Telemedicina, proteção de dados e segurança da informação: Elementos para a preservação da confidencialidade dos registros eletrônicos em saúde

Recebido: 24 de fevereiro de 2023 • Aprovado: 14 de dezembro de 2023
https://doi.org/10.22395/ojum.v24n51a4449

Jairo Victor Candeira Braga
Universidade Federal do Piauí – UFPI, Teresina, Brasil
jairo.victor@ufpi.edu.br
https://orcid.org/0000-0001-8769-7020

Gabriel Rocha Furtado
Universidade Federal do Piauí – UFPI, Teresina, Brasil
rochafurtado@ufpi.edu.br
https://orcid.org/0000-0003-0482-8465

Resumo

As linhas desta pesquisa dedicam-se à investigação da regulação jurídica dos fluxos informacionais relacionados às ações e serviços de telemedicina no contexto brasileiro. O artigo descreve como as Tecnologias da Informação e Comunicação (TIC) aplicadas aos processos de saúde-doença aumentam osriscos associados a incidentes de segurança, em virtude da disponibilização dos dados em um ecossistema digital suscetível a erros humanos e ataques de cibercriminosos. Nosso objetivo é compreender os deveres legalmente atribuídos aos agentes de tratamento de dados, quando atuam sobre os registros clínicos resultantes de atendimentos realizados por telemedicina. De forma mais específica, pretendemos avaliar se o Conselho Federal de Medicina (CFM) e a Autoridade Nacional de Proteção de Dados (ANPD) definiram critérios de segurança com uma abordagem focalizada para os sistemas de saúde, no âmbito de regulação que decorre de suas respectivas competências normativas. Para a consecução dos objetivos propostos, desenvolvemos um estudo de abordagem qualitativa, baseado em levantamento bibliográfico e documental. Como resultado, constata-se que o ordenamento jurídico brasileiro não comtempla adequadamente os riscos à confidencialidade dos dados, fornecendo apenas uma visão geral sobre quais medidas de segurança um custodiador deve implementar, a fim de proteger os dispositivos médicos e os Registros Eletrônicos em Saúde (RES).

Palavras-chave: telemedicina; registro eletrônico em saúde; dados pessoais sensíveis; proteção de dados; segurança da informação; tecnologias da informação e comunicação.

Telemedicine, data protection, and information security: Elements for the preservation of confidentiality of electronic health records

Abstract

The lines of this research are dedicated to the analysis of the legal regulation of informational flows related to telemedicine actions and services in the Brazilian setting. The article describes how Information and Communication Technologies (ICT) applied to health and disease processes increase the risks associated with security incidents, due to the availability of data in a digital ecosystem susceptible to human error and attacks by cybercriminals. This article aims to understand the legal duties attributed to data processing agents when acting on clinical records resulting from telemedicine care. More specifically, we intend to assess whether the Federal Council of Medicine (CFM) and the National Data Protection Authority (ANPD) have defined security criteria with a specific approach to health systems, within the regulatory framework deriving from their respective normative competences. To achieve the proposed objectives, a qualitative study was carried out, based on a bibliographic and documentary review. As a result, it is found that the Brazilian legal system does not adequately address the risks to data confidentiality, providing only an overview of what security measures a custodian should implement in order to protect medical devices and Electronic Health Records (EHR).

Keywords: telemedicine; electronic health record; sensitive personal data; data protection; information security; information and communication technologies.

Telemedicina, protección de datos y seguridad de la información: Elementos para la preservación de la confidencialidad de los registros electrónicos en salud

Resumen

Las líneas de esta investigación se dedican al análisis de la regulación jurídica de los flujos informacionales relacionados con las acciones y servicios de telemedicina en el contexto brasileño. El artículo describe cómo las Tecnologías de la Información y la Comunicación (TIC) aplicadas a los procesos de salud y enfermedad, aumentan los riesgos asociados a incidentes de seguridad, debido a la disponibilidad de los datos en un ecosistema digital susceptible a errores humanos y ataques de ciberdelincuentes. El objetivo de esta artículo es comprender los deberes legalmente atribuidos a los agentes de tratamiento de datos cuando actúan sobre los registros clínicos resultantes de atenciones realizadas mediante telemedicina. De forma más específica, pretendemos evaluar si el Consejo Federal de Medicina (CFM) y la Autoridad Nacional de Protección de Datos (ANPD) han definido criterios de seguridad con un enfoque específico para los sistemas de salud, en el marco de regulación que deriva de sus respectivas competencias normativas. Para el logro de los objetivos propuestos, se desarrollo un estudio de enfoque cualitativo, basado en revisión bibliográfica y documental. Como resultado, se constata que el ordenamiento jurídico brasileño no contempla adecuadamente los riesgos para la confidencialidad de los datos, proporcionando apenas una visión general sobre qué medidas de seguridad debe implementar un custodio, con el fin de proteger los dispositivos médicos y los Registros Electrónicos de Salud (RES).

P*alabras clave*: telemedicina; registro electrónico en salud; datos personales sensibles; protección de datos; seguridad de la información; tecnologías de la información y la comunicación.

Introdução

No ano acadêmico de 2023, no âmbito do Programa de Pós-Graduação em Direito da Universidade Federal do Piauí (UFPI), este artigo foi concebidocomo síntese dos estudos desenvolvidos pelo grupo de pesquisa "Novos Paradigmas das Relações Jurídicas Patrimonais". No curso de nossa investigação, contamos com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), vinculada ao Ministério da Educação (MEC) do Brasil.

Em dezembro de 2019, os primeiros casos de uma pneumonia viral de etiologia desconhecida foram notificados em hospitais da China, tendo por epicentro a cidade de Wuhan, província de Hubei (Wu et al, 2020). Estudos de sequenciamento de genoma completo e análise filogenética mostraram que o agente causal se tratava de um vírus de RNA de cadeia positiva, pertencente à família *Coronaviridae* (*β*-CoV *genus*) e homólogo ao patógeno causador da epidemia de SARS 2002-2004 (Organização Mundial da Saúde [OMS], 2021a). No dia 11 de março de 2020, quando 37.364 casos da infecção causada pelo novo vírus da síndrome respiratória aguda grave (SARS-CoV-2) já haviam sido reportados em 113 países ou territórios fora da China, a OMS (2020) declarou que o surto de COVID-19 constituía um evento pandêmico.

À semelhança de outras crises sanitárias, as medidas restritivas de interação física humana mostraram-se eficazes ao conter a propagação do SARS-CoV-2 e evitar o colapso dos sistemas de saúde (Petrazzuoli et al., 2021). Essas diretrizes de isolamento e distanciamento social, complementadas pela superação de barreiras regulatórias, criaram oportunidades para a prestação de cuidados por telemedicina, resultando em assistência clínica remota, viável e eficaz (Peine et al., 2020). A telemedicina, derivada da raiz grega *tele-* (distância) e do latim *medicina* (relativo à cura), constituium ramo da telessaúde que se refere ao exercício da medicina mediado por Tecnologias de Informação e de Comunicação (TICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde, conforme definido pelo Conselho Federal de Medicina (CFM) na Resolução nº 2.314/2022.

Segundo a OMS (2021b), tecnologias de suporte à telemedicina permitem o desenvolvimento de um conjunto contínuo de cuidados, com potencial para melhorar a precisão do diagnóstico, as decisões de tratamento e o ensino em saúde. Diversos estudos têm demonstrado que a telemedicina reduziu a necessidade de deslocamento físico para o atendimento (Freire et al, 2023), proporcionou benefício protetivo às equipes de saúde, possibilitando que profissionais com fatores de risco para a COVID-19 pudessem desempenhar sua atividade em trabalho remoto (Pinto et al, 2023), além de prevenir a transmissão comunitária (Accorsi et al, 2020). Há, contudo, repercussões disruptivas que merecem ser evidenciadas. A migração de serviços de saúde para o meio digital pode desencadear um impacto significativo sobre os direitos fundamentais dos pacientes, à medida que dados armazenados em formato eletrônico

tornam-se mais vulneráveis a incidentes de segurança, desencadeados quer por erros humanos, quer pela ação de cibercriminosos.

Diante dos apontamentos formulados, as linhas desta pesquisa dedicam-se a investigar a regulação jurídica dos fluxos informacionais das ações e serviços de telemedicina no contexto brasileiro. Nosso objetivo é o de compreender os deveres que legalmente se impõem aos agentes de tratamento de dados, quando estes intervêm sobre os registros clínicos resultantes de atendimentos realizados por telemedicina. Devido ao fato de esses registros se referirem ao estado de saúde de pessoas naturais, a sua qualificação como dados pessoais sensíveis exige que os controladores/custodiadores adotem medidas de segurança aptas a garantir sua confidencialidade, de acordo com as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados). Nessa perspectiva, é preciso avaliar se o ordenamento jurídico estabeleceu padrões mínimos para a salvaguarda desses dados, com base nos quais um controlador possa demonstrar, concretamente, a sua conformidade aos deveres previstos na LGPD. De forma mais específica, pretendemos inferir se o CFM e a Autoridade Nacional de Proteção de Dados (ANPD) definiram critérios de segurança com uma abordagem focalizada para os sistemas de saúde, no âmbito de regulação que decorre de suas respectivas competências normativas.

Para a consecução dos objetivos propostos, desenvolve-se um estudo de abordagem qualitativa, baseado em levantamento bibliográfico e documental. Para a discussão de base teórica, foram selecionados artigos de revisão e originais revisados por pares, indexados com os seguintes descritores: "telemedicina", "proteção de dados", "dados sensíveis", "registro eletrônico em saúde", "segurança da informação" e "incidentes de segurança". O acesso ao corpo de pesquisa se deu por intermédio das plataformas Google Acadêmico, PubMed, ScienceDirect, Elsevier, Portal de Periódicos CAPES e SciELO. As fontes documentais foram obtidas a partir do acesso ao repositório institucional da ANPD e à base de dados do Portal da Legislação, na qual são disponibilizados os atos normativos elaborados em âmbito federal, incluindo as leis ordinárias e as resoluções editadas pelo CFM.

A primeira seção analisa os conceitos fundamentais da telemedicina, distinguindo os sete contextos assistenciais em que ela pode ser exercida eticamente. Como se perceberá no segundo item, o exercício da telemedicina pressupõe deveres de cuidado específicos quanto à coleta e ao manuseio de dados, deveres que, no caso de descumprimento, podem causar danos aos direitos fundamentais dos pacientes. Por meio de um enfoque comparativo, que nos remete aos ordenamentos jurídicos do Brasil e da União Europeia, examina-se, na terceira e última seção, as normas de proteção de dados pessoais que impõem deveres de prevenção e segurança aos controladores, assim destinados a proteger os titulares contra os riscos resultantes do tratamento de dados.

1. Aportes conceituais e normativos sobre telemedicina

A telemedicina é uma modalidade da telessaúde, terminologia de escopo amplo que abrangetodas as profissões da área da saúde, regulamentadas pelos órgãos competentes do Poder Executivo federal. No ordenamento brasileiro, a telessaúde submete-se ao conjunto de normas jurídicas – constitucionais, legais e infralegais – que formam o Direito Sanitário, ramo da Ciência do Direito que tem como objetivo disciplinar as ações e os serviços de interesse à saúde (Aith, 2006). Recentemente, a promulgação da Lei nº 14.510/2022, em 28 de dezembro de 2022, marcou o reconhecimento formal da telessaúde como um conjunto de ações sustentadas para a promoção, proteção e recuperação da saúde humana, em todos os níveis de assistência, tendo como premissa central o uso das TICs.

Embora a telemedicina partilhe com a telessaúde o uso de tecnologias digitais, de informação e comunicação, para transferência de dados, textos, sons e imagens, ela está conceituada como um âmbito de atividade privativo dos médicos, conforme o disposto na Resolução CFM nº 2.314/2022. Considerando a competência normativa do CFM sobre o exercício ético da profissão médica, é razoável presumir que os deveres impostos na Resolução CFM nº 2.314/2022 tornam-se vinculativos para todos os médicos e médicas que exerçam a telemedicina, de forma síncrona ou assíncrona. Primeiro, a telemedicina síncrona possibilita uma interação médico-paciente em tempo real, explorando diversos protocolos de comunicação sem fio, tais como conexão banda larga via Wi-Fi, rede móvel 4G ou 5G, Bluetooth, uso de computador, smartphone ou notebook com câmera de vídeo e microfone (Devaraj, 2019). Na telemedicina assíncrona-tambem conhecida como pré-gravada ou de 'armazenamento e envio', os dados do paciente são gerados, armazenados e remetidos ao médico para revisão posterior, incluindo áudios, imagens, mensagens de texto e registros clínicos (Fischer & Zhou, 2021).

Conforme o artigo 5º da Resolução CFM nº 2.314/2022, as modalidades de telemedicina comprendeem: teleconsulta, teleinterconsulta, telediagnóstico, telecirurgia, telemonitoramento, teletriagem e teleconsultoria. Nos termos do art. 6º da Resolução CFM nº 2.314/2022, a teleconsulta consiste na consulta médica não presencial, mediada por TICs, com médico e paciente localizados em espaços geograficamente distintos. A teleconsulta é um serviço síncrono, feito por telefone, videoconferência e outras tecnologias de telepresença, e normalmente envolve apenas duas posições jurídicas: de um lado da comunicação, estará o paciente; do outro, um profissional legalmente habilitado ao exercício da medicina. Em determinados casos, a teleconsulta poderá envolver o esforço coordenado da equipe em ambos os pontos, com o paciente acompanhado por um familiar, responsável ou profissional de saúde local, e o médico ou a médica também pode se fazer acompanhar por um estudante ou por outro profissional da área da saúde (Weinstein; Krupinski; Doarn, 2018). Com base nos

dados transmitidos, o médico ou a médica avalia a condição clínica do paciente, define o diagnóstico e faz recomendações terapêuticas.

Por sua vez, o termo teleinterconsulta refere-se à troca digital de informações e opiniões entre médicos, com ou sem a presença do paciente, para auxílio diagnóstico ou terapêutico, clínico ou cirúrgico (Resolução CFM nº 2.314/2022, art. 7º). Sua estrutura subjetiva compõe-se de, pelo menos, dois médicos, interagindo à distância em diferentes pontos do território. A teleinterconsulta configura-se como um serviço síncrono ou assíncrono, no qual o médico consulente interage com o teleconsultor para discutir um caso clínico ou obter opinião especializada. A esse respeito, um estudo de Mantese et al (2020) analisou a oferta de teleinterconsulta no âmbito do projeto Regula+Brasil, entre os meses de janeiro e dezembro de 2019. Por meio de três canais telefônicos gratuitos, localizados em São Paulo, Porto Alegre e Brasília, neurologistas, médicos de família e outros especialistas respondiam às perguntas do médico assistente em tempo real, usando protocolos e diretrizes de medicina baseada em evidências. Com base nesse serviço, os médicos da Atenção Primária à Saúde (APS) tiveram a oportunidade de decidir, com o apoio de especialistas, se o encaminhamento ambulatorial de pacientes com condições clínicas complexas era necessário.

A terceira modalidade corresponde ao telediagnóstico, que pode ser descrito como o ato médico à distância, com a transmissão de gráficos, imagens e dados para emissão de laudo ou parecer por médico com registro de qualificação de especialista (RQE) na área relacionada ao procedimento, em atenção à solicitação do médico assistente (Resolução CFM nº 2.314/2022, art. 8º). O telediagnóstico pode ser executado de maneira simultânea ou diferida. Aqui, o paciente, assistido por profissional ou equipe de saúde, transmite imagens ou sinais fisiológicos para o médico especialista, que realiza a análise dos exames e elabora o respectivo laudo. Conforme demonstra a Pesquisa TIC Saúde 2023, 21% dos estabelecimentos de saúde do Brasil com acesso à Internet disponibilizaram serviços de telediagnóstico em 2023 (Núcleo de Informação e Coordenação do Ponto BR, 2024). Atualmente, há três Núcleos de Telessaúde que atuam na oferta de telediagnóstico por meio da Plataforma Nacional de Telediagnóstico: o de Goiás especializado em oftalmologia, o de Minas Gerais, especializado em eletrocardiograma, e o de Santa Catarina, especializado em dermatologia. Entre 2021 e 2022, esses núcleos realizaram em conjunto 1.181.237 telediagnósticos em benefício da população brasileira (Ministério da Saúde, 2022).

A quarta modalidade é a telecirurgia, caracterizada pelarealização de procedimentos cirúrgicos a distância, mediante recurso a equipamento robótico e intermediada por tecnologias interativas seguras (Resolução CFM nº 2.314/2022, art. 9º). Envolve o uso da combinação de robôs cirúrgicos e tecnologia de comunicação avançada, em que informações médicas, como dados de imagem, áudio e vídeo, são digitalizadas e transmitidas por meio de redes de telecomunicações a cabo ou sem fio (Chu et al, 2021).

Sua execução é feita por meio de dois sistemas principais: uma unidade robótica instalada em uma sala de cirurgia altamente especializada, e uma estação remota a partir da qual o cirurgião treinado opera o console cirúrgico (Navarro; Álvarez; Anguiano, 2022). No Brasil, a telecirurgia está regulamentada de forma mais específica na Resolução CFM nº 2.311/2022, exigindo, para a sua realização, a presença de pelo menos um médico portador de registro de qualificação de especialista (RQE). O arranjo subjetivo desta modalidade é dos mais complexos, e compreende o paciente, o cirurgião remoto e a equipe de cirurgia presencial, composta pelo cirurgião principal, cirurgião auxiliar, médico anestesiologista, instrumentador, enfermeiro de sala e técnico de enfermagem circulante de sala.

A quinta modalidade, designada telemonitoramento ou televigilância, consiste em um ato realizado sob a coordenação, indicação, orientação e supervisão por médico para monitoramento ou vigilância a distância de parâmetros de saúde e/ou doença, por meio de avaliação clínica e/ou aquisição direta de imagens, sinais e dados de equipamentos e/ou dispositivos agregados ou implantáveis nos pacientes (Resolução CFM nº 2.314/2022, art. 10). Em tempos recentes, o Instituto do Coração do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (InCor), atuando em parceria com a Samsung, iniciou um projeto de pesquisa com foco no telemonitoramento de pacientes nos períodos pré-operatório e pós-operatório de cirurgia cardiovascular. A partir da aferição e coleta de sinais vitais através dos *smartwatches Galaxy Watch*4, o projeto almeja a identificação de possíveis quadros de risco, o que permitiria intervir preventivamente quando detectadas irregularidades na frequência cardíaca, pressão sanguínea ou eletrocardiograma (Samsung Newsroom Brasil, 2022).

O exercício remoto da medicina inclui também ateletriagem, conceitualmente relacionada à avaliação dos sintomas do paciente, fornecendo uma impressão diagnóstica e de gravidade para fins de regulação ambulatorial ou hospitalar, com definição e direcionamento do paciente ao tipo adequado de assistência que necessita ou a um médico de especialidade (Resolução CFM nº 2.314/2022, art. 11). Durante a pandemia de COVID-19, Gadenz et al (2021) examinaram a implantação de teletriagens, dentro do escopo do projeto Regula+Brasil, que promove a regulação do referenciamento de casos por meio de revisão do conteúdo clínico registrado na solicitação de encaminhamento. Entre maio de 2020 e maio de 2021, os times de enfermagem e os operadores de atendimento realizaram a triagem de 26.130 encaminhamentos presentes nos sistemas de regulação, das quais 8.952 originaram teleconsultas médicas. A triagem remota permitiu compreender melhor as condições clínicas em que os pacientes se encontravam, identificando, inclusive, situações de urgência, como precordialgias típicas, alterações cognitivas agudas e ideações suicidas.

Por fim, a teleconsultoria consiste no ato de consultoria mediado por TICs entre médicos, gestores e outros profissionais de saúde, com a finalidade de prestar

esclarecimentos sobre procedimentos administrativos e ações de saúde (Resolução CFM nº 2.314/2022, art. 12). No âmbito do Programa Nacional Telessaúde Brasil Redes, em Santa Catarina, por exemplo, especialistas em Saúde da Família ou Saúde Coletiva fornecem teleconsultoria de processo de trabalho, coordenação ou gestão, em área digital restrita (Minghelli et al, 2023). O fluxo é iniciado quando um profissional da APS cria um pedido de apoio, descrevendo detalhadamente o caso. A seguir, o teleconsultor designado faz uma avaliação da demanda e gera uma resposta com recomendação de conduta para o profissional, no que se refere à organização do trabalho no contexto da Atenção Básica.

Procedemos, assim, à análise dos contextos assistenciais em que a telemedicina pode ser empregada eticamente, nos termos da Resolução CFM nº 2.314/2022. Em vista dessas modalidades, poderemos enfim compreender, na discussão posterior, como os sistemas de telemedicina tornam possível a coleta, o armazenamento e a transmissão de dados relativos à saúde.

2. Os estágios do fluxo informacional em serviços de telemedicina

Em toda avaliação clínica-seja-ambulatorial ou hospitalar -o profissional médico necessita obter informações individualizadas sobre o paciente para formular hipóteses diagnósticas, reconhecer uma entidade nosológica (doença) e definir medidas de prevenção, reabilitação ou intervenção terapêutica. Ao investigar as causas das doenças, o profissional de saúde examina as regiões do corpo do paciente, em busca de achados anormais que subsidiem a tomada de decisão clínica e todos os atos dela decorrentes. Em sua forma maiselementar, tais dados podem comunicar informações sobre processos patológicos, que envolvem doenças de uma estrutura ou sistema corporal (infecções bacterianas, virais ou fúngicas). Outros dados revelam um quadro clínico associado à desestruturação de funções biológicas, como é o caso da perda da função motora, ou tecem representações de processos psicopatológicos, sendo esta a hipótese dos transtornos psiquiátricos (Bickley, 2018).

Enquanto expressam informações referentes ao processo saúde-doença, tais dados também se vinculam a fenômenos psíquicos que causam desmesurado sofrimento – a vergonha, a culpa, a melancolia e a angústia. Como bem ressalta Sérgio Deodato (2017, p.63), ao profissional de saúde "revelam-se dados de vida que se encontram frequentemente escondidos das relações sociais estabelecidas, mesmo nas mais próximas e íntimas". Muitas dessas informações podem ser delicadas, constrangedoras ou particularmente dolorosas, e ao paciente é garantido o direito de decidir se deseja mantê-las em sigilo. Trata-se de um núcleo de dados pessoais altamente sensíveis, devido ao risco de uso discriminatório contra as pessoas a quem se referem, suas famílias e comunidades, ou grupos específicos. Uma violação desses dados poderá refletir consequências graves sobre os seus titulares, como estigmatização, exclusão

ou segregação, bem como ter impacto no emprego, nas relações familiares e no estatuto socioeconômico (Lorenzini; Shaw; Elger, 2022).

Por constituírem fonte de conhecimento sobre a intimidade de uma pessoa singular, identificada ou identificável, os dados em saúde reclamam uma forte base legal e regulatória para proteger a sua confidencialidade, integridade e disponibilidade (OMS, 2021b). Nessecontexto, o Código de Ética Médica dedica um capítulo à normatização do sigilo profissional, sendo vedado ao médico, nos termos do artigo 73, revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento do paciente. Da mesma forma, o dever de sigilo profissional abrange as informações relacionadas a paciente criança ou adolescente, desde que este tenha capacidade de discernimento (artigo 74), e as informações obtidas quando do exame médico de trabalhadores (artigo 76). No desempenho da medicina, o profissional de saúde não deverá fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou na divulgação de assuntos médicos em meios de comunicação (artigo 75).

No Brasil, a Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, inciso II, qualifica como sensíveis os dados concernentes à saúde, quando vinculados a uma pessoa singular. Disposição semelhante pode ser encontrada no artigo 9(1) do Regulamento (UE) 2016/679 (Regulamento Geral de Proteção de Dados - RGPD), texto de referência em matéria de proteção de dados na União Europeia, que considera os dados relativos à saúde uma categoria específica e estatui vedação geral ao seu tratamento. A concepção de um direito à proteção de dados, conforme delineado por Mafalda Miranda Barbosa (2017), revela-se fundamental para a salvaguarda de vários direitos da personalidade do titular dos dados – a privacidade, a identidade, a igualdade, a honra, a imagem. Buscando compreender as repercussões desse direito na telemedicina, as linhas subsequentes examinam o ciclo de vida da informação em saúde e os riscos que podem emergir de algum dos seus estágios.

O primeiro estágio do ciclo de vida da informação em saúde é a coleta. Quanto a isso, os Organismos Produtores de Serviços de Atenção à Saúde (OPSAS) são responsáveis por receber, produzir e organizar os registros informacionais em saúde, em razão dos atendimentos ofertados à comunidade nos serviços de saúde públicos e privados (Cunha et al, 2022). Dados derivados de consultas e procedimentos médicos constituem uma fonte significativa das informações em saúde. No atendimento presencial, a coleta desses dados tem inicio com o levantamento do perfil sociodemográfico do paciente, seguido por informações antropométricas, sinais vitais, dados de anamnese, achados do exame físico e resultados de exames complementares. No ato de telemedicina, por outro lado, os médicos interagem com pacientes situados

em estações remotas, usando tecnologias de informação e comunicação para recolher sons, textos e imagens sobre o seu estado de saúde.

Dado que a relação médico-paciente seestabelece virtualmente, o dever de identificação e autenticação impõe que o prestador de cuidados de saúde cumpra com oportunos e adequados procedimentos de verificação de identidade (Lecaros-Urzúa; López-Gaete, 2023). Ao longo de uma teleconsulta, os dados clínicos serão gerados, basicamente, a partir da anamnese e da observação de sinais, exceto nas especialidades que independem do exame físico ou que possibilitam o envio de imagens para revisão posterior. Se for necessário, o médico ou a médica poderá requisitar exames complementares (de imagem, laboratoriais, endoscópicos) com vistas a ampliar sua investigação. Após a anamnese e o exame físico, o profissional médico formula sua avaliação clínica vinculando os sintomas e achados anormais a um processo fisiopatológico ou psicopatológico de base, o que lhe permite definir um diagnóstico nosológico, seguido por um plano direcionado para esse problema (Bickley, 2018). Por fim, a prescrição é emitida de forma eletrônica.

Este é o quadro generativo básico da teleconsulta. Os preceitos da Resolução CFM nº 2.314/2022 sugerem que um fluxo semelhante se aplica à aquisição de dados em teleinterconsulta, com a ressalva de que, nesta modalidade, o próprio médico ou médica assistente encarrega-se de coletar e transmitir os registros para um especialista adequadamente selecionado (artigo 7º da Resolução CFM nº 2.314/2022). Em televigilância, ocorre o monitoramento continuo de parâmetros fisiológicos dos pacientes, mediante uso de dispositivos vestíveis ou implantáveis baseados em biotelemetria. A fase de aquisição desses dados é caracterizada pelo uso de sensores sem fio, que detectam e convertemsinais fisiológicos em impulsos elétricos, tais como pulseiras inteligentes, bombas de insulina e smartwatches (Morales; Ourique; Cazella, 2021). Quanto ao telediagnóstico, dados e imagens digitais do paciente são coletados localmente por um médico responsável com o auxílio de equipamentos e, então, remetidos ao tele-especialista para emissão de laudo a distância. São exemplos os laudos resultantes de informações capturadas por eletrocardiograma, telerradiografia, ultrassonografia e telepatologia.

No que concerne à telecirurgia, existem três elementos determinantes para a aquisição de dados: uma plataforma de cirurgia robótica, uma equipe assistencial treinada e uma tecnologia interativa segura de alta velocidade. De acordo com a Resolução CFM nº 2.311/2022, compete ao cirurgião remoto o manejo do console e dos instrumentais robóticos durante a realização da telecirurgia. Ao ser posto em funcionamento, esse sistema (mestre) processa um volume massivo de dados provenientes da instrumentação cirúrgica, transmite-os para a unidade do paciente (servo) e recebe os dados de retorno gerados pelo endoscópio, que é fixado a qualquer um dos braços robóticos. Desse modo, um dos principais problemas da telecirurgia é o tempo de latência, ou

tempo necessário para enviar e receber os dados auditivos, visuais e táteis entre duas estações, qualquer que seja a distância que as separa. Elevados tempos de latência podem ocasionar operações demoradas, imprecisão cirúrgica e risco à integridade dos pacientes (Wu et al, 2023). Para evitar problemas dessa ordem, o artigo 6º, § 1º, da Resolução CFM nº 2.311/2022 exige que a telecirurgia seja realizada em hospital de alta complexidade, com banda de comunicação eficiente e redundante, estabilidade no fornecimento de energia elétrica e segurança contra ataques cibernéticos.

Em teletriagem, ato de acolhimento e classificação de risco, os médicos reúnem evidências suficientes para formar uma impressão diagnóstica sobre o paciente, colocá-lo em ordem de prioridade para o atendimento ou referenciá-lo ao serviço assistencial adequado. Embora a teletriagem não se confunda com a consulta médica (artigo 11, §1º, da Resolução CFM nº 2.314/2022), sua camada de aquisição é muito semelhante à da teleconsulta, precisamente no que diz respeito às TICs, que podem envolver tecnologias de telepresença ou videotransmissão síncrona. Finalmente, é possível realizar uma teleconsultoria de forma síncrona ou diferida, utilizando diferentes protocolos de comunicação, quando um médico, um gestor ou outro profissional da área da saúde solicita esclarecimentos sobre procedimentos administrativos e ações de saúde.

À medida que se avança no ciclo de vida da informação, torna-se necessário registrar o conhecimento gerado em algum suporte documental, a exemplo do prontuário do paciente (PP), das folhas de requisição de exames, dos relatórios de quimioterapia e radioterapia, dos formulários de notificação compulsória de doenças e agravos em saúde, entre outras tipologias. Como pressuposto de conduta, o artigo 3º, § 3º, da Resolução CFM nº 2.314/2022 estabelece que os dados relacionados ao atendimento por telemedicina devem permanecer sob a guarda do médico assistente, em consultório próprio, ou do diretor/responsável técnico, se houver interveniência de empresa ou instituição prestadora de cuidados de saúde. Esses agentes são compreendidos como custodiadores das informações orgânicas em saúde. O custodiador tem por responsabilidade a custódia física e legal dos documentos arquivísticos, a preservação de sua autenticidade, bem como a garantia do acesso contínuo às cópias de registros do criador ou produtor (Meirelles; Cunha, 2020).

Nos termos do artigo 3º, § 1º, da Resolução CFM nº 2.314/2022, o registro do teleatendimento pode ser feito por meio de prontuário físico ou de Sistemas de Registro Eletrônico de Saúde (SRES). A tipologia documental prontuário, ou registro clínico do paciente, refere-se a um documento escrito, ético-legal e multidisciplinar, com um propósito duplo: reflete o raciocínio clínico do examinador e documenta os dados relativos ao atendimento prestado pelas equipes de saúde (Bickley, 2018). De acordo com o artigo 87, § 1º, do Código de Ética Médica, registram-se nesse documento os dados necessários para a boa condução do caso (anatômicos, fisiológicos, patológicos, histopatológicos, anatomopatológicos), sendo preenchido, em cada avaliação,

em ordem cronológica com data, hora, assinatura e número de registro do médico no Conselho Regional de Medicina (CRM) de sua jurisdição.

Contrapondo-se aos prontuários em suporte físico, os Registros Eletrônicos de Saúde (RES) são repositórios de informações interoperáveis sobre a assistência prestada ao indivíduo, acumuladas e disseminadas a múltiplos agentes de saúde com fins de potencializar a criação do conhecimento, aprendizagem e suporte às intervenções assistenciais e administrativas (Cunha et al, 2022). De acordo com a Sociedade Brasileira de Informática em Saúde (SBIS, 2020), a definição de um SRES é bastante ampla, e engloba todos os subsistemas e componentes de software necessários para implementação de suas funcionalidades, tais como o sistema de gerenciamento de banco de dados (SGBD), o sistema de prescrição eletrônica ou videoconferência integrados ao SRES, e o sistema de diretórios utilizado para armazenar parâmetros de usuários, papéis e grupos. Neste caso, os dados e imagens do paciente são armazenados numa base de dados acessível aos médicos, durante todo o período de vigência legal da sua preservação (artigo 3º, §8º, da Resolução CFM nº 2.314/2022).

Um terceiro estágio importante diz respeito a quem tem acesso a esses dados e quem, em última análise, recebe as informações resultantes do seu processamento. O acesso a essas informações pode ocorrer por meio de estruturas de transferência de informações nos sistemas e nas redes de atenção à saúde, compreendendo os repositorios arquivísticos locais dos OPSAS, os Sistemas de Informação em Saúde (SIS) de base nacional, integrados ao Portal do Departamento de Informática do Sistema Único de Saúde (DATASUS), e os bancos de dados da Agência Nacional de Saúde Suplementar (ANS) (Meirelles; Cunha, 2020). Sistemas de RES poderão ser desenvolvidos localmente pelas equipes de Tecnologia da Informação (TI) das Secretariais Estaduais e Municipais de Saúde. Em outros casos, os OPSAS utilizam soluções de software desenvolvidas pelo DATASUS, e o armazenamento dos dados ocorre em bases centralizadas no Ministério da Saúde. Pode ocorrer, ainda, que o agente de tratamento utilize os serviços de um servidor de terceiros para armazenar os dados do paciente, um processo denominado terceirização de dados.

Resulta que, em virtude dessa disponibilidade em um ecossistema digital, grande parte dos RES está mais vulnerável à ocorrência de incidentes de segurança. O art. 48 da LGPD, interpretado em sintonia com o art. 46, emprega o termo "incidente de segurança" para referir-se a acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O conceito em causa é correspondente ao de "violação de dados pessoais" enunciado no art. 4(12) do RGPD. Neste texto, preferiu-se o recurso à terminologia incidente de segurança, de abrangência mais vasta, uma vez que o evento assim qualificado pode ter outras consequências além da violação de dados.

Alguns incidentes de segurança são o resultado de erros humanos, como a digitação incorreta de um comando ou a divulgação inadvertida de senhas na internet (Herrmann; Pridöhl, 2020). Em contrapartida, os atos maliciosos ou intencionais – também chamados de ataques – ocorrem quando adversários exploram as vulnerabilidades presentes em um sistema de informação ou utilizam técnicas de engenharia social para ter acesso não autorizado às bases de dados. A título de ilustração, em agosto de 2022, o *Centre Hospitalier Sud Francilien* (CHSF) em Corbeil-Essonnes, a sudeste de Paris, França, foi alvo de um ataque cibernético que paralisou seu sistema de armazenamento e o sistema relativo à admissão de pacientes. Devido à indisponibilidade dessas plataformas, o fluxo ambulatorial e a sala de operações foram temporariamente comprometidos. Três semanas depois do ataque, o coletivo de hackers Lockbit 3.0 reivindicou a responsabilidade pela inserção de um ransomware criptográfico nas bases de dados do CHSF. Além de exigirem um resgate de 10 milhões de doláres, os cibercriminosos ameaçaram divulgar mais de um milhão de dados sequestrados (Caruso & Cosson, 2022).

O incidente suportado pelo *Centre Hospitalier Sud Francilien* é um exemplo de ransomware ou ataque de extorsão. Ele consiste em uma variante de software malicioso projetada com módulos criptográficos, que tem por finalidade o sequestro dos dados críticos de uma organização, tornando-os inacessíveis e exigindo o pagamento de resgate (em inglês, ransom) para restabelecer o acesso (Reshmi, 2021). Dessa forma se produziria a primeira consequência de um ataque: a violação da confidencialidade. Quem rompe as defesas de um sistema, possivelmente faz o download dos registros dos pacientes para depois vendê-los em uma área profunda da Internet, chamada de dark web. Os dados roubados podem ser vendidos a outro criminoso, que os usará para extorquir o hospital (Wasserman & Wasserman, 2022).

A segunda consequência a ser considerada diz respeito à interrupção dos serviços. Depois do sequestro, os adversários ameaçam lançar um ataque de negação de serviço distribuída (DDoS) contra o estabelecimento de saúde. Esses ataques – que operam por inundação de tráfego da rede – enviam múltiplas solicitações de serviço à rede do alvo, exaurindo a banda disponível ou a capacidade computacional do servidor (Khalaf et al., 2019). Se executados isoladamente, sua finalidade não consiste em roubar, criptografar ou corromper dados sigilosos, mas impedir o funcionamento do serviço e o acesso às bases de dados, ocasionando prejuízos financeiros ou danos à reputação de um concorrente.

Se prosseguirmos com esta análise, perceberemos que ataques cibernéticos aos estabelecimentos de saúde impõem riscos não apenas à privacidade, mas, em algumas circunstâncias, tais incidentes representam um risco geral à vida e à integridade física das pessoas. Assim ocorre quando comprometem sistemas de informação existentes em hospitais com leitos cirúrgicos e Unidades de Terapia Intensiva (UTI), impedin-

do que as equipes de saúde acessem os prontuários e prestem assistência oportuna. Em outros casos, as informações geradas por dispositivos de televigilância podem ser interceptadas e adulteradas por um invasor, e, como consequência, o ataque pode implicar na morte do paciente (Zanon et al, 2022). Por último, incidentes de segurança precipitam uma série de despesas com a transição para protocolos de emergência, a reparação ou recuperação dos sistemas afetados, as ações judiciais subsequentes e a comunicação do incidente de segurança (Wasserman & Wasserman, 2022).

Cada um dos fluxos informacionais que descrevemos está suscetível a diferentes vulnerabilidades, que podem se tornar o ponto de partida para uma violação dos dados transmitidos ou armazenados em SRES. Diante dos riscos que a investigação pretendeu elucidar, os sistemas de saúde são obrigados a pôr-se em defesa contra essas ameaças, conforme será apresentado na terceira seção.

3. A segurança da informação na assistência remota à saúde

Conforme exposto anteriormente, a legislação brasileira sobre proteção de dados impõe uma série de deveres aos controladores, assim destinados a proteger os titulares contra os riscos resultantes do tratamento de dados. Conforme dispõe o art. 47 da LGPD, qualquer interveniente em uma das fases do tratamento obriga-se a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término. Segundo Dominik Herrmann e Henning Pridöhl (2020), a segurança da informação visa atender a três objetivos: confidencialidade (impedir a obtenção não autorizada de dados e de qualquer informação derivada da sua interpretação), integridade (impedir ou detectar a modificação não autorizada) e disponibilidade (impedir a exclusão ou a interrupção não autorizada).

Diante desses apontamentos, o artigo 46 da LGPD preceitua que medidas de segurança, técnicas e administrativas, devem ser adotadas pelos agentes de tratamento a fim de proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas que resultem na destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Oparágrafo segundo estabelece que tais medidas de segurança devem ser implementadas tanto na fase de concepção do produto ou do serviço, quanto na fase de sua execução. De forma análoga, o artigo 25 do RGPD introduz o conceito de " proteção de dados desde a concepção e por padrão" (em inglês, *data protection by design and by default*), assegurando que o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, medidas técnicas e organizativas para que os dados pessoais não sejam disponibilizados a um número indeterminado de pessoas.

Segundo Ann Cavoukian (2013), o conceito de privacidade desde a concepção enfatiza a necessidade de ser proativo, ao considerar os requisitos de privacidade na fase de concepção e durante todo o ciclo de vida dos dados. Sua abordagem é caracterizada

por medidas proativas, eis que antecipa e evita eventos invasivos à privacidade, antes que eles aconteçam. Como bem ressalta Bruno Bioni (2022), ao prescrever que "*privacy by design*" é uma obrigação dos agentes de tratamento de dados, a LGPD obriga-os a procedimentalizar um fluxo informacional de acordo com as normas de proteção de dados e, com isso, garantir que a conformidade regulatória se dê em toda a sua extensão. A relevância dessa diretriz foi expressamente reconhecida pelo legislador brasileiro no inciso VIII do artigo 6ºda LGPD, identificando-a com o princípio da prevenção, pelo que resulta exigível do controlador a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Ao nível da estrutura normativa da LGPD, uma das obrigações atribuídas ao controlador consiste na elaboração do relatório de impacto à proteção de dados pessoais (RIPDP), documento correspondente à avaliação de impacto sobre a proteção de dados prevista no art. 35(1) do RGPD. O artigo 38, parágrafo único, da LGPD, dispõe que o controlador deve descrever os tipos de dados coletados, a metodologia utilizada para a coleta, os riscos a direitos fundamentais resultantes da sua atividade de tratamento de dados, bem como as medidas de segurança, salvaguardas e mecanismos de mitigação de risco adotados. Diferentemente do Regulamento Europeu, o texto da LGPD não menciona em quais hipóteses os relatórios de impacto seriam de elaboração obrigatória, nem define quais atividades de tratamento seriam consideradas de alto risco (Mendes; Bioni, 2019). Foi o Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD) que, exercendo a competência regulatória prevista no artigo 55-J, incisos XIII e XVIII, da LGPD, dedicou um capítulo da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022 para definir hipóteses tratamento de alto risco. Essas hipóteses foram nitidamente inspiradas no Considerando 91 e no artigo 35(3) do RGPD, que definem quando uma avaliação de impacto sobre a proteção de dados deve ser realizada. Nos termos da mencionada resolução, será considerado de alto risco o tratamento de dados pessoais que atender, cumulativamente, a pelo menos um critério geral e um critério específico previstos no seu artigo 4º. A observância desses critérios revela que qualquer tratamento de dados realizado no contexto de telemedicina pode ser classificadocomo de alto risco.

Isto porque haveria, em qualquer caso, um tratamento capaz de afetar significativamente interesses e direitos fundamentais dos pacientes, considerando que o setor de saúde projeta formas particulares de estigma e discriminação associadas aos processos de saúde-doença (artigo 4º, I, b). Com isso, atende-se a pelo menos um dos critérios gerais. De outro lado, o primeiro requisito específico já seria suficiente para atestar o risco, na medida em que o exercício da telemedicina está baseado no uso de tecnologias emergentes ou innovadoras (artigo 4º, II, a). A telemedicina também satisfaz o quarto requisito específico, pois o seu exercício implica o tratamento de informações sensíveis relativas ao estado de saúde das pessoas (artigo 4º, II, d). Devido às singularidades dos sistemas de saúde, seria desejável que a ANPD editasse

uma resolução específica sobre a elaboração de RIPDP, quando a atidade de tratamento tiver por objeto dados concernentes à saúde.

Fundamentando-se na avaliação de impacto dos riscos que o tratamento implica, o artigo 32(1) do RGPD enuncia que os agentes são obrigados a implementar medidas técnicas e organizativas adequadas para assegurar um nível de segurança ajustado ao risco. Tais medidas devem possibilitar, conforme o caso, a pseudonimização e a criptografia dos dados, a confidencialidade, integridade, disponibilidade e resiliência dos sistemas, a capacidade de restabelecer o acesso aos dados pessoais no caso de um incidente, bem como definir um processo para avaliar regularmente a eficácia das medidas. No que se refere à LGPD, observa-se que o artigo 46 não trouxe um conjunto mínimo de condições que precisam ser atendidas para garantir a segurança do tratamento. Apesar de o artigo 46, §1º, da LGPD prever a possibilidade de a Autoridade Nacional estabelecer padrões técnicos mínimos de segurança, especialmente nas hipóteses em que se processam dados sensíveis, nenhum regulamento voltado para a telemedicina – ou para o setor de saúde em geral – foi editado até o momento.

Uma terceira obrigação relacionada à segurança dos dados pessoais é a resposta do controlador aos incidentes de segurança. O artigo 48 da LGPD impõe ao controlador o dever de comunicar à Autoridade Nacional e ao titular, em prazo razoável, a ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos titulares. De acordo com o artigo 5º da Resolução CD/ANPD nº 15, de 24 de abril de 2024, um incidente precisa ser comunicado quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver dados pessoais sensíveis, dados de crianças, de adolescentes ou de idosos, dados financeiros, dados de autenticação em sistemas, dados protegidos por sigilo fiscal, judicial ou profissional, ou dados em larga escala. Um ataque cibernético aos sistemas de um hospital, por exemplo, pode não ser capaz de causar risco relevante aos titulares, se nenhum RES for violado e nenhum serviço de saúde interrompido.

De forma semelhante, o art. 33(1) do RGPD prevê que, em caso de violação de dados pessoais, o responsável pelo tratamento notificará a ocorrência do fato à autoridade de controle competente e, sempre que possível, até 72 horas após ter tido conhecimento do incidente, à exceção das hipóteses em que a violação dos dados pessoais não represente risco aos direitos e liberdades das pessoas singulares. Em continuidade, nos termos do art. 33(5) do RGPD, impõe-se ao responsável pelo tratamento o dever de documentar quaisquer violações de dados pessoais, abrangendo os fatos associados ao incidente, os respectivos efeitos e as medidas de reparação adotadas. É igualmente obrigatória a comunicação aos titulares dos dados, conforme previsto no artigo 34(1) do RGPD, quando uma violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas afetadas.

Por tudo o que se mencionou, a LGPD e o RGPD nos remetem para o conceito de *role-responsibility*, conforme proposto por H.L.A. Hart (2008) em seu pós-escrito do texto P*unishment and* R*esponsibility*. Quer isto dizer que, sempre que uma pessoa ocupa um cargo distinto em uma organização, ao qual estão associados deveres específicos, diz-se que ela é responsável por fazer o que é necessário para cumpri-los. Tais deveres, segundo Hart (2008), correspondem às responsabilidades de uma pessoa. Trata-se do sentido a que se refere o RGPD, em seu artigo 4(7), ao designar o responsável pelo tratamento de dados como aquele que determina as finalidades e os meios de tratamento. No direito brasileiro, o controlador é legalmente responsável pela eliminação dos dados após o término do tratamento (artigo 16 da LGPD), pelo registro das operações de tratamento (artigo 37), pela elaboração do relatório de impacto à proteção de dados pessoais (artigo 38), pela adoção de medidas de segurança, técnicas e administrativas (artigo 46), bem assim pela formulação de regras de boas práticas e de governança (artigo 50).

A consequência da violação de algum desses deveres, como nos ensina Mafalda Miranda Barbosa (2017), é que um controlador pode tornar-se civilmente responsável pela reparação dos danos que deveriam ser evitados. Naturalmente, os médicos têm o dever de confidencialidade para com os seus pacientes, e a violação deste dever pode dar origem à responsabilidade civil. Os demandantes podem argumentar que a divulgação, perda, alteração ou acesso não autorizado de seus prontuários constitui uma violação do sigilo profissional, com base no art. 73 do Código de Ética Médica. O titular dos dados pode alegar, ainda, que um custodiador violou o dever de diligência ao deixar de implementar medidas de segurança adequadas ao risco, nos termos do art. 46 da LGPD, causando danos materiais ou imateriais ao paciente. Para que se determine o nexo de causalidade e, portanto, para que se impute uma obrigação reparatória ao agente responsável, é preciso verificar em que medida se deu o cumprimento dos deveres estabelecidos na LGPD, ou seja, quais medidas de segurança foram adotadas, se existem regras de boas práticas, relatórios de impacto, planos de resposta a incidentes e/ou programa de governança em privacidade integrados ao serviço de saúde.

Contudo, ao buscar referências especificas para aa telemedicina, encontrou-se- uma penumbra normativa em torno das questões relacionadas à privacidade e à segurança da informação. Apesar de todos os deveres impostos ao controlador, a LGPD não parece ter feito um esforço especial para orientá-lo sobre a modelagem dessas medidas de segurança. Consoante refere Lee A. Bygrave (2015), as leis de proteção de dados são formuladas utilizando uma terminologia demasiadamente aberta. Ao incorporar em seu texto conceitos genéricos ou tecnologicamente neutros, diz Bygrave (2015), os legisladores esperam que as leis resistam às contingências do desenvolvimento industrial, sem que a sua interpretação e aplicação fiquem vinculadas a uma tecnologia específica. Se, por um lado, essa imprecisão de linguagem amplia

a longevidade das normas, evitando que sejam constantemente revistas, por outro, ela também concede ao controlador uma margem ampla de discricionariedade para decidir sobre a tessitura das operações de tratamento.

Na hermenêutica da LGPD, o significado e o escopo do termo ' medidas de segurança' permanecem indefinidos no texto legal. Um controlador que se baseia somente na literalidade do artigo 46 dificilmente será capaz de atingir um nível de segurança adequado aos riscos provenientes do seu fluxo informacional. Diante dessa concepção, é digno de nota que a ANPD tenha decidido publicar, ainda em 2021, um guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte (ANPD, 2021). Nesse guia, a ANPD considera que as medidas de segurança do art. 46 podem traduzir-se tanto na definição de práticas administrativas (política de segurança da informação, treinamento de equipes, gerenciamento de contratos), quanto na adoção de ferramentas técnicas (controle de acesso por senha, biometria ou autenticação multi-fatores, criptografia da base de dados, antivírus, firewall e medidas relacionadas ao uso de dispositivos móveis e serviços em nuvem).

Porém, um ato normativo dessa natureza – sem efeito vinculante, endereçado apenas aos agentes de tratamento de pequeno porte – não aborda corretamente os riscos à confidencialidade dos dados em telemedicina. Os sistemas de saúde no Brasil constituemdomínios particularmente complexos, com ampla diversidade de atuação e estrutura de governança. Examinando mais detidamente a abrangência e complexidade do SUS, por exemplo, distinguimos que seus fluxos informacionais são volumosos, heterogêneos e envolvem múltiplos atores distribuídos em três níveis de gestão (federal, estadual e municipal) e no âmbito da Saúde Complementar. Todos estes atores podem, potencialmente, desenvolver ações e serviços de telemedicina, seja de forma direta, seja por intermédio dos programas de telessaúde vigentes no país. Dada a vagueza com que o legislador brasileiro decidiu enunciar as normas relativas à segurança e ao sigilo de dados, seria desejável que a ANPD exercesse sua competência normativa na formulação de normas técnicas e estabelecimento de padrões mínimos para a segurança dos dados, com uma atenção focalizada para os sistemas de saúde.

Por fim, os antecedentes desta pesquisa permitem concluir que o Conselho Federal de Medicina fornece apenas uma visão geral – incompleta e inconclusiva – sobre quais salvaguardas um custodiador deve implementar a fim de proteger os dispositivos médicos e os Registros Eletrônicos em Saúde. Tais normas podem exigir que os dados do teleatendimento sejam registrados atendendo a padrões de integridade, confidencialidade e garantia do sigilo profissional, mas elas não proporcionam a padronização de processos internos ou a integração dos fluxos informacionais da telemedicina com medidas de segurança específicas para as sete modalidades. Como consequência, a definição desess parâmetros acaba por depender da discricionariedade dos próprios sistemas de saúde, marcados por inúmeras desigualdades no acesso à tecnologia e na gestão de sistemas informáticos.

Conclusões

Ao longo desta investigação, demonstrou-se que os sistemas de telemedicina são particularmente suscetíveis à ocorrência de incidentes de segurança. Além da violação dos dados armazenados em Registros Eletrônicos de Saúde (RES) ou dispositivos médicos, tais ataques podems igualmente interromper a prestação de serviços de telemedicina, ao impedir o acesso das equipes aos prontuários e tecnologias digitais de interação com os pacientes. Como mencionado anteriomente, cada prontuário reúne dados que refletem informações sensíveis sobre a saúde de uma pessoa, e, por isso, os médicos e as médicas que com eles tiveram contato resultam sujeitos ao dever de sigilo profissional. Adicionalmente, a LGPD impõe aos controladores o dever de adotar medidas preventivas, desde a fase de concepção, contra acessos não autorizados e situações acidentais ou ilícitas que envolvam a destruição, perda, alteração ou comunicação de dados pessoais.

Apesar dos diversos deveres previstos para os controladores, observa-se que a LGPD não fornece diretrizes especificas sobre a modelagem das medidas de segurança que, se bem implementadas, poderiam garantir a segurança e o sigilo de dados. E, embora o artigo 46, §1º, da LGPD estabeleça que a Autoridade Nacional poderá dispor sobre padrões técnicos mínimos de segurança, especialmente nas hipóteses em que se processam dados sensíveis, nenhum regulamento voltado para a telemedicina – ou para o setor de saúde em geral – foi editado até o momento. A ausência de padrões mínimos de segurança compromete a aplicação prática da LGPDe dificultaa atuação do julgador na análise de eventuais litígios de responsabilidade civil, avalie se as medidas adotadas pelo controlador cumprem, ou não, com as exigências do ordenamento jurídico.

Conclui-se, portanto, que há necessidade premente de uma normatização mais robusta sobre o tema. Desse modo, as escolhas do controlador/custodiador seriam feitas com base em parâmetros mais consistentes, e a confidencialidade das informações em saúde seria mais bem protegida, em todo e qualquer estágio dos serviços prestados por telemedicina. Uma regulação nesse sentido revela-se imprescindível para fortalecer a confiança dos usuários nos serviços de saúde, bem como para viabilizara prestação de cuidados mais precisos, centrados no paciente e baseados em evidências.

Referências

Accorsi, T. A. D., Amicis, K. D., Brígido, A. R. D., Belfort, D. de S. P., Habrum, F. C., Scarpanti, F. G., Magalhães, I. R., Silva Filho, J. R. de O., Sampaio, L. P. C., Lira, M. T. S. de S., Morbeck, R. A., Pedrotti, C. H. S. & Cordioli, E. (2020). Assessment of patients with acute respiratory symptoms during the COVID-19 pandemic by Telemedicine: clinical features and impact on referral. *Einstein (São Paulo)*, *18*, eAO6106. https://doi.org/10.31744/einstein_journal/2020AO6106

Aith, F. M. A. (2006). *Teoria Geral do Direito Sanitário Brasileiro* [tese doutoral, Universidade de São Paulo]. Biblioteca Digital USP. https://doi.org/10.11606/T.6.2006.tde-23102006-144712

Autoridade Nacional de Proteção de Dados. (2024, 26 de setembro). *Resolução* CD/ANPD *nº* 2, *de* 27 *de janeiro de* 2022. *Aprova o Regulamento de aplicação da Lei nº* 13.709, *de* 14 *de agosto de* 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), *para agentes de tratamento de pequeno porte*. Diário Oficial da União de 26/09/2024. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022

Autoridade Nacional de Proteção de Dados. (2024, 24 de abril). *Resolução* CD/ANPD *nº* 15, *de* 24 *de abril de* 2024. *Aprova o Regulamento de Comunicação de Incidente de Segurança*. Diário Oficial da União de 26/04/2024. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

Barbosa, M. M. (2017). Proteção de dados e direitos de personalidade: Uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil. AB *Instantia* 5(7), 13-47. https://abreuadvogados.com/conhecimento/publicacoes/instituto-do-conhecimento/protecao-de-dados-e-direitos-de-personalidade-uma-relacao-de-interioridade-constitutiva/

Bickley, L. S. (2018). *Bates Propedêutica Médica* (12. ed.). Guanabara Koogan.

Bioni, B. R. (2022). *Regulação e Proteção de Dados Pessoais*: O *Princípio da Accountability*. Editora Gen Forense.

Bygrave. L. A. (2015). Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxford Journal of Legal Studies*, *35*(1), 91-120. https://doi.org/10.1093/ojls/gqu011

Caruso, D. L. & Cosson, N. (2022, 12 de setembro). *Hôpital de Corbeil-Essonnes: le groupe russophone Lockbit* 3.0 *revendique la cyberattaque et lance un chantage aux données*. Le Parisien. https://www.leparisien.fr/high-tech/hopital-de-corbeil-essonnes-le-groupe-russophone-lockbit-30-revendique-la-cyberattaque-et-lance-le-chantage-aux-donnees-12-09-2022-7IM7PZYIYNFPVBIJXYVUNXZPOI.php

Cavoukian, A. (2013). Privacy by Design: Leadership, Methods, and Results. In Gutwirth, S., Leenes, R., de Hert, P. & Poullet, Y. (eds) *European Data Protection: Coming of Age* (pp 175-202). https://link.springer.com/chapter/10.1007/978-94-007-5170-5_8

Chu, G., Yang, X., Luo, L., Feng, W., Jiao, W., Zhang, X., Wang, Y., Yang, Z., Wang, B., Li, J. & Niu, H. (2021). Improved robot-assisted laparoscopic telesurgery: feasibility of network converged communication. *The British journal of surgery*, *108*(11), e377–e379. https://doi.org/10.1093/bjs/znab317

Conselho Federal de Medicina (CFM). (2018, 27 de setembro). *Resolução CFM nº 2217, de 27 de setembro de 2018. Código de Ética Médica*. Diário Oficial da União de 27/09/2018. https://portal.cfm.org.br/images/PDF/cem2019.pdf

Conselho Federal de Medicina (CFM). (2022, 28 de março). *Resolução CFM nº* 2.311, *de* 28 *de março de 2022. Regulamenta a cirurgia robótica no Brasil*. Diário Oficial da União de 28/03/2022. https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2022/2311

Conselho Federal de Medicina (CFM). (2022, 20 de abril). *Resolução CFM nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação*. Diário Oficial da União de 05/05/2022. https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852

Cunha, F. J. A. P., Matos, J. R. F., Jr., Amaral, L. A. F. de O. do & Meirelles, R. F. (2022) A interlocução da qualificação profissional e dos mecanismos de transferência de informação para a gestão dos repositórios digitais em saúde. *Informação em Pauta, 7*. http://periodicos.ufc.br/informacaoempauta/article/view/78596/227458

Deodato, S. (2017). A proteção da informação de saúde. *Forum de Proteção de Dados*, (4), 60-69. https://ciencia.ucp.pt/pt/publications/a-prote%C3%A7%C3%A3o-da-informa%C3%A7%C3%A3o-de-sa%C3%BAde

Devaraj, S. J. (2019) Emerging Paradigms in Transform-Based Medical Image Compression for Telemedicine Environment. In H. D. Jude y V. E. Balas (eds.), *Telemedicine Technologies: Big data, deep learning, robotics, mobile and remote applications for global healthcare* (pp. 15-30). Elsevier.

Fischer, S. H. & Zhou, L. (2021). Uso de tecnologias da informação e da comunicação na área da saúde: a telessaúde em 2021. In Núcleo de Informação e Coordenação do Ponto BR, *TIC Saúde 2021. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros* (pp. 109-125). Comitê Gestor da Internet no Brasil. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2021/

Freire, M. P., Silva, L. G., Meira, A. L. P. & Louvison, M. C. P. (2023). Telemedicina no acesso à saúde durante a pandemia de covid-19: uma revisão de escopo. *Rev Saúde Pública, 57*(Supl 1). https://doi.org/10.11606/s1518-8787.2023057004748

Gadenz, S. D., Sperling, S., Leão, B. F. & Kersanach, M. (2021). Estratégia digital como organizadora do acesso equitativo aos serviços de saúde. In Núcleo de Informação e Coordenação do Ponto BR, *TIC Saúde 2021. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros* (pp. 155-165). Comitê Gestor da Internet no Brasil.

Hart, H. L. A. (2008). *Punishment and Responsibility: Essays in the Philosophy of Law* (2. ed.). Oxford Academic.

Herrmann, D. & Pridöhl, H. (2020). Basic Concepts and Models of Cybersecurity. In Christen, M., Gordijn, B. & Loit, M. (eds.), *The Ethics of Cybersecurity* (pp. 11-44). Springer.

Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A. & Abduallah, W. M. (2019). Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. *IEEE Access, 7*, 51691-51713. https://doi.org/10.1109/ACCESS.2019.2908998

Lecaros-Urzúa, J. A. & López-Gaete, G. E. (2023). Responsabilidad civil médica en telemedicina: una propuesta de principios para una lex artis telemédica. *Revista de Bioética y Derecho*, (57), 33-51. https://doi.org/10.1344/rbd2023.57.41222

Lorenzini, G., Shaw, D. M. & Elger, B. S. (2022). It takes a pirate to know one: ethical hackers for healthcare cybersecurity. *BMC Med Ethics, 23*. https://doi.org/10.1186/s12910-022-00872-y

Mantese, C. E., Aquino, E. R. D. S., Figueira, M. D., Rodrigues, L., Basso, J. & Raupp DA Rosa, P. (2021). Telemedicine as support for primary care referrals to neurologists: decision-making between different specialists when guiding the case over the phone. *Arquivos de neuro-psiquiatria, 79*(4), 299-304. https://doi.org/10.1590/0004-282x-anp-2020-0137

Meirelles, R. F. & Cunha, F. J. A. P. (2020). Autenticidade e preservação de Registros Eletrônicos em Saúde: proposta de modelagem da cadeia de custódia das informações orgânicas do Sistema Único de Saúde. *Revista Eletrônica De Comunicação, Informação & Inovação Em Saúde, 14*(3). https://doi.org/10.29397/reciis.v14i3.2117

Mendes, L. S. M. & Bioni, B. R. (2019). O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: Mapeando convergências na direção de um nível de equivalência. *Revista de Direito do Consumidor, 28*(124), 157-180.

Minghelli, M., Garcia, B. B., Vale, M. A. do & Santos, P. S. (2024). Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. *Em Questão*, 30, e–138249. https://doi.org/10.1590/1808-5245.30.138249

Ministério da Saúde. (2022). *Relatório de Gestão 2022*. Governo Federal Brasil. https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_gestao_2022.pdf

Morales, A. S., Ourique, F. D. O. & Cazella, S. C. (2021). A Comprehensive Review on the Challenges for Intelligent Systems Related with Internet of Things for Medical Decision. In G. Marques, A. Khumar Boi, I. De la Torre Díez & B. García-Zapirain (eds.), *Enhanced Telemedicine and e-Health. Studies in Fuzziness and Soft Computing, vol 410* (pp. 221-240). Springer. https://doi.org/10.1007/978-3-030-70111-6_11

Navarro, E. M., Álvarez, A. N. R. & Anguiano, F. I. S. (2022). A new telesurgery generation supported by 5G technology: benefits and future trends. *Procedia Computer Science*, 200, 31-38. https://www.sciencedirect.com/science/article/pii/S1877050922002113

Núcleo de Informação e Coordenação do Ponto BR. (2024). TIC *Saúde 2023. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros*. Comitê Gestor da Internet no Brasil. https://cetic.br/media/docs/publicacoes/2/20241104103447/tic_saude_2023_livroeletronico.pdf

Organização Mundial da Saúde (OMS). (2020a). *Coronavirus disease* 2019 (*COVID-19*) *Situation Report – 51: Data as reported by national authorities by 10 AM CET 11 March 2020*. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200311-sitrep-51-covid-19.pdf?sfvrsn=1ba62e57_10

Organização Mundial da Saúde (OMS). (2021a). *WHO-convened Global study of Origins of* SARS-*CoV-2: China part. Joint WHO-China study, 14 January – 10 February* 2021, *Joint Report*. https://www.who.int/publications/i/item/who-convened-global-study-of-origins-of-sars-cov-2-china-part

Organização Mundial da Saúde (OMS). (2021b). *Global strategy on digital health 2020-2025*. https://www.who.int/publications/i/item/9789240020924

Parlamento Europeu. (2016, 27 de abril). *Regulamento* (UE) *2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva* 95/46/CE (*Regulamento Geral sobre a Proteção de Dados*). Jornal Oficial da União Europeia L119. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Peine, A., Paffenholz, P., Martin, L., Dohmen, S., Marx, G. & Loosen, S. H. (2020). Telemedicine in Germany During the COVID-19 Pandemic: Multi-Professional National Survey. *Journal of medical Internet research*, *22*(8), e19745. https://doi.org/10.2196/19745

Petrazzuoli, F., Kurpas, D., Vinker, S., Sarkisova, V., Eleftheriou, A., Żakowicz, A., Aarendonk, D. & Ungan, M. (2021). COVID-19 pandemic and the great impulse to telemedicine: the basis of the WONCA Europe Statement on Telemedicine at the WHO Europe 70th Regional Meeting September 2020. *Primary health care research & development*, *22*, e80. https://doi.org/10.1017/S1463423621000633

Pinto, C. da S., Borsatto, A. Z., Vaz, D. C., Sampaio, S. G. dos S. M. & Oliveira, L. C. de. (2023). Telemedicina em Cuidados Paliativos Oncológicos: um Legado da Pandemia. *Revista Brasileira De Cancerologia*, *69*(1), e-142698. https://doi.org/10.32635/2176-9745.RBC.2023v69n1.2698

Presidência da República do Brasil. (1990, 19 de setembro). *Lei nº 8.080, de 19 de setembro de* 1990. *Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências*. Diário Oficial da União de 20/09/1990. https://www.planalto.gov.br/ccivil_03/leis/l8080.htm

Presidência da República do Brasil. (2018, 15 de agosto). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais* (*LGPD*). Diário Oficial da União de 15/08/2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Presidência da República do Brasil. (2022, 27 de dezembro). *Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de* 1990, *para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº* 13.146, *de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020*. Diário Oficial da União de 28/12/2022. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm

Reshmi, T.R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Samsung Newsroom Brasil. (2022, 14 de junho). *Galaxy Watch4 da Samsung será usado pelo InCor em pesquisa com pacientes cardiopatas*. https://news.samsung.com/br/samsung-e-incor-firmam-parceria-em-pesquisa-de-monitoramento-remoto-para-pacientes-cardiopatas

Sociedade Brasileira de Informática em Saúde. (2020). *Manual de Certificação de Sistemas de Registro Eletrônico em Saúde Versão* 5.0: *Instituído e regido pela Resolução CFM nº 1821/2007*. https://www.sbis.org.br/certificacao/Manual_Certificacao_S-RES_SBIS_v5-0.pdf

Wasserman, L. & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in digital health*, *4*, 1-20. https://doi.org/10.3389/fdgth.2022.862221

Weinstein, R. S., Krupinski, E. A. & Doarn, C. R. (2018). Clinical Examination Component of Telemedicine, Telehealth, mHealth, and Connected Health Medical Practices. *The Medical clinics of North America*, *102*(3), 533-544. https://doi.org/10.1016/j.mcna.2018.01.002

Wu, C. T., Lin, T. Y., Lin, C. J. & Hwang, D. K. (2023). The future application of artificial intelligence and telemedicine in the retina: A perspective. *Taiwan journal of ophthalmology*, *13*(2), 133-141. https://doi.org/10.4103/tjo.TJO-D-23-00028

Wu, Y. C., Chen, C. S. & Chan, Y. J. (2020). The outbreak of COVID-19: An overview. *Journal of the Chinese Medical Association*: JCMA, *83*(3), 217-220. https://doi.org/10.1097/JCMA.0000000000000270

Zanon, V., Romancini, E., Manoel, B., Lau, J., Ourique, F. & Morales, A. (2022). Avaliação experimental de uma camada de segurança implementada em dispositivo vestível cardíaco para Internet das Coisas Médicas. In *Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* (pp. 97-110). SBC. https://sol.sbc.org.br/index.php/sbseg/article/view/21661