervozes.org.br/wp-content/uploads/2022/11/Resumo-Executivo-Saude-e-Dados-2023.pdf . Acesso em: 02.maio.2023.

OLIVEIRA, Diogo Luís Manganelli. **Telemedicina no Brasil**: ameaças à proteção de dados pessoais em decorrência da flexibilização da pandemia e da regulamentação precária. Revista De Direito Sanitário, 2022. Disponível em: https://www.revistas.usp.br/rdisan/article/view/176159 . Acesso em: 02.maio.2023.

SANCHES, Pedro; GIOVANNI, Carolina. **A telessaúde no Brasil: Quais os desafios para a proteção de dados pessoais?** 2023. Disponível em: https://www.migalhas.com.br/depeso/379831/a-telessaude-no-brasil. Acesso em: 22 abr. 2023.