RESPONSABILIDADE ÉTICA-PROFISSIONAL DOS MÉDICOS SOBRE O TRATAMENTO DE DADOS NA PRÁTICA DA TELEMEDICINA

LAVRAS - MG

2023

MARIA DE LOURDES CANÇADO BARCELOS

RESPONSABILIDADE ÉTICA-PROFISSIONAL DOS MÉDICOS SOBRE O TRATAMENTO DE DADOS NA PRÁTICA DA TELEMEDICINA

Artigo científico apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Direito para a obtenção do título de Bacharel.

Prof. Dr. Sthéfano Bruno Divino Santos
Orientador

LAVRAS - MG
2023

RESUMO

A telemedicina é uma prática de atendimento à distância que utiliza recursos de tecnologia e comunicação para fornecer diagnóstico, tratamentos e troca de informações médicas. No Brasil, sua regulamentação teve um desenvolvimento gradual, culminando com a atual Resolução nº 2.314/2022 do Conselho Federal de Medicina (CFM), que define e regulamenta a telemedicina como prestação de serviços médicos por meio de Tecnologias de Informação e Comunicação (TICs). Contudo, essa normativa não aborda a responsabilização ético-profissional por vazamento de dados sensíveis durante o atendimento. Há uma cadeia de agentes envolvidos no tratamento dos dados, incluindo médicos, clínicas e terceiros contratados, mas a falta de clareza na legislação dificulta a definição de responsabilidades em caso de incidentes. O presente estudo ressalta a importância de garantir a segurança dos dados dos pacientes, tanto sob a Lei Geral de Proteção de Dados quanto sob as regulamentações do CFM e busca entender como os princípios éticos e do sigilo profissional se aplicam à telemedicina, bem como as sanções disciplinares que podem ser aplicadas aos médicos em caso de vazamento de dados. Em suma, a responsabilização por vazamento de dados varia de acordo com a função exercida por cada pessoa na relação médico-paciente e seu envolvimento no incidente de segurança, de modo que é necessário esclarecer e definir claramente as responsabilidades de todos os agentes envolvidos para garantir uma telemedicina ética e segura.

Palavras-chave: Proteção de Dados. Direito Digital. Direito à Saúde. Telemedicina.

ABSTRACT

Telemedicine is a practice of remote care that utilizes technology resources to provide medical diagnosis, treatments, and exchange of medical information. In Brazil, its regulation has undergone gradual development, culminating in the current Resolution nº 2.314/2022 of the Federal Council of Medicine (CFM), which defines and regulates telemedicine as the provision of medical services through Information and Communication Technologies (ICTs). However, this regulation does not address the ethical-professional accountability for sensitive data leakage during the care process. There is a chain of agents involved in data treatment, including physicians, clinics, and contracted third parties, but the lack of clarity in the legislation hinders the definition of responsibilities in case of incidents. This study highlights the importance of ensuring the security of patient data, both under the General Data Protection Law and CFM regulations, and seeks to understand how ethical and professional secrecy principles apply to telemedicine, as well as the disciplinary sanctions that can be applied to physicians in case of data leakage. In short, accountability for data leakage varies according to the role each person plays in the doctor-patient relationship and their involvement in the security incident, so it is necessary to clarify and clearly define the responsibilities of all parties involved to ensure an ethical and safe telemedicine practice.

Keywords: Data protection. Digital Law. Health Law. Telemedicine.

SUMÁRIO

1. Introdução.

A telemedicina[1] enquanto prática de atendimento à distância tem sido aplicada em diferentes contextos e sua utilização por médicos envolve diferentes recursos de tecnologia e comunicação para atender e beneficiar seus pacientes, seja por meio da troca de informação entre as equipes médicas, seja como forma de contatar pacientes e auxiliá-los por uma comunicação virtual. Nesse contexto, essa prática pode ser definida como o exercício de atividades médicas à distância, com o objetivo de propagar a informação, fornecer diagnóstico e indicar tratamentos a pacientes, utilizando dados, informações e documentos que são transmitidos por meio de recursos da telecomunicação (FRANÇA, 2020, p. 221).

Isso posto, é importante ressaltar que a aplicação da telemedicina está sujeita a regulamentações específicas de cada país ou jurisdição. No caso do Brasil, a primeira norma do Conselho Federal de Medicina sobre o assunto foi a Resolução CFM n.º 1.643/2002[2], que considerava o uso de métodos interativos de comunicação audiovisual e dados apenas para as finalidades de assistência, educação e pesquisa em Saúde, sem definir exatamente quais atividades poderiam ser realizadas. Nesse sentido, o desenvolvimento gradual de normativas favoráveis à telemedicina começou apenas em 2011, quando foi permitido o uso ampliado do contato telefônico para dúvidas e orientações, atrelado à posterior normatização do telediagnóstico em 2014 (SCHMITZ, GONÇALVES E UMPIERRE, 2020).

A atual Resolução nº 2.314/2022 do Conselho Federal de Medicina (CFM) define e regulamenta a Telemedicina como forma de prestação de serviços médicos mediados por Tecnologias de Informação e Comunicação (TIC's). De modo geral, o art. 3°, §7° da referida normativa determina que "os dados pessoais e clínicos do teleatendimento médico devem seguir as definições da LGPD e outros dispositivos legais, quanto às finalidades primárias dos dados". Em outros termos, a responsabilidade jurídica e por danos civis aparentemente tem o condão de atrair a Lei Geral de Proteção de Dados e seu indefinido regime de responsabilização (se subjetivo, objetivo ou misto/sui generis).

Contudo, o respectivo normativo não dispõe ou menciona sobre a responsabilização ético-profissional por vazamento de dados, sejam eles sensíveis ou não, perante o próprio Conselho Federal de Medicina. Além disso, durante a execução deste serviço existem múltiplos

[1] A telemedicina refere-se à prestação de serviços médicos à distância, por meio de tecnologias de comunicação e informação, o que envolve a realização de consultas, diagnósticos, monitoramento de pacientes e outras atividades relacionadas à saúde, utilizando recursos como videoconferências, plataformas online e dispositivos médicos conectados.

[2] CONSELHO FEDERAL DE MEDICINA (Brasil). **Resolução nº 1.643**. [S. l.], 2002.

agentes diretamente inseridos em uma cadeia de coleta e tratamento de dados, sejam eles: o médico responsável pelo atendimento; a clínica médica enquanto pessoa jurídica; bem como eventuais tomadores de serviços contratados cuja função é a guarda e o compartilhamento desses dados.

Nesse contexto, verifica-se que na Resolução n. 2.314/2022 há omissões sobre quem pode ser indicado como agente responsável por eventual ato ilícito caracterizado mediante vazamento de dados no curso da Telemedicina[3], bem como faltam esclarecimentos sobre a possibilidade de responsabilização dos médicos e quais as sanções éticas aplicáveis caso ocorra algum incidente de vazamento de dados de seus pacientes durante a prática da medicina mediada por tecnologias digitais de informação e comunicação.

Disso tudo, surge o questionamento: qual(is) agente(s) deve(m) ser responsabilizados pelo vazamento de dados coletados e tratados durante o procedimento da Telemedicina e quais são as sanções éticas e jurídicas cabíveis?

O presente estudo pretende destacar a importância da segurança da informação e assegurar que os dados sensíveis dos pacientes sejam tratados de maneira segura, tanto sob a base legal da Lei Geral de Proteção de Dados, quanto sob a base normativa disciplinar das regulamentações do Conselho Federal de Medicina. Contudo, há desafios sobre a falta de clareza na legislação quanto às responsabilidades dos agentes envolvidos na proteção e arquivamento seguro dos dados.

A metodologia utilizada na análise se pautou na pesquisa documental sobre a intersecção entre normas do conselho de classe e proteção de dados para entender como os princípios da ética e do sigilo profissional são aplicáveis à telemedicina, atrelada à pesquisa bibliográfica sobre as disposições normativas pertinentes, com enfoque na responsabilização ético profissional de médicos na prática da Telemedicina e na aplicação de sanções disciplinares. Disso tudo, foi utilizada pesquisa bibliográfica e documental para a metodologia exploratória, de modo que primeiro foi buscado a contextualização fática, seguida da identificação do regime jurídico aplicável e sua problematização, passando pela reflexão sobre as informações encontradas. Por fim, foi feita uma análise crítica em que foi verificada que a responsabilização varia de acordo com função que cada pessoa exerce na relação médico-paciente, bem como seu envolvimento no incidente de segurança.

---

[3] Art. 5º A telemedicina pode ser exercida nas seguintes modalidades de teleatendimentos médicos: I) Teleconsulta; II) Teleinterconsulta; III) Telediagnóstico; IV) Telecirurgia; V) Telemonitoramento ou televigilância; VI) Teletriagem; VII) Teleconsultoria.

2. Telemedicina e Dados Pessoais Sensíveis:

Com a Resolução CFM n.º 1.643/2002[4], a regulamentação de consultas remotas começou a ganhar destaque, o que foi acentuado a partir da Resolução CFM nº 2.227/2018[5] que falava sobre a prestação de serviços médicos mediados por tecnologias. No entanto, a normativa do Conselho Federal de Medicina promulgada em 2018 permaneceu vigente por pouco tempo e foi revogada em 2019, com determinação do conselho profissional que restabeleceu a vigência da Resolução n.º 1.643/2002 (SCHMITZ et al, 2020). Posteriormente, durante a pandemia do coronavírus, foi promulgada a Lei 13.989/2020[6] que, apesar de não estabelecer diretrizes claras para utilização de meios remotos para consultas médicas, conceituou telemedicina como "o exercício da medicina mediado por tecnologias interativas para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde" (MARTINS e TELES, 2021).

Nesse cenário, em todas as modalidades de serviço médico prestado por meios digitais, a relação entre os dados[7], tecnologias e atividade médica deve ser pautada pela tutela de proteção das informações pessoais, prezando pela veracidade de dados, acessibilidade controlada, concordância do paciente ou seus representantes e utilização apenas para a finalidade direcionada. Disso tudo, a principal preocupação quanto aos dados pessoais, diz respeito à utilização das informações como mercadoria na internet, o que deve ser absolutamente vedado na prática da telemedicina (FELIX e MONTEIRO, 2022). Logo, é preciso compreender qual a base legal da telemedicina, com foco em garantir a confidencialidade necessária para sua prática, entendendo quais dados são coletados na prática médica e os riscos da coleta realizada de maneira indevida.

Isso posto, durante as consultas podem ser coletados diferentes tipos de informações, o que deve ocorrer de acordo com as regulamentações e diretrizes éticas aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) e os princípios de privacidade e confidencialidade médica previstos no Código de Ética Médica[8]. Alguns exemplos de dados que podem ser coletados

---

[4] CONSELHO FEDERAL DE MEDICINA (Brasil). **Resolução nº 1.643**. [S. l.], 2002.

[5] CONSELHO FEDERAL DE MEDICINA (Brasil). **Resolução nº 2.227**. [S. l.], 2018.

[6] BRASIL. **Lei nº 13.989**, de 15 de abril de 2020. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). [S. l.], 2002. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328. Acesso em: 25 jun. 2023.

[7] Segundo Danilo Doneda, em seu artigo intulado A Proteção dos Dados Pessoais Como Um Direito Fundamental, o "dado" está associado a uma espécie de "pré-informação", anterior ao processo interpretativo, já "informação", vai além da representação contida no dado, considerando que já aborda o viés interpretativo, sobre a redução do estado de incerteza.

[8] CONSELHO FEDERAL DE MEDICINA (Brasil). ***Código de ética médica***. Resolução nº 2.217. [S. l.], 2017.

durante as consultas no registro do prontuário eletrônico, conforme as Resoluções CFM nº 1.638/2002 e nº 1.821/2007 incluem:

I. Dados de identificação: Nome completo, data de nascimento, número de identificação (como CPF ou RG), informações de contato (endereço, telefone, e-mail) e outras informações pessoais necessárias para identificação e comunicação.

II. Histórico médico: Informações sobre condições médicas anteriores, histórico de doenças, cirurgias, alergias, medicamentos em uso, resultados de exames anteriores e tratamentos médicos prévios.

III. Sintomas e queixas atuais do paciente: Descrição dos sintomas, duração, intensidade e fatores relacionados, com o objetivo de auxiliar no diagnóstico e tratamento.

IV. Exames físicos: Dados obtidos durante o exame físico, como pressão arterial, frequência cardíaca, temperatura corporal, avaliação de órgãos e sistemas, entre outros.

V. Dados de imagem e laboratoriais: Resultados de exames de imagem (como radiografias, tomografias) e exames laboratoriais (como análises de sangue, urina) que possam ser relevantes para avaliação e diagnóstico.

Neste contexto destaca-se que, de acordo com o artigo 5º, incisos I, II e III da Lei Geral de Proteção de Dados (LGPD)[9], são fornecidos conceitos para dados pessoais, dados pessoais sensíveis e dados anônimos. De acordo com a referida lei, os dados pessoais são definidos como informações relacionadas a uma pessoa física identificada ou identificável, já os dados pessoais sensíveis são aqueles que contém informações que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relacionados à saúde ou à vida sexual, bem como dados genéticos ou biométricos, quando relacionados a uma pessoa física. Por fim, os dados anônimos são aqueles que se referem a um titular que não pode ser identificado.

Ademais, de acordo com o entendimento de Schmitz, Gonçalves e Umpierre[10], em uma consulta remota, todos os dados pessoais utilizados são considerados dados pessoais sensíveis.

---

[9] BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2023.

[10] SCHMITZ, Carlos A A.; GONÇALVES, Marcelo R.; UMPIERRE, Roberto N.; et al. **Consulta Remota**: Fundamentos e Prática. Grupo A, 2020. E-book. ISBN 9786558820031. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786558820031/. Acesso em: 06 jul. 2023.

Logo, é importante que os dados coletados durante as consultas sejam armazenados e tratados de forma segura e confidencial, em conformidade com as regulamentações de proteção de dados, incluindo o consentimento informado do paciente sobre a coleta e o uso dos dados. Assim, os profissionais de saúde que trabalham com telemedicina devem estar cientes das responsabilidades e obrigações legais envolvidas no tratamento desses dados e assegurar o consentimento informado dos pacientes para a utilização dessas informações sensíveis durante a consulta remota (SCHMITZ, GONÇALVES E UMPIERRE, 2020).

Contudo, as normativas do Conselho Federal de Medicina não esclarecem a responsabilização ético-profissional perante o próprio CFM por vazamento de dados. Além disso, ressalta-se que durante a execução deste serviço existem múltiplos agentes diretamente inseridos em uma cadeia de coleta e tratamento de dados, sejam eles: o médico responsável pelo atendimento; a clínica médica enquanto pessoa jurídica ou seus administradores; bem como eventuais tomadores de serviços contratados cuja função é a guarda e o compartilhamento desses dados.

Mesmo havendo diferentes agentes de tratamento, a guarda e o tratamento de dados devem ser realizados da maneira mais segura possível, considerando os diversos casos de vazamento de dados ocorridos em empresas privadas e em bancos de dados do próprio Governo Federal. A título de exemplo, antes de a Lei Geral de Proteção de Dados entrar em vigor ocorreu o incidente de segurança com informações de clientes da Netshoes em 2018[11]. Neste caso, o acesso não autorizado a um banco de dados da empresa comprometeu informações pessoais de clientes, como nomes, endereços, CPFs, e-mails, telefones e senhas criptografadas, consequentemente, foram levantadas preocupações sobre a segurança e a proteção das informações pessoais no comércio eletrônico. De acordo com informações divulgadas Jornal Estado de Minas[12], o incidente foi constatado pelo Ministério Público e a empresa tomou medidas imediatas para investigar o incidente, corrigir as vulnerabilidades de segurança e notificar os clientes afetados sobre o vazamento.

[11] NETSHOES terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes: Valor de indenização foi firmado em acordo com Ministério Público do DF. Incidente comprometeu dados pessoais de servidores da Presidência, da Polícia Federal e do STF. **G1 Distrito Federal**, 5 fev. 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml. Acesso em: 5 jul. 2023.

[12] NETSHOES deverá avisar 2 milhões de clientes sobre vazamento de dados: Vazamento de dados pessoais, entre eles o CPF, comprometem segurança de clientes do site. Ministério Público pede que empresa avise os afetados. **Estado de Minas**, 26 jan. 2018. Economia. Disponível em: https://www.em.com.br/app/noticia/economia/2018/01/26/internas_economia,933890/netshoes-devera-avisar-2-milhoes-de-clientes-sobre-vazamento-de-dados.shtml. Acesso em: 5 jul. 2023.

Há que se falar também no megavazamento ocorrido em 2021, posteriormente ao início da vigência da LGPD, da plataforma Hariexpress[13], que é uma plataforma brasileira utilizada por varejistas para monitoramento de e-commerce. Neste caso, a Hariexpress armazenava informações em seu servidor "ElasticSearch" sem aplicar criptografia para proteção. Em outras palavras, não havia uma senha ou qualquer forma de segurança para limitar o acesso aos dados dos consumidores finais e dos vendedores tanto de pequenas lojas quanto de grandes empresas como Mercado Livre, Magazine Luiza, Shopee e Amazon[14].

Disso tudo, o setor público também não fica livre de incidentes de segurança, considerando que já ocorreram vazamentos de dados do Sistema Único de Saúde (SUS) e do Ministério da Economia[15]. No caso do SUS, foi encaminhada à Polícia Federal uma denúncia sobre vazamento de dados pessoais de terceiros obtidos pelo Banco de Dados do SUS, considerando o crime previsto na lei de crimes cibernéticos. Já no caso do Ministério da Economia, o vazamento de dados foi identificado pela empresa de cibersegurança Group-IB, e constatou que servidor do Ministério da Economia apresentava uma falha de segurança, expondo informações pessoais de mais de 20 mil brasileiros, incluindo RGs e selfies de identificação[16]. A descoberta ocorreu em janeiro de 2021 e foi divulgada em um relatório de inteligência, revelando que o servidor estava exposto há pelo menos dois meses antes da publicação do relatório.

Não obstante, segundo Nota Técnica da Autoridade Nacional de Proteção de Dados (ANPD)[17] em 2023 ocorreu a fiscalização de farmácias e drogarias por coleta excessiva de

---

[13] PANCINI, Laura. Hariexpress, entenda o que pode acontecer com envolvidos em megavazamento: 1,7 bilhão de dados sensíveis de brasileiros foram vazados da plataforma Hariexpress, que tem parceria com gigantes como Mercado Livre, Magazine Luiza, Shopee e até os Correios. **Exame**, 23 out. 2021. Disponível em: https://exame.com/tecnologia/entenda-caso-hariexpress-megavazamento/. Acesso em: 25 jun. 2023.

[14] BRANDÃO, Raquel. Plataforma vaza 1,75 bilhão de dados de clientes de marketplaces e Correios: Prestadora de serviços para vendedores no Magazine Luiza, Mercado Livre, Shopee, Amazon e Americanas afirmou estar "apurando o ocorrido para corrigir as falhas expostas". **Valor Investe**, São Paulo, 13 out. 2021. Empresas. Disponível em: https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/10/13/plataforma-vaza-175-bilhao-de-dados-de-clientes-de-marketplaces-e-correios.ghtml. Acesso em: 2 jul. 2023.

[15] Segundo Reportagem publicada pela EPSJV/Fiocruz em 03 dez. 2020: "O jornal O Estado de São Paulo publicou reportagens denunciando dois casos de vazamentos de dados que jogaram luz sobre as brechas existentes na governança dos dados pessoais dos usuários do Sistema Único de Saúde (SUS) e sobre o risco de que elas sejam exploradas para fins comerciais."

[16] Conforme reportagem de Aryel Fernandes para a Istoé Dinheiro em 16 jun. 2022: "A empresa de cibersegurança Group-IB, que tem parceria com órgãos de investigação como a Interpol, divulgou uma falha no servidor do Ministério da Economia. Pelo problema, os RGs e selfies de identificação de mais de 20 mil brasileiros estavam expostos na internet."

[17] Conforme Nota Técnica nº 4/2023/CGTP/ANPD: "Diante dessa análise, por meio de solicitação do Conselho Diretor (18ª Reunião, em 05 de maio de 2021), elaborou-se estudo (Relatório Farmácias MPDFT 01/06/2021) em que as informações obtidas foram detalhadas. Posteriormente, analisaram-se políticas de privacidade desses e de

informações dos clientes atrelada ao repasse de informações a terceiros sem a ciência do titular. Apesar de não ter sido partilhado o nome das redes de farmácias e drogarias envolvidas na fiscalização, sabe-se que a investigação está verificando o vazamento de históricos de compras, que facilmente poderiam ser ligados à utilização de medicação e prescrições, o que torna os dados vazados identificáveis e sensíveis por serem vinculados a questões de saúde pelo histórico de compras de medicamentos pelos pacientes.

Disso tudo, ainda é importante mencionar que incidentes de segurança não se limitam apenas a empresas nacionais, uma vez que mesmo em organizações estrangeiras, medidas de proteção insuficientes podem expor dados valiosos. É fundamental que as empresas adotem medidas robustas de segurança cibernética para garantir a privacidade e a proteção adequada das informações dos usuários, minimizando assim os riscos de vazamentos e preservando a confiança dos proprietários dos dados. Deste modo, sabendo sobre a existência de incidentes de segurança e quais dados devem ser coletados na telemedicina, constata-se o cuidado necessário com dados da saúde e a atenção requerida para que a coleta e tratamento seja feita de maneira a resguardar o paciente.

3. Dado Pessoais: Necessidades e maneiras de coleta

A coleta adequada de dados pessoais na telemedicina desempenha um papel fundamental na garantia da privacidade e segurança dos pacientes, além de proporcionar um atendimento eficiente. Isso posto, é necessário entender qual é a maneira correta de armazenar e tratar os dados e informações coletados, considerando que eventual incidente de segurança na telemedicina pode gerar danos aos pacientes, e, como consequência, um mau resultado decorrente desta forma de prestação de serviço médico. Nesse contexto, segundo Genival França (2020), a utilização da Telemedicina por médico, mesmo que em benefício e por solicitação do paciente, não exime o profissional da responsabilidade sobre os resultados ruins decorrentes da Telemedicina. Consequentemente, o médico poderá ser responsabilizado por não exercer a profissão de acordo com os princípios e regras de atuação profissional.

outros grupos farmacêuticos de maior abrangência territorial e em termos de número de clientes, com o objetivo de verificar sua atualização e adequação ao regime de privacidade e proteção de dados instaurado pela LGPD, desde sua entrada em vigor.”

Conforme apresentado acima, percebe-se que incidentes de segurança cibernética são acontecimentos comuns em plataformas digitais[18], mesmo com os procedimentos de segurança existentes. No contexto de serviços de saúde em meios digitais, destaca-se o posicionamento de Veloso de França (2020, p. 61) que afirma que "o aumento da capacidade de armazenamento de dados e o sistema de telecomunicações já estão revolucionando a forma de prestar serviços de saúde." Consequentemente, o avanço dos meios tecnológicos está caminhando para transformar a área da saúde em uma indústria da informação, no sentido de um sistema amplo para tratamento inteligente de uma série de dados. Logo, a proteção de dados de pacientes é uma preocupação que deve ser amplamente discutida no campo da saúde digital, considerando a crescente adoção da telemedicina. (FRANÇA, 2020, p. 61).

Mesmo que a telemedicina entregue uma forma mais conveniente de atendimento médico aos pacientes e profissionais envolvidos, ainda há os desafios em relação à segurança dos dados pessoais dos pacientes. Assim, diante de ataques cibernéticos cada vez mais sofisticados e de casos de vazamento de informações sensíveis, é crucial que as plataformas de telemedicina e seus responsáveis adotem medidas rigorosas para garantir a proteção desses dados. Além da conscientização sobre a cultura de segurança cibernética e a implementação de sistemas robustos de criptografia e segurança, também é necessário destacar as responsabilidades éticas que envolvem a segurança cibernética de informações e prontuário eletrônicos, a fim de minimizar os riscos de incidentes de segurança e preservar a confidencialidade e dignidade dos pacientes. (SCHMITZ, GONÇALVES E UMPIERRE, 2020).

A coleta de dados pessoais de forma segura e eficiente para garantir um atendimento adequado ao paciente é crucial para garantir a efetividade da telemedicina como um meio adequado de cuidado dos pacientes. Neste contexto, o prontuário eletrônico desempenha um papel fundamental na coleta e guarda dessas informações. Assim, para garantir a precisão, confidencialidade e segurança das informações de saúde dos pacientes, o Conselho Federal de Medicina (CFM) estabeleceu regras específicas para o uso e guarda dos prontuários eletrônicos.

Em 2002, a Resolução CFM nº 1.638 foi expedida para definir o prontuário médico[19] e estabelecer seus requisitos técnicos para a guarda e manuseio. No entanto, com a vigência da

[18] Proteção de dados pessoais não ocorre apenas em dados obtidos por meios digitais, mas também se dá em arquivos físicos (art. 1° da LGPD), ou seja, mesmo para os casos em que o atendimento médico ocorra em plataformas digitais e o armazenamento dos dados, como o prontuário, ocorra em meio físico, os dados armazenados devem ter o cuidado requerido pela LGPD.

[19] Nas palavras de Garcia e Costa (2022), o prontuário médico é um documento que contém informações e registros relacionados à saúde do paciente e aos cuidados prestados, permitindo a comunicação entre os membros de equipes multiprofissionais e garantindo a continuidade da assistência. No entanto, é importante ressaltar que o prontuário

Resolução nº 1.821 em 2007, a antiga normativa perdeu sua validade e foram estabelecidos os requisitos técnicos para a digitalização e uso dos sistemas informatizados para a guarda e manuseio dos prontuários dos pacientes. Nessa toada, nota-se que a elaboração e guarda do prontuário eletrônico faz parte do arcabouço regulatório da telemedicina. (Garcia e Costa, 2022).

Nesse cenário surgiu a Lei nº 13.787/2018[20], que trata da regulamentação do prontuário eletrônico, em especial sobre a digitalização de documentos físicos envolvidos na relação médico-paciente. Além disso, tal legislação[21] aborda tanto a utilização, guarda e manuseio de prontuários já criados em ambiente originalmente eletrônico, quanto a digitalização de documentos elaborados no meio físico, que deverão ser armazenados em ambiente digital.

Segundo Schimitz, Gonçalves e Umpierre[22], os dados coletados durante a relação profissional-paciente remota devem ser aqueles necessários para a função a que se destinam, e não mais do que isso. Isso posto, é necessário que sejam coletados os dados pessoais de identificação necessários ao prontuário eletrônico que incluem nome completo, data de nascimento, endereço, número de telefone, endereço de e-mail e informações de contato de emergência.

Já sobre o histórico médico e informações de saúde, é pertinente a coleta de informações sobre doenças pré-existentes, histórico familiar, alergias, medicamentos em uso, cirurgias anteriores, resultados de exames laboratoriais, registros de vacinação, entre outros. Essas informações ajudam o médico a ter uma compreensão abrangente da saúde do paciente e auxiliam no diagnóstico, tratamento e monitoramento adequados. Também poderão ser coletadas informações da consulta de telemedicina, como a queixa atual do paciente, sintomas, duração, intensidade, fatores desencadeantes, entre outros detalhes relevantes. Esses dados

não é verdadeiramente único, pois incorpora diversos elementos, como exame clínico, fichas de ocorrência, prescrições terapêuticas, relatórios de enfermagem, relatórios de cirurgia, registros de exames complementares e solicitações de exames, entre outros.

[20] BRASIL. **Lei nº 13.787**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. [S. l.], 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 7 jul. 2023.

[21] Apesar de existir regulamentação sobre a guarda de informações de pacientes em ambiente eletrônico, Garcia e Costa destacam que a regulamentação vigente não é capaz de sanar todas as dúvidas acerca de quais informações são necessárias ao prontuário médico, conforme exposto: "Sendo este o caso, recomenda-se que uma eventual regulação da telemedicina repercuta a informação de que a telemedicina gera um prontuário médico eletrônico, como forma de evitar futuros questionamentos sobre o tema, e que dispense a obrigatoriedade de informações sobre o exame físico constarem no prontuário. Além disso, é possível que a lei estabeleça outros elementos para o prontuário telemédico, caso se entenda necessário, devendo a comunidade médica se posicionar sobre eles."

[22] SCHMITZ, Carlos A A.; GONÇALVES, Marcelo R.; UMPIERRE, Roberto N.; et al. **Consulta Remota**: Fundamentos e Prática. Grupo A, 2020. E-book. ISBN 9786558820031. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786558820031/. Acesso em: 05 jul. 2023.

auxiliam o médico a fazer uma avaliação precisa e a propor um plano de tratamento adequado. (SCHIMITZ, GONÇALVES E UMPIERRE, 2020)

Quanto à guarda dos dados e informações, esta deve ser realizada de forma segura em sistemas de prontuários eletrônicos protegidos por criptografia, com acesso restrito apenas a profissionais autorizados, como iClinic, Amplimed[23], Doctor's Office, entre outros. Além disso, é importante cumprir as regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, para garantir o cumprimento das medidas de segurança necessárias, conforme pontuado por Mendes e Doneda[24]:

> *A LGPD estabelece também uma obrigação central aos agentes de tratamento de adoção das medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. É o que estabelece o seu art. 46, que inaugura o capítulo de segurança da informação da LGPD, aplicável tanto aos controladores quanto aos operadores. (DONEDA e MENDES, 2018).*

Ademais, o paciente tem assegurado o sigilo das informações contidas no prontuário, pois o médico não pode[25], sem o consentimento do paciente[26], revelar o conteúdo do prontuário ou da ficha médica, direito este assegurado pelo artigo 1º da Resolução do CFM no 1.605 de 15 de setembro de 2000 e no artigo 85 do Código de Ética Médica[27]. (Martins e Teles, 2021)

No contexto da telemedicina, o tratamento de dados de saúde deve ser realizado exclusivamente para a proteção da saúde do paciente, sendo que o termo "exclusivamente" deve ser interpretado de forma restritiva, mas não absoluta. Nesse cenário, de acordo com a Declaração de Tel Aviv[28], caso a informação seja relevante para o problema do paciente e for

---

[23] A título de exemplo, Amplimed integra o software de consultas digitais com armazenamento de prontuário eletônico ou prontuários digitalizados em um sistema em nuvem que utiliza criptografia como forma de segurança e em sua Política de Privacidade atesta que poderá tratar os dados pessoais coletados junto à profissional da saúde, clínica e/ou empresa que utiliza a plataforma.

[24] DONEDA, Danilo e MENDES, Laura Schertel. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, n. 1, p. 5, 2018.

[25] Segundo entendimento do STJ, o profissional médico está incluído no rol de pessoas proibidas de depor em razão de sua atividade profissional, considerando que não deve expor informação do paciente que teve conhecimento em razão da profissão exercida, conforme notícia publicada em 14/03/2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/14032023-Sexta-Turma-tranca-acao-penal-por-aborto-ao-ver-quebra-de-sigilo-profissional-entre-medico-e-paciente.aspx

[26] O consentimento do paciente na telemedicina deve ser realizado por meio do Termo de Consentimento Livre e Esclarecido (TCLE), em que o paciente declara anuência sobre o tratamento dos seus dados para a finalidade informada no documento. A título de exemplo, algumas plataformas de telemedicina como Clude e Conexa incluem o TCLE junto aos Termos de Uso de sua plataforma.

[27] Já no âmbito de pesquisa clínica, tem seus direitos resguardados por normativas éticas do Conselho Nacional de Saúde, órgão vinculado ao Ministério da Saúde, em especial a Resolução No 466 de 15 de dezembro de 2012 e Resolução no 510 de 7 de abril de 2016.

[28] Israel. World Medical Association. WMA Statement On Accountability, Responsibilities And Ethical Guidelines In The Practice Of Telemedicine. [Declaração de Tel Aviv, 1999]. Israel, 1999 [Acesso em

transferida a outro médico com o consentimento do paciente com o intuito de buscar soluções para um problema de saúde, esse intercâmbio de informações não violaria a confidencialidade inerente à atuação médica[29].

Disso tudo, além das questões sobre consentimento do paciente e confidencialidade das informações médicas, um ponto adicional de desafio refere-se ao tempo mínimo de guarda dos prontuários, que atualmente é de 20 anos para os documentos físicos, segundo a Lei nº 13.787/2018 (Lei do Prontuário Eletrônico) e indeterminado para os documentos originalmente digitais[30]. O intuito da Lei do Prontuário eletrônico ao elencar a extensão do período de retenção de informações é equilibrar a confidencialidade e a proteção dos dados, por um lado, e a obrigação de manter um grande volume de documentos por um longo período, por outro. Enfim, essa situação impõe desafios para respeitar a confidencialidade do paciente em um ambiente de crescente troca de informações entre os diversos atores da saúde.

Ante o exposto, tendo em consideração quais dados devem ser coletados e a maneira correta de coleta durante consultas remotas, percebe-se que os profissionais envolvidos devem seguir as diretrizes deontológicas das regulamentações éticas, mas também obrigações civis sobre a guarda de dados pessoais segundo a LGPD. Paralelamente, ainda é necessário entender quem são os agentes de tratamento envolvidos como forma de minimizar os riscos de vazamento e garantir a segurança cibernética do atendimento médico à distância, conforme será apresentado a seguir.

4. Agentes responsáveis pelo tratamento e guarda de dados:

Tendo como ponto de partida o fato que a telemedicina trouxe avanços significativos na prestação de serviços de saúde, também é necessário compreender os agentes responsáveis pelo tratamento e guarda de informações obtidas por meio da prestação de serviço médico em meios digitais, a fim de estabelecer as responsabilidades das pessoas envolvidas sobre a proteção e o arquivamento seguro dos dados dos pacientes. Ao analisar a atuação de cada agente nesse processo, teremos uma visão mais abrangente das obrigações e responsabilidades relacionadas ao arquivamento seguro dos dados sensíveis coletados.

02.jul.2023]. Disponível em: https://www.wma.net/policies-post/wma-statement-on-accountability-responsibilities-and-ethical-guidelines-in-the-practice-of-telemedicine/.

[29] A declaração de Tel Aviv foi adotada pela 51ª Assembléia Geral da Associação Médica Mundial em Tel Aviv, sendo utilizada no Brasil em preâmbulos de normas do CFM, considerando que o Brasil é signatário da declaração.

[30] Art. 6º da Lei Nº 13.787 de 2018: "Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados."

Dito isso, esse modelo de atendimento médico traz consigo uma série de desafios concernentes à segurança e privacidade dos dados, relacionados ao intenso aumento de fluxo de informações, pelas novas possibilidades criadas pelo uso de big data[31] e algoritmos, que permitem reunir dados, analisar, identificar perfis comportamentais, tendências de resultado e lucro. (SCHULMAN E CAVET, 2021)[32]. Com a transmissão e armazenamento de dados do paciente, existe um risco de tornar informações sensíveis em mercadoria, conforme exposto:

> Apenas para tomar como exemplo, na saúde, o acesso aos dados poderia influenciar na tomada de decisão em relação a contratos de planos de saúde ou seguros de vida. De igual modo, a indústria farmacêutica poderia extrair dados clínicos de pacientes para desenvolver ou aprimorar seus medicamentos. (SCHULMAN E CAVET, 2021)

Logo, compreender as responsabilidades de cada agente envolvido no tratamento e guarda de dados na telemedicina é fundamental para estabelecer um ambiente seguro e confiável. Para tanto, a recomendação de agências reguladoras nacionais e internacionais perpassa a minimização de dados, para que somente os dados necessários sejam transmitidos da maneira estritamente permitida (SCHMITZ, GONÇALVES e UMPIERRE, 2020).

Isso posto, para reconhecer quais agentes, sejam pessoas físicas ou jurídicas, podem ser responsabilizados em caso de incidente de segurança na telemedicina, é necessário entender primeiro o papel dos envolvidos no tratamento de dados, ou seja, quem é classificado como controlador, operador e encarregado. Logo, partimos do pressuposto que, segundo o art 5º, VI e VII da LGPD, controlador é a pessoa que determina as finalidades e métodos de tratamento de dados, já o operador é o que realiza a atividade do tratamento de acordo com as instruções repassadas pelo controlador (LEONARDI, 2020)[33].

Há que se falar também sobre os requisitos de uma pessoa ser considerada controlador de dados pessoais, sendo eles: (i) o controlador pode ser tanto uma pessoa natural como uma pessoa jurídica, de direito público ou privado; (ii) o controlador pode exercer o tratamento de dados pessoais de forma isolada ou em conjunto com outros controladores; e (iii) o poder e a

---

[31] Big Data é uma área de análise de informações que envolve o uso de tecnologias avançadas e algoritmos de processamento de dados para identificar padrões, tendências e insights úteis que possam ser aplicados em diferentes setores.

[32] SCHULMAN, Gabriel; CAVET, Caroline Amadori. **A Violação de Dados Pessoais na Telemedicina:** Reparação do Paciente À Luz Da LGPD. Pensar Acadêmico, [*s. l.*], ano 2021, v. 19, ed. 3, 30 jul. 2021. Disponível em: https://www.pensaracademico.unifacig.edu.br/index.php/pensaracademico/article/view/2541. Acesso em: 10 jul. 2023.

[33] LEONARDI, Marcel. Transferência Internacional dos Dados Pessoais. In: BIONI, Bruno Ricardo et al, (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2020. p. 301. ISBN 978-85-309-9219-4. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/10%5B%3Bvnd.vst.idref%3Dhtml4%5D!/4/44/1:0%5B%2CCam%5D. Acesso em: 11 jul. 2023.

responsabilidade por definir as finalidades do tratamento e os meios utilizados para alcançá-las (OLIVEIRA, 2021).

Nesse contexto, cabe ressaltar que o controlador também pode realizar todas as obrigações e deveres estabelecidos para um operador, considerando que este último atua mediante solicitação e instrução do primeiro. Dito isso, o operador é o agente que auxilia no cumprimento das normas de proteção de dados sem possuir poder decisório, sendo responsável por: (i) manter os registros das atividades de tratamento, (ii) assegurar a privacidade e segurança dos dados; e (iii) implementar programas de conformidade para proteger os direitos dos titulares (OLIVEIRA, 2021).

Já o encarregado sobre o tratamento, nos termos da Lei 13.709/2018, é a pessoa indicada pelo controlador, que atua como um canal de comunicação entre os titulares dos dados, os órgãos governamentais e a ANPD, além de orientar os funcionários sobre as práticas necessárias à proteção de dados pessoais (SANTOS, 2021).

Nesse cenário, aqui serão analisadas as hipóteses de tratamento de acordo com as pessoas envolvidas e as diferentes atribuições de cada uma enquanto agente de tratamento de dados. Assim, as hipóteses aqui analisadas são as mais comuns na telemedicina, sendo elas: (i) atuação com apenas um médico e o paciente; (ii) atuação conjunta entre o médico e a clínica que oferece serviços de telemedicina; (iii) o médico e uma empresa terceirizada que disponibiliza a plataforma digital de telemedicina; e (iv) uma pessoa jurídica, seja clínica ou hospital, que contrata uma plataforma digital de telemedicina onde o médico presta seus serviços.

4.1. Atuação na telemedicina com apenas um médico e um paciente:

Nessa situação, tem-se o caso de um médico que presta seus serviços de maneira autônoma, sem que haja um superior hierárquico ou pessoa que delegue tarefas para viabilizar a prestação de serviço. Logo, o médico é o controlador nos termos do art 5º, VI da LGPD: “a quem competem as decisões referentes ao tratamento de dados pessoais”. Da mesma forma, o Código de Boas Práticas de Proteção de Dados para Prestadores Privados em Saúde confirma que o próprio médico, pessoa natural, enquanto responsável pelo atendimento e pelo preenchimento do prontuário médico, é considerado o controlador dos dados.

4.2. Atuação conjunta entre o médico e a clínica que oferece serviços de telemedicina:

O médico, vinculado à pessoa jurídica, seja ela uma clínica médica, hospital ou similar, presta seus serviços sob a supervisão de um superior hierárquico. Ele não possui poder de decisão em questões estratégicas da entidade, mas é responsável por fornecer atendimento médico de qualidade por meio da plataforma de telemedicina. O médico é considerado o operador dos dados pessoais dos pacientes, responsável por armazenar e manusear os dados e informações dos pacientes, atuando de acordo com as diretrizes estabelecidas pela clínica e em conformidade com as normas do conselho regional de sua profissão.

Assim, a clínica como controladora dos dados pessoais dos pacientes, terá o poder de decisão sobre como esses dados serão utilizados e tratados, sendo responsável também por designar o médico para realizar os atendimentos. Além disso, a clínica também terá autonomia para definir as políticas de privacidade e segurança dos dados, estabelecendo as diretrizes sobre o armazenamento, compartilhamento e descarte das informações dos pacientes, sempre em conformidade com as normas e regulamentos pertinentes. Nesse cenário, o médico, como operador, seguirá as orientações e diretrizes estabelecidas pela clínica para garantir a proteção dos dados pessoais dos pacientes e a qualidade dos serviços prestados na telemedicina.

4.3. Atuação de um médico e uma empresa terceirizada que disponibiliza a plataforma digital de telemedicina:

Aqui temos que a atuação do médico e da empresa terceirizada na plataforma digital de telemedicina é colaborativa e complementar, de modo que o médico utiliza a ferramenta eletrônica para oferecer atendimento pré-clínico, consultas, diagnósticos e monitoramento remoto aos pacientes. Por outro lado, a empresa terceirizada é responsável por disponibilizar e gerenciar a plataforma, desenvolvendo e mantendo o software, website, aplicativos e outras extensões tecnológicas. Assim, considera-se que a empresa terceirizada atua apenas para viabilizar a atividade médica, devendo garantir a segurança dos dados, a confidencialidade das informações e a disponibilidade contínua do serviço, proporcionando uma experiência de telessaúde eficiente e segura para pacientes e profissionais de saúde. Isso posto, aqui o médico é considerado o Controlador dos dados, já que possui o poder decisório de delegar tarefas à plataforma, ao passo que a empresa responsável pela plataforma deve atuar como como operadora dos dados. Além disso, cabe ao médico enquanto controlador nomear um encarregado para estar em contato com as agências reguladoras e os titulares dos dados, conforme é requerido pela legislação. Não obstante, também será responsabilidade da clínica indicar e nomear o encarregado, nos termos da LGPD.

4.4. Atuação de uma pessoa jurídica, seja clínica ou hospital, que contrata uma plataforma digital de telemedicina onde o médico presta seus serviços:

Nessa situação, a clínica assume o papel de controlador de dados, detendo o poder decisório sobre o tratamento dos dados pessoais dos pacientes. Já o médico é contratado pela clínica e age como operador de dados, prestando serviços sob a subordinação da entidade controladora. Disso tudo, o médico utiliza a plataforma de telemedicina, que é terceirizada, para realizar atendimentos e consultas virtuais, respeitando as orientações e finalidades definidas pela clínica como a controladora. Dessa forma, a clínica é a responsável por definir como os dados serão tratados, o médico executa os serviços sob sua supervisão e a plataforma digital de telemedicina atua apenas como ferramenta contratada para viabilizar o exercício da medicina. Ou seja, tanto o médico quanto a plataforma podem ser considerados operadores por atuarem em subordinação à clínica ou hospital, dependendo do que for solicitado pela controladora.

Além disso, a Lei Geral de Proteção de Dados exige seja designado um encarregado de proteção de dados como responsável por assegurar o cumprimento da legislação de proteção de dados dentro da organização. No cenário descrito, a clínica ou hospital pode designar um encarregado de proteção de dados para garantir que todas as atividades relacionadas ao tratamento de dados pessoais na plataforma de telemedicina estejam em conformidade com as normas de privacidade e segurança estabelecidas pela LGPD.

Dito isso, a classificação apresentada acima é apenas um indicativo sobre o que é mais comum no contexto da telemedicina, de modo que para cada caso específico é necessário que os prestadores de serviços privados de saúde avaliem a finalidade do tratamento de dados e o papel de cada agente de acordo com cada caso específico. Além disso, também é possível existir hipóteses em que os envolvidos sejam co-controladores, como ocorre com o armazenamento de prontuários eletrônicos, caso tanto o médico quanto o estabelecimento de saúde tenham poder decisório sobre o prontuário.

Ademais, a proteção de dados na telemedicina se baseia em um ambiente de dupla regulação, em que os agentes de tratamento envolvidos são regulados tanto pela Autoridade Nacional de Proteção de Dados (ANPD) quanto pelo Conselho Federal de Medicina (CFM) Assim, a ANPD estabelece diretrizes e fiscaliza a aplicação da Lei Geral de Proteção de Dados (LGPD), por sua vez, o CFM emite normas e regulamentos específicos relacionados à prática médica, incluindo a telemedicina. Essa regulação por diferentes entidades garante que os agentes de tratamento na telemedicina estejam sujeitos a um conjunto de regras e padrões de

proteção de dados, visando assegurar a privacidade e a segurança das informações dos pacientes. Ou seja, podem ser aplicadas sanções administrativas pelas duas entidades, sem prejuízo de eventuais responsabilizações por outras esferas.

5. Incidente de Segurança na Telemedicina:

Após identificar os agentes envolvidos no tratamento de dados na telemedicina, é fundamental compreender as medidas a serem adotadas em caso de incidente de segurança e quais normas e sanções são aplicáveis nessa situação. Isso posto, tem-se em mente que um incidente de segurança, segundo Menke e Goulartt[34], diz respeito à ocorrência em que uma vulnerabilidade no armazenamento de dados é explorada por uma ameaça, o que pode resultar, no caso da telemedicina, em violação à confidencialidade do prontuário do paciente, a título de exemplo. Assim, é necessário analisar como deve ocorrer o procedimento de aplicação de sanções éticas aos profissionais envolvidos em eventual incidente de vazamento de dados coletados na Telemedicina, conforme será abordado adiante.

Na hipótese de um incidente de segurança é essencial que sejam localizados os agentes responsáveis pela ocorrência do incidente para que a responsabilização seja adequadamente atribuída. No contexto da telemedicina, os sujeitos envolvidos - médico, clínica e empresa terceirizada - devem ser investigados para identificar suas respectivas responsabilidades no ocorrido. Assim, a pessoa que atua como controladora, seja a clínica ou o médico com poder decisório, é responsável por garantir a segurança dos dados dos pacientes e pela adoção de medidas de proteção adequadas. Já os operadores, seja o médico subordinado ou uma empresa terceirizada responsável pela plataforma, também devem agir em conformidade com as diretrizes e medidas de segurança estabelecidas pela clínica e pela legislação. Disso tudo, a pessoa que for nomeada como encarregado de dados terá a função de notificar a Agência Nacional de Proteção de Dados (ANPD) caso ocorra eventual incidente de segurança.

Caso seja constatado que um dos envolvidos não cumpriu suas obrigações no que diz respeito à segurança dos dados, podem ser aplicadas as sanções por parte da ANPD, que tem o poder de aplicar penalidades previstas na legislação de proteção de dados. Além disso, o médico ou a entidade médica, também deve agir em conformidade com as diretrizes e medidas de segurança e confidencialidade essenciais ao exercício da profissão, caso contrário, se for

[34] MENKE, Fabiano e GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados. In: BIONI, Bruno Ricardo et al, (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2020. p. 355. ISBN 978-85-309-9219-4.

constatado que o incidente de segurança ocorreu por negligência ou violação das regras de proteção de dados, podem ser aplicadas sanções no viés ético profissional por parte do CFM, o Conselho Federal de Medicina.

Isso posto, o objetivo do presente artigo não é esgotar todas as esferas de responsabilização pertinentes caso ocorra eventual incidente de segurança na Telemedicina, mas apenas apurar como ocorreria a responsabilização sob a ANPD e sob o CFM, conforme serão apresentadas a seguir.

5.1. Responsabilização segundo a LGPD:

Em caso de violação de medidas adequadas e eficazes para cumprir as normas de proteção de dados pessoais, tanto o controlador quanto o operador podem ser responsabilizados individualmente ou solidariamente. A LGPD (Lei Geral de Proteção de Dados)[35] estabelece sanções administrativas no artigo 52 para o tratamento inadequado de dados, que podem variar desde advertências até multas por infrações, com limite máximo de 2% do faturamento da empresa ou até R$ 50.000.000,00.

No contexto do ordenamento jurídico brasileiro, as sanções previstas no artigo 52 da LGPD são aplicadas pelo órgão administrativo responsável, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e a dosimetria das sanções é determinada com base em critérios estabelecidos pela lei (também no art. 52) incluindo a gravidade e natureza das infrações, a boa-fé do infrator, a vantagem obtida ou pretendida, a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, a adoção de medidas internas de proteção de dados, a adoção de boas práticas e governança, a pronta adoção de medidas corretivas e a proporcionalidade entre a falta cometida e a intensidade da sanção. Esses critérios são utilizados para determinar a penalidade adequada em cada caso de violação da proteção de dados pessoais.

Nas hipóteses específicas de tratamento de Dados na telemedicina, podem ter casos em que a empresa terceirizada, responsável pela plataforma não seja responsabilizada, conforme pontuado por Ricardo Oliveira[36]:

> Segundo o artigo 52, a delimitação é clara no sentido de que terceiros que não participem do tratamento de dados pessoais não são destinatários das sanções, como poderia ser considerado, por exemplo, a empresa que licencia software,

[35] Brasil. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018 [Acesso em 12.jun.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[36] OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 14 jul. 2023.

> mas não tem acesso ou gestão sobre os dados nele imputados. No caso de vazamento de dados, se tal empresa não tratou os dados, poderá até ser penalizada de outra forma, mas não por meio das sanções previstas no artigo 52. (OLIVEIRA, Ricardo, 2021, p. 9)

Da mesma forma, como o encarregado não é considerado um agente de tratamento de dados pessoais nos termos da lei, ele não poderia ser apenado com as referidas sanções.

Além disso, em 06 de julho de 2023 foi aplicada a primeira multa em decorrência de um processo administrativo contra a empresa Telekall Infoservice[37], que infringiu os artigos 7º e 41 da LGPD, além do artigo 5º do Regulamento de Fiscalização da ANPD. Como se tratava de uma microempresa, o valor por cada infração foi limitado a 2% do faturamento bruto da Telekall Infoservice, totalizando uma multa de R$14.400,00.

Por fim, é importante ressaltar que todo o assunto é muito recente, assim como o início da vigência da LGPD, de modo que a fiscalização e aplicação de sanções ainda é algo incipiente no Brasil. Não obstante, a aplicação de penalidades em vias administrativas são independentes, ou seja, a aplicação ou não de eventual penalidade na LGPD não exime a aplicação de uma sanção sobre o mesmo assunto por outra agência reguladora, conforme apresentado por Ricardo Oliveira[38]:

> As sanções administrativas da LGPD não se confundem com outros tipos de sanções previstas em outras leis, como Código de Defesa do Consumidor ou Marco Civil da Internet. Em outras palavras, as autoridades que aplicam estas últimas não têm competência para aplicar a primeira. A LGPD estabeleceu precisamente, em seu artigo 52, que as sanções serão aplicadas pela autoridade nacional, ou seja, a ANPD (OLIVEIRA, Ricardo, 2021, p. 10)

5.2. Responsabilização segundo as normas do CFM:

Quando o foco é a responsabilidade profissional, segundo Genival Veloso de França, no âmbito do exercício da medicina, entende-se que diz respeito às obrigações que o médico deve cumprir e cuja abstenção gera sanções de diferentes normativas. Assim, um profissional médico deve ser responsabilizado perante seu órgão de classe, quando na apreciação do

[37] A fiscalização foi iniciada a partir de denúncia de que a empresa estava ofertando uma listagem de contatos de WhatsApp de eleitores para fins de campanha eleitoral sem respaldo legal. A ANPD verificou que o tratamento de dados estava ocorrendo sem respaldo legal e a empresa não comprovou a indicação de um encarregado para o tratamento de dados pessoais. Diante dos indícios de infração, a CGF/ANPD lavrou Auto de Infração, iniciando o Processo Administrativo Sancionador, que resultou na aplicação das sanções mencionadas. A empresa pode recorrer da decisão ao Conselho Diretor da Autoridade.

[38] OLIVEIRA, Ricardo. LGPD: Como evitar as sanções administrativas. São Paulo: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 14 jul. 2023.

ocorrido seja comprovada a conduta atípica ou em inobservância às normas técnicas durante ou em face da atividade médica e que gere algum dano contra o paciente (FRANÇA, 2020).

Dito isso, segundo o Código de Processo Ético-Profissional do Conselho Federal de Medicina, as sanções disciplinares aplicáveis são as previstas no artigo 22 da Lei nº 3.268/1957, conforme segue:

> Art. 22. As penas disciplinares aplicáveis pelos Conselhos Regionais aos seus membros são as seguintes:
> a) advertência confidencial em aviso reservado;
> b) censura confidencial em aviso reservado;
> c) censura pública em publicação oficial;
> d) suspensão do exercício profissional até 30 (trinta) dias;
> e) cassação do exercício profissional, ad referendum do Conselho Federal.

Nesse cenário, em eventual incidente de segurança em que seja constatada a responsabilidade do médico ou da pessoa jurídica habilitada no Conselho Federal de Medicina, para dar início à investigação para apuração da necessidade de aplicação de sanção disciplinar, é instaurada uma sindicância, que é julgada por um órgão colegiado, para verificar o ocorrido. Nesse sentido, para ocorrer a responsabilização de um médico sobre alguma ação ou omissão deve ser comprovada sua culpa, seja por imperícia, imprudência ou negligência[39].

Na sindicância verifica-se existência ou não de infração ao Código de Ética Médica e decide-se pelo arquivamento ou abertura de Processo Ético Profissional, sempre de maneira fundamentada. Durante a fase de sindicância, são apresentadas provas sobre o cumprimento das responsabilidades e obrigações do médico ou entidade médica enquanto controlador ou operador dos dados, podendo ser comprovada a exoneração da responsabilidade conforme o caso. Assim, o principal ponto para aplicação de sanções disciplinares é verificar se o sigilo e a confidencialidade essenciais ao exercício da medicina foram preservados.

Nesse sentido, para Genival França, a deontologia da medicina deve partir do pressuposto que, para incidir a responsabilização ética-profissional de um médico, basta existir a voluntariedade de uma conduta contrária às regras vigentes e que não esteja relacionada à prudência, como ocorre em casos de desrespeito aos deveres de vigilância, abstenção de abuso e sigilo médico. Além disso, na efetivação da responsabilidade médica, há alguns requisitos indispensáveis, sendo eles: (i) o autor da conduta antiética; (ii) o ato ilícito ou infração delituosa;

---

[39] Nas palavras de Genival Veloso de França: Por fim, quando da avaliação da culpa médica, deve ficar evidente que sem a existência de um dano efetivo e real não se pode caracterizar a responsabilidade profissional, tal qual ela está inserida nos dispositivos específicos, seja por imperícia, imprudência ou negligência. A determinação concreta do dano, além de indispensável em relação à configuração da responsabilidade médica, pode estabelecer o grau da culpa e a extensão da liquidação. Mesmo assim, ainda há de se concretizar o nexo de causalidade e as condições em que se verificou o dano. (FRANÇA, 2020, p.384)

(iii) presença de culpa, ou seja, o dano foi produzido por negligência, imprudência ou imperícia na ausência de dolo; (iv) dano real, efetivo, concreto e determinado; (v) nexo de causalidade entre o ato ilícito e o dano causado (FRANÇA, 2020).

Isso posto, sobre a análise da responsabilidade médica, Caio Mário destaca que:

> Em nosso direito, à vista do que dispõe o art. 951 do Código Civil, em conjunto com o art. 14, § 4º do Código de Defesa do Consumidor, é lícito extrair uma regra definidora da responsabilidade médica, quando o dano resultar de imprudência, negligência ou imperícia, valendo as situações aqui descritas, e outras mais, como elementos informativos destas hipóteses legislativas de responsabilidade médica (PEREIRA, 2022).

Além da imputação de responsabilidade perante o Conselho Federal de Medicina e, eventualmente, o conselho regional que o médico estiver inscrito, é importante ressaltar também que, no caso de incidente de vazamento de dados na prática da telemedicina, em que o dever de sigilo não é respeitado, a responsabilidade civil do agente responsável pelo incidente é subjetiva, como exceção à regra geral da responsabilidade civil objetiva presente nas relações de consumo (TEPEDINO, 2022). Logo é considerado que o foco da responsabilização sobre incidente de vazamento de dados na prática da telemedicina é a figura do ato ilícito, contrário às normas do Código de Ética Médica e da própria Lei Geral de Proteção de Dados.

Enfim, ao abordar a responsabilidade ética-disciplinar na atuação médica, é essencial reconhecer a relação intrínseca com a responsabilidade civil. A responsabilidade ética-disciplinar, fundamentada em princípios e normas da profissão médica, é essencial para garantir padrões de conduta e cuidado adequados, visando o bem-estar do paciente e a qualidade dos serviços prestados. Da mesma forma, a responsabilidade civil é crucial para assegurar a reparação de danos em casos de negligência ou falhas na prestação dos serviços médicos, proporcionando amparo aos pacientes afetados. Em outras palavras, a responsabilidade médica abrange diferentes esferas, não sendo possível separá-las por completo.

6 CONCLUSÃO

A telemedicina trouxe avanços significativos na prestação de serviços de saúde, mas também trouxe desafios em relação à segurança e privacidade dos dados coletados e tratados durante o processo. Dentre os desafios, estabelecer as responsabilidades dos agentes envolvidos na proteção e arquivamento seguro dos dados dos pacientes não é algo exposto de maneira clara pela legislação vigente. Assim, é necessário compreender a atuação de cada pessoa envolvida e suas responsabilidades conforme a função exercida no tratamento dos dados.

Sob a perspectiva da Lei Geral de Proteção de Dados (LGPD), tanto os controladores quanto os operadores podem ser responsabilizados individualmente ou solidariamente, podendo ser aplicadas sanções administrativas que variam desde advertências até multas significativas, dependendo da gravidade e natureza da infração.

Por outro lado, no âmbito da ética profissional, os médicos e entidades médicas estão sujeitos às normas do Conselho Federal de Medicina (CFM). Em caso de incidente de vazamento de dados que envolva condutas antiéticas ou violações do Código de Ética Médica, pode ser instaurado um Processo Ético Profissional, e o médico pode ser submetido a sanções disciplinares, como advertência confidencial, censura pública, suspensão do exercício profissional ou até mesmo cassação do exercício profissional.

Em vista disso, a proteção de dados na telemedicina é uma questão que perpassa diferentes esferas de responsabilização e os agentes envolvidos devem estar em conformidade tanto com as normas de proteção de dados quanto com as normas éticas e profissionais relacionadas à prática médica. No entanto, ainda falta clareza e colaboração entre a ANPD e os Conselhos de Medicina para garantir um ambiente plenamente seguro na telemedicina. Assim, enquanto as agências reguladoras ainda não atuam de maneira cooperada, é crucial que os agentes de tratamento de dados na telemedicina estejam cientes de suas responsabilidades e se empenhem na adoção de boas práticas para proteger a privacidade dos pacientes e assegurar a boa atuação médica.

7 REFERÊNCIAS

BRASIL. **Lei nº 13.989**, de 15 de abril de 2020. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). [S. l.], 2002. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328. Acesso em: 25 jun. 2023.

CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019. Brasília, 2019.

CONSELHO FEDERAL DE MEDICINA. **Processo Ético-Profissional**: Resolução CFM nº CFM nº 2.306/2022. Brasília: **Diário Oficial da União**, 2022. Disponível em: https://portal.cfm.org.br/etica-medica/codigo-de-processo-etico-profissional-atual/. Acesso em 21 jun. 2023.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.314, de 20 de abril de 2022. Brasília: **Diário Oficial da União**, 2022. Disponível em:

https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em 21 jun. 2023.

CONSELHO FEDERAL DE MEDICINA (Brasil). **Resolução nº 1.643**. [S. l.], 2002.

CONSELHO FEDERAL DE MEDICINA (Brasil). **Resolução nº 2.227**. [S. l.], 2018.

COHEN, Claudio; OLIVEIRA, Reinaldo Ayer de. **Bioética, direito e medicina**. Manole, 2020.

FÉLIX, V.; MONTEIRO, J. R. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com**, v. 11, n. 1, p. 1-31, 29 jun 2023.

FRANÇA, Genival Veloso. **Direito Médico**. Grupo GEN, 2020. ISSN 9788530992316.

FRANÇA, Genival Veloso. Telemedicina: breves considerações ético-legais. **Bioética,** v. 8, n. 1, p. 107-126, 2000. Disponível em: https://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/view/266. Acesso em: 21 jun. 2023.

GARCIA, Marcos Vinicius Fernandes e GARCIA, Marco Aurélio Fernandes. Telemedicina, segurança jurídica e COVID-19: onde estamos?. **Jornal Brasileiro de Pneumologia**, v. 46, n. 04, 2020. ISSN 1806-3756. Disponível em: https://doi.org/10.36416/1806-3756/e20200363. Acesso em: 21 jun. 2023.

GARCIA, M. A. F.; COSTA, J. A. F. **O (novo) marco civil da telemedicina**: a construção de um ambiente regulatório saudável para as novas práticas telemédicas. Revista de Direito Sanitário, *[S. l.]*, v. 22, n. 2, p. e0003, 2022. DOI: 10.11606/issn.2316-9044.rdisan.2022.173191. Disponível em: https://www.revistas.usp.br/rdisan/article/view/173191. Acesso em: 6 jul. 2023.

GUIMARÃES, Ana Carolina et al.. Telemedicina e COVID-19: uma revisão de literatura. **Revista Bioética Cremego**, v. 3, n. 1, p. 40-48, 2021. Disponível em: https://revistabioetica.cremego.org.br/cremego/article/download/30/12. Acesso em: 21 ago. 2022.

LEONARDI, Marcel. Transferência Internacional dos Dados Pessoais. In: BIONI, Bruno Ricardo et al, (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2020. p. 301. ISBN 978-85-309-9219-4. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/10%5B%3Bvnd.vst.idref%3Dhtml4%5D!/4/44/1:0%5B%2CCam%5D. Acesso em: 11 jul. 2023.

MALDONADO, Jose Manuel Santos de Varge; MARQUES, Alexandre Barbosa; e CRUZ, Antonio. Telemedicina: desafios à sua difusão no Brasil. **Cadernos de Saúde Pública**. 2016, v. 32. Disponível em: https://doi.org/10.1590/0102-311X00155615. Acesso em 21 jun. 2023.

MARTINS, Guilherme Magalhães; TELES, Carlos André Coutinho. A Telemedicina na Saúde Suplementar e a Responsabilidade Civil do Médico no Tratamento de Dados à Luz da LGPD. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, v. 7, n. 1, p. 182-197, abr. 2021.

ISSN 2447-5467. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/608. Acesso em: 21 jun. 2023.

NEVES, Mariana Patrão. Thomas Percival: inovação e tradição. **Bioética**, v.11, n. 01. Disponível em: https://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/view/145. Acesso em 08 jul. 2023.

OLIVEIRA, A. B. et al.. Desafios do avanço da Telemedicina e seus aspectos éticos: revisão integrativa**. Comunicação em Ciências da Saúde, Brasília**, v. 31, n. 01, p. 55-63, 2020. Disponível em: http://www.escs.edu.br/revistaccs/index.php/comunicacaoemcienciasdasaude/article/view/566. Acesso em: 21 jun. 2023.

OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 14 jul. 2023.

PANCINI, Laura. Hariexpress, entenda o que pode acontecer com envolvidos em megavazamento: 1,7 bilhão de dados sensíveis de brasileiros foram vazados da plataforma Hariexpress, que tem parceria com gigantes como Mercado Livre, Magazine Luiza, Shopee e até os Correios. **Exame**, 23 out. 2021. Disponível em: https://exame.com/tecnologia/entenda-caso-hariexpress-megavazamento/. Acesso em: 25 jun. 2023.

PEREIRA, Caio Mário da S. **Responsabilidade Civil**. Grupo GEN, 2022. E-book. ISBN 9786559644933. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559644933/. Acesso em: 09 jul. 2023.

SANTOS, Tiago Francisco Campanholi dos. **O (possível) conflito de interesse na função e atribuições do Encarregado (Data Protection Officer – DPO)**: uma abordagem prática de acordo com a realidade dos profissionais de privacidade no Brasil. 2021. Projeto de Pesquisa (Mestrado) - Faculdade de Direito, Fundação Getúlio Vargas, São Paulo, 2022. Disponível em: https://direitosp.fgv.br/sites/default/files/arquivos/103.pdf. Acesso em: 14 jul. 2023.

SCHMITZ, Carlos A A.; GONÇALVES, Marcelo R.; UMPIERRE, Roberto N.; et al. **Consulta Remota**: Fundamentos e Prática. Grupo A, 2020. E-book. ISBN 9786558820031. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786558820031/. Acesso em: 05 jun. 2023.

SCHULMAN, Gabriel; CAVET, Caroline Amadori. **A Violação de Dados Pessoais na Telemedicina:** Reparação do Paciente À Luz Da LGPD. Pensar Acadêmico, [*s. l.*], ano 2021, v. 19, ed. 3, 30 jul. 2021. Disponível em: https://www.pensaracademico.unifacig.edu.br/index.php/pensaracademico/article/view/2541. Acesso em: 10 jul. 2023.

SOUZA, Alessandra Varrone de Almeida P. **Direito Médico**. Grupo GEN, 2022. ISSN 9786559645565.

TEPEDINO, Gustavo, et al. **Fundamentos do Direito Civil**: Responsabilidade Civil. v.4. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022.