ISSN 1808-6136

ISSN on-line 2674-7499

REPERCUSSÕES DA TELEMEDICINA NA REPARAÇÃO DE DANOS POR VIOLAÇÃO DE DADOS PESSOAIS

GABRIEL SCHULMAN[1], CAROLINE AMADORI CAVET[2]

[1] Doutor em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Mestre em Direito Civil pela Universidade Federal do Paraná (UFPR). Integra a Comissão de Saúde da OAB/PR. Advogado, é Sócio de TRAJANO NETO E PACIORNIK ADVOGADOS. Professor da Universidade Positivo na Graduação e Mestrado. E-mail: gabriel@schulman.com.br

[1] Pós-Graduada em Direito Público pela UNIBRASIL/Curitiba. Pós-graduanda em Direito Médico pela Universidade de Curitiba. Especialista em Direito de Medicina pela Universidade de Coimbra. Presidente da Comissão de Juizados Especiais da Ordem dos Advogados do Brasil Seção Paraná (OAB/PR). Integra a Comissão da Saúde e da Comissão de Inovação e Gestão, ambas da Ordem dos Advogados do Brasil Seção Paraná (OAB/PR), gestão 2019-2021. Advogada, é Sócia Fundadora da CAROLINE CAVET ADVOCACIA. E-mail: caroline@carolinecavet.adv.br

RESUMO

A intensificação da circulação de dados, consequência das inovações tecnológicas, desafia o sistema jurídico e colocam *sub judice* as respostas tradicionalmente oferecidas. No campo da saúde, destacam-se a utilização de novos sistemas que permitem, de diversas maneiras, a realização de atendimentos, exames e até procedimentos à longa distância. O presente artigo, em vistas dessa transformação, tem como objetivo problematizar os reflexos jurídicos da telemedicina na seara do direito de danos (responsabilidade civil), em especial, associados à proteção de dados pessoais do paciente; expor as modalidades de telemedicina; e explorar desafios e novas questões de direito de danos em relação a proteção de dados pessoais na medicina a distância.

Palavras-chave: Telemedicina; E-Health; Direito Médico; Responsabilidade Civil; Danos; Saúde.

REPERCUSSIONS OF TELEMEDICINE ON DAMAGE REPAIR FOR VIOLATION OF PERSONAL DATA

ABSTRACT

The intensification of the circulation of data, a consequence of technological innovations, challenges the legal system and undermines the responses traditionally offered. In the health field, we highlight the use of new systems that allow, in different ways, the performance of consultations, exams and even long distance procedures. This article, in view of this transformation, aims to discuss the legal consequences of telemedicine in the harvest of the right to damages (liability), in particular associated with the protection of personal data of the patient; expose telemedicine modalities; and to explore challenges and new issues of damage law in relation to the protection of personal data in distance medicine.

Keywords: Telemedicine; E-Health; Medical Law; Civil responsability; Damage; Health.

Recebido em 26/01/2021 e aprovado para publicação em 17/05/2021

1 INTRODUÇÃO

O sistema de saúde, tradicionalmente, mostra-se permeado de ineficiências e desperdícios, em parte, pela complexidade da sua engenharia funcional, que dificulta a integração de cuidados necessários e gera níveis elevados de insatisfação de seus usuários, inclusive pelas enormes listas de espera para consulta, exames e cirurgias (RIBEIRO, 2019). O desafio para gerir este sistema é gigante, em especial pelas múltiplas dimensões para o atendimento à saúde do indivíduo de forma integral, isto é: física, psíquica e social. Uma tarefa essencial; porém, enorme e cara (SCHAEFER, 2019).

De encontro às dificuldades, a era digital, impulsionada pela quarta revolução industrial e os seus avanços tecnológicos, inspira novas abordagens na área da saúde (SCHWAB, 2016) como promessa de solução às dificuldades do sistema de saúde. Potenciais inovações evidenciadas pelo surgimento da Telemática da Saúde, associação do termo telecomunicação e informática, possibilitam o serviço de saúde à distância com a finalidade de promover a saúde, monitorar as doenças e o acompanhamento de suas evoluções, a instrução ao paciente ou à comunidade, a estruturação e a integração de dados de pacientes e sua evolução clínica, entre outras possibilidades.

Diante deste cenário, ainda que entre incertezas normativas, o investimento em tecnologias aplicadas ao setor de saúde teve um aumento significativo entre 2014 e 2019. Durante este período o número de *startups* de base tecnológica voltadas ao setor da saúde passou de 160 para 389 (NERY, 2019), o que representa crescimento de 141% (cento e quarenta e um por cento) de *health techs* no Brasil. E a Covid-19 e consequente distanciamento social, houve o alargamento da adoção da Telemedicina que, atualmente, é presente em 75% (setenta e cinco por cento) de Hospitais Particulares (ANAHP, 2020).

Assim, a prestação de saúde à distância populariza-se como uma alternativa para a redução de custos, sem perder de vista, a maior eficiência no atendimento ao paciente, de forma personalizada e humana (RIBEIRO, 2019). Contudo, seu emprego merece cuidados especiais, a começar pelos deveres de sigilo da informação e a garantia de privacidade do paciente. Isso porque o emprego da Telemedicina amplia a circulação, a conexão e a coordenação de dados de pacientes, potencializando os riscos de que os dados, estruturados, sejam vazados (RIBEIRO, 2019; LOES, 2017).

Para atingir os objetivos propostos, a pesquisa visa, incialmente, examinar o conceito de Telemedicina, com a identificação de alguns marcos legais relevantes, assim como, salientar-se a ausência de regulamentação suficiente. Na sequência, examinam-se as repercussões da Lei Geral de Proteção de Dados para o tema proposto, sobretudo os requisitos e os limites para tratamento dos dados sensíveis do Paciente. Para, finalmente, expor sobre as repercussões quanto à reparação de danos nos casos em que há violação da proteção desses dados pelo emprego da Telemedicina.

2 MODALIDADES, REGULAMENTAÇÃO E RISCOS NA TELEMEDICINA

A Telemedicina, conforme Organização Mundial da Saúde (OMS), é a oferta de serviços relacionados à saúde, por meio de recursos avançados de informática e telecomunicações,

> em que a distância é um fator crucial, com o intuito de promover o intercâmbio de informações válidas para diagnósticos, prevenção e tratamento de doenças e a contínua educação de prestadores de serviços em saúde, assim como para fins de pesquisas e avaliações (WORLD HEALTH ORGANIZATION, 2005, on-line).

Nota-se que a Telemedicina, por sua concepção, está intimamente relacionada à evolução da comunicação e, desse modo, não se trata de "invenção" do mundo moderno, mas a otimização causada pelo aprimoramento de antigas tecnologias (telegrafo, telefone, rádio, etc.) e pelo desenvolvimento de novas. Portanto, ao contrário do que se pode presumir, os primeiros relatos sobre o uso da "Telemedicina" remota ao século XIX, com o emprego de cartas e mensageiros para troca de informações entre médico e pacientes ou outros médicos, a fim de prestar orientações ou acompanhar a evolução de doenças.

Com a popularização dos microcomputadores, na década de 70, a expansão de projetos na Telemática da Saúde, seja para gestão (telessaúde) ou atendimento clínico (telemedicina), recebeu maior destaque e versatilidade (SCHAEFER, 2009). E, desde então, a Telemedicina, atrelada às inovações tecnológicas e à disseminação ao acesso à internet, desenvolve-se, exponencialmente, como um instrumento para assegurar o direito humano e fundamental à saúde.

2.1 Modalidades de Telemedicina na Declaração Tel Aviv

Consultas por telefone e videoconferência, orientações por plataformas, cirurgias à distância, a Telemedicina engloba diversas modalidades e suas aplicações variam em grau de complexidade, da adequação e da necessidade da instituição de saúde e das comunidades a que se destina.

As primeiras orientações e diretrizes sobre o emprego da Telemedicina advieram de debate suscitados na 51ª Assembleia Geral da Associação Médica Mundial, em *Tel Aviv*, em 1999, dando origem a "Declaração de *Tel Aviv*" que estabeleceu 05 (cinco) modalidades, a constar: a) teleassistência; b) televigilância; c) teleconsulta; c) interação entre dois médicos; e d) teleintervenção.

A **Teleassistência** permite que, mesmo a distância, seja avaliada a gravidade da situação clínica e sejam implementadas providências adequadas para atender o paciente. Em termos atuais, consiste no emprego de telefones ou detectores – inclusive robôs –, instalados no domicílio do paciente, o que permite uma comunicação direta a um centro de atendimento ou ao médico, no caso de uma emergência (Declaração de Tel Aviv, 1999).

A **Televigilância,** também designada de telemonitoramento, permite o monitoramento do paciente à distância e em tempo real, o que possibilita a adaptação medicamentosa e avaliação assertividade do tratamento receitado. Essa modalidade, ordinariamente é associada a aplicativos em *smartphone*s ou *smartwatches* que transmitem os dados sobre a condição do paciente (pressão arterial, eletrocardiogramas *etc*.) (DECLARAÇÃO DE TEL AVIV, 1999).

A **Teleconsulta,** como a própria designação aponta, consiste numa consulta não presencial. O atendimento médico ocorre por meio de plataforma ou outros mecanismos de telecomunicação (LEÃO, 2018), sem que haja exame clínico ou contato direto entre o médico e o paciente, tampouco a presença de um médico assistente supervisionando o ato (SCHAEFER, 2009).

Já a **interação entre dois médicos,** caracteriza-se pelo atendimento ao paciente por meio de um médico presente com auxílio remoto de outro médico especialista na área. A interação, como no caso da Teleconsulta, pode ocorrer por qualquer forma de telecomunicação (DECLARAÇÃO DE TEL AVIV, 1999).

Finalmente, a **Teleintervenção,** modalidade extraída das disposições gerais da Declaração de *Tel'Aviv*, consiste na intervenção à distância em exames médicos ou procedimentos cirúrgicos, em que o médico, com auxílio de médico assistente ou de robôs, executa ações de natureza cirúrgica (Telecirurgia) ou de diagnóstico (DECLARAÇÃO DE TEL AVIV, 1999).

Reforça-se que as referidas modalidades estão previstas na Declaração de *Tel Aviv* de acordo com a forma que são empregadas, entretanto, por ausência de conceito uniforme, há variação entre nomenclaturas de acordo com a região ou instituição de saúde que a implementa.

2.2 Marcos Legais da Telemedicina

O atendimento médico convencional é dado na forma presencial; entretanto, os avanços tecnológicos permitem, por meio da Telemedicina, o encontro entre paciente e médico de forma virtual e indireta, o que repercute em implicações ético-jurídicas. Isso porque, em uma leitura apressada, o Código de Ética Médica (CONSELHO FEDERAL DE MEDICINA, 2018), sugere entraves éticos para o emprego da Telemedicina, tais como vedação ao médico à prescrição de tratamento ou procedimentos sem exame direto ao paciente, o compartilhamento de fatos e casos clínicos, a transmissão, o manuseio e a guarda de prontuários e a utilização de comunicação de massa.

Apesar disso, o mesmo diploma, além de impor a adoção de todos os meios disponíveis ao diagnóstico e ao tratamento, cientificamente reconhecidos e ao alcance, em favor do paciente, expressamente autoriza o atendimento não presencial em caso de urgência e emergência e estabelece que o atendimento médico à distância, nos moldes da Telemedicina ou de outro método, será regulado pelo referido Conselho (CONSELHO FEDERAL DE MEDICINA 2018).

Nesse sentido, evidencia-se que não há proibição ao emprego da Telemedicina no Brasil, sendo o seu emprego para atendimento e tratamento médico inclusive recomendado para o acesso à saúde, nos artigos 6º, 196 e 200 da Constituição Federal, afora inúmeros tratados que versam sobre direitos humanos, como determinam a Declaração Universal dos Direitos Humanos art. 2º (ONU, 1948) e o Pacto Internacional de Direitos Econômicos, Sociais e Culturais. Universal dos Direitos Humanos (ONU, 1966).

Com o intuito de regulamentar a Telemedicina no Brasil, o Conselho Federal de Medicina editou a Resolução nº 1.643/2002 que, em seu art. 2º, a define como "o exercício da Medicina através da utilização de metodologias interativas de comunicação áudio-visual (*sic*) e de dados, com o objetivo de assistência, educação e pesquisa em Saúde" (CFM, 2002), impondo ao prestador de serviço de Telemedicina, seja pessoa física ou jurídica, a inscrição no referido Conselho.

Nota-se que referida Resolução, por sua brevidade, não atende à finalidade que se propõe com omissões significativas, tais como as modalidades admitidas, o modo de emprego, dentre outras questões que acarretam a imprecisão e a insegurança para sua ampla adoção por clínicas, hospitais e médicos (GARCIA, 2020). Para além disso, os avanços significativos dos meios tecnológicos de quase 20 anos de sua vigência permitem a transmissão de dados, em especial som e imagem, com qualidade inimaginada ao tempo da sua edição, o que revela a defasagem normativa.

Para suprir essa lacuna, o Conselho Federal de Medicina, editou a Resolução nº. 2.227/2018 que disciplinava o emprego da Telemedicina, de forma mais abrangente, com especificação de modalidades, modo de emprego, forma de armazenamento de dados, além de deveres e obrigações aos seus prestadores. Entretanto, pelo clamor da comunidade médica (CONSELHO FEDERAL DE MEDICINA, 2019), com o intuito de promover maiores debates sobre a temática, a referida Resolução foi revogada pela Resolução nº. 2.228/2019, a qual repristinou a Resolução nº. 1.643/2002.

A insuficiência da norma vigente, gera a necessidade de regulamentação da matéria por meio de diversas normas esparsas. A exemplo, a Resolução nº. 2.107/2014, do Conselho Federal de Medicina, regulamenta a Telerradiologia pelo emprego de "tecnologias de informação e de comunicação para o envio de dados e imagens radiológicas com o propósito de emissão de relatório, como suporte às atividades desenvolvidas localmente" (CONSELHO FEDERAL DE MEDICINA, 2014). No mesmo sentido, a Teleopatologia, disciplinada pela Resolução nº. 2.264/2019 (CONSELHO FEDERAL DE MEDICINA, 2019). Nota-se que essas resoluções versam sobre especialidades da medicina aplicadas de forma remota e não da modalidade propriamente dita que, em ambos os casos, corresponderiam a Teleintervenção.

A Teleconsulta é a modalidade com maior resistência no Brasil. Para alguns autores (FALEIROS JUNIOR, 2020), haveria a sugestão de proibição a consultas médicas à distância por força da Resolução nº 1.974/2011 do Conselho Federal de Medicina, o que, atualmente, não prevalece por força da Lei nº 13.989/2020.

Quanto à comunicação com o paciente, fora do ambiente de consultas, o parecer nº 14/2017 do Conselho Federal de Medicina permite a interação por via do WhatsApp e outras plataformas similares, embora pareça haver mecanismos mais seguros e específicos. O parecer preconiza: "É permitido o uso do WhatsApp e plataformas similares para comunicação entre médicos e seus pacientes, bem como entre médicos e médicos, em

caráter privativo, para enviar dados ou tirar dúvidas, bem como em grupos fechados de especialistas ou do corpo clínico de uma instituição". (CFM, 2017).

Por fim, o prontuário médico teve sua guarda digital regulamentada pela Resolução nº. 1.639/2002 do Conselho Federal de Medicina, com a aprovação de "Normas Técnicas para Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico". Esta, por sua vez, foi revogada pela Resolução nº 1.821/2007, do Conselho Federal de Medicina, que passou a disciplinar a digitalização e uso dos sistemas informatizados, e agora impondo às empresas prestadoras do serviço de telemedicina que possuam meios tecnológicos seguros para armazenamento *on-line* de informações dos seus pacientes (BRASIL, 2007).

Dessa maneira, no Brasil, ainda que haja lacunas legislativas pertinentes em relação à disciplina, é permitida a Telemedicina, a qual deve ser empregue "como meios complementares e não substitutos da Medicina tradicional*" (*SCHAEFER, 2019), atrelada, naturalmente, as boas práticas de proteção de dados.

2.3 Riscos na Telemedicina: violação da privacidade dos dados clínicos

A análise das diferentes modalidades de Telemedicina permite constatar sua pluralidade. Por ser empregada pelos mais diversos canais, inclusive pelo simples envio de e-mail pelo paciente, por plataformas digitais em sites ou até WhatsApp, seu tráfego de dados em redes digitais e seu armazenamento em servidores externos ou nuvem, requer a atenção para a forma como são recebidos, processados, para assegurar sua integridade, segurança e confidencialidade.

Se por um lado os meios tecnológicos devem ser considerados para promoção da saúde, de outro, é preciso levar em conta os riscos e impactos ocasionados pela digitalização do corpo (CORREA, 2010), com a estruturação de dados, genéticos e de saúde (COLOMBO, FACCHINI NETO, 2019) que são disponibilizados em rede digital. Esse novo aspecto da pessoa natural, atribui, além de massa física, a uma dimensão virtual com novas particularidades que exteriorizam a personalidade que é representada pelos dados (COLOMBO, FACCHINI NETO, 2019). Ao lado da contribuição das novas tecnologias para os cuidados, há um consolidado mercado – lícito e ilícito – de dados de dados. Ademias, o cruzamento de dados obtidos em documentos médicos pode permitir abertura de contas bancárias, podendo resultar em fraudes bilionárias (COVENTRY, BRANLEY, 2018).

Em tal contexto, os dados dos pacientes convertem-se então em potencial mercadoria de grande valor (PARKINS , 2017) e podem ser dissociados do sujeito a quem pertencem, independente dos seus fins (DONEDA, 2019). Essa conversão, movida pela nova economia (LOVERLUCK, 2018) (*data-driven economy*) (CAVANILLAS, CURRY, WAHLSTER, 2016), é ampliada pelo intenso aumento de fluxo de dados, pelas novas possibilidades criadas pelo uso de *big data* e algoritmos. Essas ferramentas permitem reunir dados, analisar, identificar perfis comportamentais (COLOMBO, FACCHINI NETO, 2019), tendências, otimização resultados (DESCH, FALEIROS JUNIOR, 2019) e, sobretudo, lucro.

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.

As preocupações, contudo, não se limitam a utilização dos dados fora das finalidades adequadas. Não é possível esquecer que a insegurança dos sistemas é recorrente, o que pode ensejar acessos indevidos, perda ou mesmo vazamentos de dados. Na Inglaterra, noticiou-se o acesso de dados de pacientes por auditores governamentais do Departamento de Saúde e Serviços Humanos da Inglaterra, por *laptops*, enquanto estavam sentados em estacionamentos de hospitais (TAITSMAN, GRIMM, AGRAWAL, 2013), pelo uso de redes de *wifi* não seguras (TAITSMAN, GRIMM, AGRAWAL, 2013). Já nos Estados Unidos, foram roubados 78.8 milhões de registros de pacientes (O'FLAHERTY, 2018), com dados como nome, endereço, número do seguro social e data de nascimento. Na Alemanha, um hospital teve os dados sequestrados, causando a morte de um paciente (BBC, 2000)

Falha-se ainda no eixo informativo da Telemedicina. Muitos pacientes, hesitantes em fornecer seus dados, terminam por adotar uma postura de retenção de dados, ou até prover o profissional com falsos dados (HALL, MCGRAW, 2014). Para além disso, a velocidade da abertura de sites com "orientações sobre saúde", o advento do "Dr. Google" como se costuma designar, não se fez acompanhar da necessária qualidade da informação. E como destacou o editorial da *Medicine, Health Care and Philosophy*, intitulado "*Cybermedicine and e-ethics" (*HAVE, 2001), há a necessidade de um repensar crítico da proteção do paciente, diante da oferta de informações, produtos e serviços à distância.

Pelo todo exposto, os dados clínicos, que antes detinham apenas o caráter clínico com sua relevância restrita ao tratamento do paciente ou para embasar pesquisas científicas

(ensaios clínicos), ganham atenção mercadológica, fazendo crescer a preocupação para além da sua proteção, ao controle de acesso e de seu conteúdo.

Desse modo, a Telemedicina abre diversas possibilidades de reflexões e desafios, tornando-se um campo fértil de estudo sobre a forma de assegurar o resguardo dos direitos do paciente, com enfoque à informação integral e segura (privacidade de dados, qualidade de informação e confiabilidade), sob pena da imposição de dever de reparar àquele que violar a proteção de dados.

3 PRIVACIDADE E PROTEÇÃO DE DADOS DO PACIENTE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

O discurso sobre a privacidade está associado a questões relacionadas a dados pessoais e, portanto, à informação relacionada ao indivíduo (DONEDA, 2019). Nessa toada, a Lei Geral de Proteção de Dados Pessoais, define *dados pessoais* como a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Com mais vigor, a lei trata o dado sensível. Sem pré-estabelecer um critério para o enquadramento, o art. 5º, inc. II, conceitua como:

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à **saúde** ou à vida sexual, **dado genético ou biométrico**, quando vinculado a uma pessoa natural.

Nota-se que o instrumento legislativo adota um conceito aberto com o propósito de constituir uma noção ampla quanto aos dados pessoais, sensíveis ou não, para incluir toda a informação que se associa ou pode ser associada a uma pessoa identificável (COLOMBO, FACCHINI NETO, 2019). Tal concepção ampla é relevante porque *"dados aparentemente 'inocentes'*", a depender do modo como são tratados, podem revelar informações sensíveis de determinada pessoa (COLOMBO, FACCHINI NETO, 2019).

Repete-se que os dados pessoais sensíveis pertinentes à atenção à saúde por meio da Telemedicina, estão subordinados às hipóteses de tratamento do art. 11 da Lei Geral de Proteção de Dados Pessoais e a maior atenção nos cuidados em vista do maior impacto que os incidentes de segurança podem provocar.

3.1 Transformações na Proteção dos Dados Pessoais no Ordenamento Jurídico Brasileiro

Está em curso, no Brasil e internacionalmente, uma mudança profunda na compreensão sobre a proteção de dados pessoais (RODOTÀ, 2008). Paradoxalmente, vive-se um momento de hiperexposição e preocupação redobrada com a privacidade (BARNES, 2006). Como aponta a doutrina, a privacidade percorreu um interessante percurso (CÓDIGO DE ÉTICA MÉDICA, 2009), desde a noção do direito de estar só (WARREN, BRANDEIS, 1890), passando pela intimidade, até à concepção contemporânea, lastreada na autodeterminação, ou seja, no controle do fluxo dos dados pessoais (RODOTÀ, 1977).

Conjura-se, desse modo, a tutela da privacidade e da proteção dos dados pessoais (EUROPEAN DATA PROTECTION SUPERVISOR, 2001). À luz do conceito contemporâneo, além do tradicional sigilo médico, ao paciente é assegurada a autodeterminação informativa. No campo da saúde, significa, confidencialidade, acesso adequado a informação, controle dos dados, segurança, entre outros aspectos. A proteção se estende pelo fluxo dos dados (*data cycle)*, que – em regra – pressupõe o consentimento para o seu tratamento, ao acesso aos dados, a transparência em relação às hipóteses de compartilhamento, a sua retificação *etc*. (MULHOLLAND, 2018).

Tal acervo de direitos reforça a posição do paciente como o titular de dados, cuja conexão não deixa de existir com este, mesmo que ocorra sua revelação para finalidade de seu tratamento. Isso, porque os dados pessoais integram a privacidade que, por sua vez, está vinculada à personalidade do indivíduo e ao seu desenvolvimento (DONEDA, 2019).

A tecnologia criou inúmeras novas soluções, todavia, brindou-nos com enormes desafios no campo da privacidade. No direito brasileiro, a proteção de dados pessoais compõe-se em uma sólida rede de normas, que inclui naturalmente a Lei Geral de Proteção de Dados Pessoais, assim como a Constituição Federal, Código Civil, Marco Civil da Internet, Lei do Cadastro Positivo, Código de Defesa do Consumidor. A proteção da pessoa é reforçada pelo caráter constitucional da matéria, inclusive pelo reconhecimento da proteção de dados pessoais como um direito fundamental (RODOTÀ, 2009).

Ainda sobre a legislação, no campo da saúde, deve-se levar em conta a existência de legislação específica (ainda que insuficiente), com ênfase para a Lei Orgânica da Saúde (Lei n. 8.080/90), a Lei de Saúde Mental (Lei n. 10.216/2001). Entre outras normas que, de maneira direta ou indireta, também reforçam os deveres da proteção de dados na saúde. Deve-se registrar, porém, que há diversas lacunas relevantes, como a falta especificidade, e um

campo que demanda soluções peculiares e apresenta riscos enormes aos direitos fundamentais.

A Telemedicina, com suas peculiaridades, não escapa do desafio imposto pela bioética de equilibrar novas vantagens, com a indispensável proteção da pessoa (BARBOZA, BARRETO, MEIRELLES, 2002). Torna-se necessário que a saúde prestada na esfera virtual esteja atrelada a uma ética concreta (SCHRAMM, ESCOSTEGUY, 2000).

O emprego da Telemedicina, como previamente mencionado, relaciona-se diretamente com os sistemas que coletam, armazenam, processam, recuperam e/ou comunicam dados sobre os pacientes identificáveis ou identificados (SCHAEFER, 2019) assim, nos termos do artigo 5º, inciso X da Lei Geral de Proteção de Dados, possibilita o tratamento de dados (COLOMBO, FACCHINI NETO, 2019*)* que, por sua vez, acarreta na digitalização do corpo humano. A silhueta do indivíduo, que até então era um vulto, passa a ter contornos nítidos, com riqueza de detalhes dados (COLOMBO, FACCHINI NETO, *2019)* o que produz, consequentemente, questionamentos quanto à valorização econômica das informações extraídas dessas bases (SCHAEFER, 2019).

O uso da Telemedicina e, por conseguinte, o aumento de fluxo de dados pessoais sensíveis, exige a "fixação de normas relativas à transmissão dos dados, normas técnicas de trabalho e capacitação profissional, além de normas de vigilância e controle dos sistemas dentro, é claro, dos limites jurídicos fixados"(SCHAEFER, 2019, p.133). Isso porque, apesar de ensejar diversos benefícios, pode "significar sérios riscos aos pacientes se alguns cuidados, fiscalizações e avaliações periódicas de sua qualidade, segurança, eficiência e, especialmente confidencialidade, não forem tomadas" (SCHAEFER, 2019, p.134). Nesse cenário, o grande desafio é manter "todos os avanços da digitalização da saúde sem comprometer o seu lado ético e humano, reforçando os códigos de conduta para proteger a informação clínica e os dados pessoais" (RIBEIRO, 2019, p.27) e garantir a tutela da privacidade do paciente (DONEDA, 2019).

Como exposto, há riqueza de normas protetivas da privacidade e confidencialidade aplicáveis na atenção à saúde e, para além disso, não há como se ignorar que os dados pessoais de saúde e genéticos, indubitavelmente, têm utilidades que ultrapassam a esfera privada, com contornos de interesse público para promoção de políticas públicas e serviços públicos.

3.2 Autorização legal para o Tratamento de Dados Pessoais do Paciente

No caso da saúde, entre as autorizações legais para tratar dados sensíveis, merecem destaque o "consentimento do titular" (Artigo 11, inciso I) "para a proteção da vida ou da incolumidade física do titular ou de terceiros" (Artigo 11, inciso VII), "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (Artigo 11, inciso VII). (BRASIL, 2018).

Esses são aspectos centrais da adequação à Lei Geral de Proteção de Dados Pessoais, tanto o consentimento do titular e a adequada informação, quanto o dever de transparência (Artigo 6º. inciso VI) demanda clareza no compartilhamento e uso das informações. Para verificação da conduta esperada, propõe Zhou (2019), o dever de observar se o consentimento do paciente inclui a privacidade restrita a sistemas de Telemedicina, havendo, ou não, autorização para o uso de fotografia, filmagem ou outras formas de gravação, sistemática de transferência de dados para terceiros.

Isso dito, deve-se observar que o consentimento deve ser adequado para também discorrer sobre as questões atinentes à autodeterminação informativa do paciente. Em especial, no campo da Telemedicina, em que o risco de exposições é considerado mais profundo (HALE, KVEDAR , 2014), até porque dados de saúde são considerados como um alvo potencial de crimes virtuais (COVENTRY,BRANLEY, 2018).

Na Lei Geral de Proteção de Dados, o consentimento não é requisito essencial para tratamento de dados do paciente. Há outras hipóteses legais como o dever legal que autorizam o tratamento de dados em saúde. É preciso também ressaltar que o consentimento, quanto presente, precisa ser específico – não se admite a mera autorização genérica para as mais diversas possibilidades de uso atual e futuro dos dados. Nesse sentido, deve-se ter em conta "exceções para a utilização destes dados sem o consentimento do titular, mas estas devem ser interpretadas restritivamente, também em respeito aos demais princípios da legislação, especialmente" (SCHAEFER, GONDIM, 2020).

Igualmente, o consentimento está sempre atrelado a alguma finalidade (BRASIL, 2018), a questão a ser levantada neste ponto, em eventual discussão de reparação de danos, não reside em identificar a presença ou ausência do consentimento, mas antes sua validade, seu sentido e seu alcance.

A saúde recebe tratamento diferenciado na Lei Geral de Proteção de Dados. Para além da restrição das bases legais de tratamento, há restrição de finalidade, de maneira

enfática, a teor do disposto pelo artigo 11, § 4º, conforme a redação dada pela Lei nº 13.853/2019

> É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde (...)

Em complemento, dispõe artigo 11, §5º,

> É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários

Apesar de avançar no tema, a Lei Geral de Proteção de Dados não deixa claros os limites do tratamento de dados pessoais na saúde. Uma leitura literal da Lei Geral de Proteção de Dados Pessoais, a teor dos artigos 1º e 12, ainda sugere que, diante da anonimização de dados, não haveria incidência da lei. Essa interpretação, todavia, não esgota a matéria, em especial diante do caráter constitucional da proteção de dados pessoais e os riscos envolvidos nos dados em saúde, como denota a própria recomendação da lei para que ensaios clínicos empreguem anonimização ou ainda estabelece a eliminação dos dados de pesquisas com seres humanos.

Evidencia-se, dessa maneira, lacunas importantes na disciplina da matéria, uma vez que a transparência e o direito à informação como princípios expressamente adotados pela Lei Geral de Proteção de Dados Pessoais, confrontam com a previsão de não incidência da norma quando há anonimização.

A Lei Geral de Proteção de Dados Pessoais também alcança as entidades públicas, inclusive da Administração Pública Indireta (empresas públicas e as sociedades de economia mista). Novamente, sem maior detalhamento e com uma omissão relevante para a saúde, a lei estabelece que o "uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal". (BRASIL, 2018).

A abertura legislativa é interessante ao conferir maior possibilidade de adequação ao caso concreto. Entretanto, o legislador poderia oferecer parâmetros além dos princípios que elencados no artigo 6º, em especial porque, em matéria de saúde, os interesses individual e coletiva, muitas vezes, são postos em conflito. É o caso da preservação de dados pessoais úteis à pesquisa, todavia, em relação a quais o paciente, titular de dados, deseja que haja eliminação completa. (PARLAMENTO EUROPEU E CONSELHO, 2016)

4 A REPARAÇÃO DE DANOS AO PACIENTE NA TELEMEDICINA: NOVAS QUESTÕES PARA VELHOS DESAFIOS DO DIREITO DE DANOS

A Telemedicina, como já exposto, representa uma enorme contribuição à saúde. As novas tecnologias permitem soluções inimagináveis e potencializam o seu acesso. No entanto, devem ser levados em conta também os impactos negativos, em especial porque os sistemas digitais oferecem velocidade e grande difusão não apenas de seus aspectos positivos, como de seus "efeitos colaterais", inclusive no plano da proteção dos dados pessoais. Em relação à telemedicina, destaca-se que o uso de transmissão de dados sensíveis em tempo real ultrapassa fronteiras e se perpetua no tempo pela possível reprodução da informação entre os diferentes elos da cadeia informativa (COLOMBO, FACCHINI NETO, 2019).

Os jornais ao redor do mundo já anunciam diversos casos de violação de dados que envolvem a Telemedicina. A exemplo, na Suécia, noticiou-se que 2.7 milhões de conversas feitas ao serviço nacional de atenção à saúde, por telefone, foram localizadas em um servidor não protegido, totalizando 170.000 horas, com exposição de sintomas, doenças e outros dados pessoais (BBC, 2019). Já no México, a falha na configuração de um servidor conduziu ao vazamento de dados banco de dados com 2.373.764 atendimentos por telemedicina pela empresa *Hova Health*. Esse banco de dados continha nomes de pacientes, códigos de identificação dos cidadãos, números da apólice de seguro e respectivas datas de validade, datas de nascimento e endereços. Igualmente, ainda constavam observações sobre o *status* migratório e deficiências (DAVIS, 2018).

Enquanto no Canadá, hackers, ou melhor, crackers para maior precisão técnica, sequestraram os dados de pacientes depois de romper o primeiro nível de segurança da província canadense de Saskatchewan. De acordo com o site canadense, a eHealth Saskatchewan coordena e implementa chaves eletrônicas para acesso de informações em sistemas públicos de saúde, inclusive o sistema de prontuários eletrônicos - Electronic Health Record (EHR) (CANADA, 2019). A notícia informa que a empresa sofre 100.000 tentativas de invasão diárias.

Para compreensão sobre a dimensão da segurança de dados, um relatório da empresa *Insight* revela que um terço dos dados de pacientes estão vulneráveis. Em seu levantamento, foram verificados 50 (cinquenta) bancos de dados, dos quais 15 (quinze) foram considerados

como vulneráveis, assim permitindo acesso a 1,5 milhão de registros de pacientes (DAVIS, 2018).

Portanto, a violação dos dados do paciente pode ocorrer de diversas maneiras e em diferentes etapas da atenção à saúde. Sem pretensão de exaurir as hipóteses, além dos exemplos expostos, merece grande atenção a falta de transparência no uso de algoritmos aplicado, na construção de perfis. O uso de algoritmos de difícil acesso e compreensão pelos usuários torna obscuros e pode gerar danos pelo uso de dados imprecisos, tais como erros estatísticos, dados equivocados ou inverídicos e correlações inadequadas (COLOMBO, FACCHINI NETO, 2019).

No que tange à autorização paciente, entre as formas de violação de dados, está a revelação indevida de dados clínicos a terceiros, tais como resultados de exames, suspeitas de determinados quadros, assim como o tratamento desses dados sem o consentimento do paciente. É preciso também atentar para a hipótese de compartilhamento de dados do paciente com a finalidade distinta ao propósito do consentimento outorgado pelo paciente.

Merecem atenção também o tratamento de forma inadequada, como a situação em que há circulação de dados com baixo nível de segurança, sem uso de criptografia, com falhas na organização de níveis de acesso, ou, ainda, a falta de mecanismos de controle para a gestão de dados por colaboradores e/ou outros, quando o consentimento para seu uso for revogado pelo paciente.

Não há dúvidas que o lançamento de informações pessoais no sistema da Telemedicina, desacompanhado de um filtro ético, pode colocar a pessoa em situações extremamente vexatórias e insalubres. Assim, trazendo à luz "novos contornos e novas peculiaridades que não permitem ao direito se desprender da aferição específica daquilo que lhe permite ressignificar institutos como a responsabilidade civil" (DRESCH, FALEIROS JUNIOR, 2019)

4.1 Singularidades da proteção de dados pessoais no tocante a pacientes

Como destaca Bodin de Moraes (2019), o legislador estabeleceu um regime especialíssimo de responsabilidade civil na Lei Geral de Proteção de Dados. Ao invés de simplesmente estabelecer a possibilidade da reparação, de forma inovadora, procurou-se, ainda que, com certo grau de generalidade, estabelecer critérios para as boas práticas na proteção de dados pessoais. Tais elementos se mostram como critérios úteis para aferir

hipóteses de atribuição ou exclusão do dever de reparar, aplicando-se, subsidiariamente, pelo Código Civil e Código de Defesa do Consumidor (BODIN DE MORAES , 2019).

Consoante a própria Lei Geral de Proteção de Dados define, em seu artigo 42, quem "causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Sublinha-se o caráter solidário da responsabilidade civil entre os diferentes agentes envolvidos e a necessidade de uma compreensão larga da noção de vítima, afinal, além do titular de dados, os prejudicados podem ser seus familiares, ou até pessoas jurídicas que cuidam dos dados (BODIN DE MORAES, 2019).

Há controvérsia sobre a natureza da responsabilidade civil, dado que, em certos momentos, o legislador pareceu assinalar a culpa como critério para reparação. Balizada doutrina defendeu a responsabilidade subjetiva na Lei Geral de Proteção de Dados. Contudo, o tema parece merecer, ainda, reflexão mais cautelosa. Primeiro, porque a possibilidade de previsão de culpa para determinadas situações precisa ser equilibrada com outros diplomas, em especial, com o Código de Defesa do Consumidor e a cláusula geral de responsabilidade civil objetiva, fundada no risco, prevista no artigo 927, do Código Civil. Segundo, porque os cuidados tomados pelo ofensor poderão ser levados em conta na imposição de penalidades, em consonância com a incidência da regra da proporcionalidade e com o teor do disposto no artigo 944, do Código Civil.

Entre as inovações legislativas, destaca-se o princípio da responsabilidade e prestação de contas (LGPD, Artigo 6, inciso X), que para além da perspectiva de não gerar danos, elastece os deveres para impor a necessidade de comprovar adequadamente as medidas preventivas. É um componente que traduz um novo sentido por estabelecer que "é preciso 'proativamente' prevenir a ocorrência de dano" (BODIN DE MORAES, 2019). Trata-se de perspectiva que se harmoniza com a função preventiva do direito de danos, mas como dito, com um sentido mais amplo, ao exigir não apenas o cuidado, mas um agir proativo e o registro das providências implementadas.

Outro ângulo a ser considerado diz respeito à informação e ao consentimento. Tratam-se de dois aspectos diretamente interligados, haja vista que não há consentimento sem a adequada informação. Como já sublinhou o STJ, o dever de informação constitui dever autônomo, cuja violação, mesmo sem falha na realização de procedimento, enseja o dever de reparar (STJ, 2018). Transposto o ensinamento para esfera a proteção de dados pessoais, em primeiro, não há consentimento para tratamento de dados pessoais sem a clareza adequada e

vinculação da finalidade (BRASIL, 2018); em segundo, o consentimento para o procedimento (telemedicina) não se confunde com o consentimento para o tratamento de dados pessoais.

No tocante à reparação por danos decorrentes de incidentes de segurança, vale resgatar a lição de Bodin de Moraes (2019) no sentido de que a atividade de proteção de dados pessoais, quando envolver atividade de risco, atrairá a incidência da responsabilidade objetiva, por força, inclusive, da cláusula geral do Código Civil. Tema para futura reflexão, diz respeito ao regime (sobretudo de excludentes) aplicável em ataques praticados por terceiros. Enquanto o tema não é aprofundado, parece razoável a aplicação por analogia, do enunciado da súmula 479 do STJ, que preconiza a responsabilidade das instituições financeiras, por fraudes, ainda que praticadas por terceiros.

Além disso, vale lembrar que há diversos protocolos de proteção de dados pessoais. Ainda que não haja um padrão oficial no Brasil, a adoção de protocolos demonstra boa prática de segurança e pode atender ao dever de demonstração das medidas implementadas par proteção de dados. Nos Estados Unidos, também recebem destaque a *Health Insurance Portability and Accountability Act of 1996* (HIPAA) e a *Health Information Technology for Economic and Clinical Health (HITECH)* como mecanismos legais voltados à privacidade e à segurança da identidade e das informações de saúde protegidas. Em complemento, a *American Medical Association* estabeleceu diretrizes para atenção por Telemedicina e Telessaúde, tais como protocolos para integridade e segurança do paciente (AMERICAN TELEMEDICINE ASSOCIATION, 2019) que podem inspirar soluções para o Brasil

Em caso de danos com sistemas digitais, a noção de territorialidade por vezes pode ser fluída. Nessa linha, quanto ao foro competente, é interessante observar que, na Europa, para discussão da reparação de dados, o teor da Directiva n. 2011/24/UE do Parlamento Europeu e do Conselho relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços estabelece que "No caso da telemedicina, considera-se que os cuidados de saúde são prestados no Estado-Membro em que o prestador dos cuidados de saúde está estabelecido". A aplicação desse critério no direito brasileiro mostra-se improvável, seja pela imperativa proteção do consumidor, seja pela própria teoria da aparência. Por conseguinte, a violação da proteção de dados, seja pelo tratamento inadequado, seja por abuso de autoridade ou ainda insegurança (de forma ampla), impõe a revisitação de institutos da responsabilidade civil e reflexões que ultrapassam as disposições postas pela Lei Geral de Proteção de Dados.

5 NOTAS CONCLUSIVAS E INDAGAÇÕES RELEVANTES

Em uma sociedade em constante mudança, com uma mutação constante na forma de agir que dificulta a capacidade de compreensão (e regulação), (BAUMAN, 2009), a Telemedicina é realidade, uma "novidade antiga" e demanda urgentes providências éticas e legais. Cada vez mais, os profissionais de saúde recorrem a meios a distância como alternativa para prestação de serviços com maior abrangência, velocidade, comodidade e com menor custo operacional, o que contou com profundo avanço em virtude da COVID19 (TIAGO, 2020).

Entretanto, a Telemedicina, apesar de representar um avanço considerável para o atendimento aos pacientes, acarreta importante desafios ético-jurídicos, em especial quanto à garantia de proteção à privacidade que, como observado no presente estudo, é dividida em 02 (duas) perspectivas: a primeira, no que refere ao direito do paciente a decidir sobre o acesso e o fluxo dos dados pessoais (intimidade); a segunda, quanto ao direito à informação (segurança, transparência, adequação e retificação de dados) (GEDIEL, 2008).

E a elevação do fluxo de dados, pelo emprego da Telemedicina, incorpora novo aspecto à pessoa natural, atribuindo-lhe uma dimensão virtual (digitalização do corpo) e aumenta a exposição do indivíduo, o que, pelas características da própria rede, potencializa o dano, posto que passa a ter maior alcance (no tempo e no espaço) nos caminhos do mundo virtual.

As novidades tecnológicas impõem novos desafios jurídicos e a revisão de paradigmas. A proteção de dados pessoais, para além da tutela da intimidade, avança para novos campos, inclusive pela necessidade de integração de sistemas de informações e a existência de novos riscos.

As novas possibilidades oferecem campo fértil para reflexões jurídicas em temas de alta indagação, tais como a natureza e extensão da responsabilidade no campo da proteção de dados pessoais. Nesse passo, os casos mencionados neste artigo suscitam importantes questões. É preciso perguntar: como fixar os parâmetros para reparação dos danos cuja extensão não é totalmente conhecida? O vazamento de dados proporciona danos *in re ipsa?* A nacionalidade dos hackers importa para definir o foro competente? Pode-se aplicar nessa seara a distinção entre obrigações de meio e de resultado? De que maneira o empenho em prevenir o vazamento e, posteriormente, em contê-lo deve ser levado em conta? Em que medida a demonstração das providências anteriores (*accountability)* é relevante para redução

da reparação, em atenção à finalidade pedagógica ou preventiva da reparação? Deve-se considerar que uma invasão seria um fato inevitável ou exige um incremento ainda maior do sistema de *firewall* adotado?

A responsabilidade civil precisará, dessa maneira, procurar avaliar temas como *firewalls*, protocolos de segurança robustos, proteção de antivírus, sistemas adequados de autenticação de senhas, o que impõe um repensar sobre institutos da responsabilidade civil e reflexões que ultrapassam as disposições postas pela Lei Geral de Proteção de Dados.

O caminho a trilhar é longo e faz lembrar as palavras de Mia Couto: "O que faz andar a estrada? É o sonho. Enquanto a gente sonhar a estrada permanecerá viva. É para isso que servem os caminhos, para nos fazerem parentes do futuro" (COUTO, 2007, p.5).

6 REFERÊNCIAS

AMERICAN TELEMEDICINE ASSOCIATION (ATA). Arlington, VA. 3.212019.

BAUMAN, Zygmunt. **Vida Líquida.** Rio de Janeiro: Zahar, 2009.

BARBOZA; Heloisa Helena; BARRETO; Vicente; MEIRELLES; Jussara. (Org.). **Novos Temas de Biodireito e Bioética**. Rio de Janeiro: Renovar, 2002.

BAROLD SS. «**Willem Einthoven and the birth of clinical electrocardiography a hundred years ago»**. Card Electrophysiol Review 2003; 7(1):99-104. Disponível em <https://www.ncbi.nlm.nih.gov/pubmed/12766530>.

BRASIL. **Decreto-lei nº 591**, Presidência da República Federativa do Brasil. Publicada no Diário Oficial da União de 6 de julho de 1992.

BRASIL. **Decreto-lei nº 47.344**, da República de Portugal. Publicado em 25 de novembro de 1966 e atualizado pela Lei 59/99 de 30/06.

BRASIL. **Lei nº 8.080**, República Federativa Brasileira, Publicada em Diário Oficial da União em 20 de setembro de 1990.

BRASIL. **Lei nº 12.527**, República Federativa Brasileira, Publicada em Diário Oficial da União em 18 de novembro de 2011 (Lei de Acesso à Informação).

BRASIL. **Lei nº 12.965**, República Federativa Brasileira, Publicada em Diário Oficial da União em 23 de abril de 2014 (Marco Civil da Internet).

BRASIL. **Lei nº 13.709**, República Federativa Brasileira, Publicada em Diário Oficial da União em publicado 15 de agosto de 2018, e republicado parcialmente em 15 de agosto de 2018 - Edição extra.

BRASIL. **Portaria nº. 2.546/2011**, Ministério da Saúde, publicada no Diário Oficial da União de 27 de outubro de 2011.

BRASIL. **Regulamento nº. 14/2009**, da Ordem dos Médicos, Diário da República de Portugal, nº 8, II Série, de 11 de janeiro de 2009.

BRASIL. **Resolução CFM nº 1.639/2002**. Publicada no D.O.U. de 12 de agosto de 2002, Seção I, p. 124-5.

BRASIL. **Resolução CFM nº 1.643/2002.** Publicada no Diário Oficial da União de 26 de agosto de 2002, Seção I, p. 205.

BRASIL. **Resolução CFM nº 1.821/2007**. Publicada no D.O.U. de 23 de novembro de 2007, Seção I, p. 252. Parcialmente revogada pela Resolução CFM 2.218/2018.

BRASIL. **Resolução CFM nº 1.931/2009.** Publicada no D.O.U. de 24 de setembro de 2009, Seção I, p. 90; Retificação publicada no D.O.U. de 13 de outubro de 2009, Seção I, p.173.

BRASIL. **Resolução CFM nº 2.107/2014**. Publicada no D.O.U. de 19 de janeiro de 2014, Seção I, p. 94-5.

BRASIL. **Resolução CFM nº 2.227/2018.** Publicada no D.O.U. de 06 de fevereiro de 2019, Seção I, p. 58-59. Revogada pela Resolução CFM 2.228/2019.

BRASIL. **Resolução CFM nº 2.227/2018.** Publicada no D.O.U. de 06 de março de 2019, Seção I, p. 91.

BRASIL. **Resolução ANS nº 389/2016**. Publicada no D.O.U de 01 de agosto de 2016.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito "proativo". Editorial à Civilistica.com. **Revista Civilística.** Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>.

CANADÁ. **Saskatchewan**. Disponível em: <https://www.saskatchewan.ca/government/health-care-administration-and-provider-resources/ehealth>.

CAVANILLAS, José Maria; CURRY, Edward; WAHLSTER, Wolfgang (editores). **New Horizons for a Data-Driven Economy.** A Roadmap for Usage and Exploitation of Big Data in Europe. Alemanha: Springer, 2016.

COUTO, Mia. **Terra sonâmbula**. São Paulo: Cia das Letras, 2007.

CAPITÃO, António; LEITE, Patrícia; ROCHA, Álvaro. **Telemedicina:** Uma análise da situação portuguesa. Iberian Conference on Information Systems and Technologies, CISTI. 2008. [consult. 11-05-19]. Disponível em

<https://www.researchgate.net/publication/278020133_Telemedicina_Uma_analise_da_situacao_portuguesa>.

CÓDIGO DE ÉTICA MÉDICA. **Resolução CFM n. 1.931/2009.** Disponível em: http://www.cfm.org.br. Acesso em: 15 out. 2018.

CORREA. Adriana Espíndola. **O Corpo Digitalizado.** Florianópolis: Conceito Editorial, 2010.

_____. Reflexão sobre as potencialidades da informação como tutela da autonomia privada no âmbito contratual**. Revista da Faculdade de Direito da UFPR**, Curitiba, v. 35, p. 121-133, 2001.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. "Corpo Eletrônico" como Vítima de ofensas em matéria de Tratamento de Dados Pessoais: Reflexões acerca da Responsabilidade Civil por Danos à Luz da Lei Geral de Proteção de Dados Brasileira e a Viabilidade da Aplicação da Noção de Dano Estático ao Mundo Digital. In: BRAGA NETO, Felipe Peixoto. FARIAS, Cristiano Chaves e ROSENVALD, Nelson. **Novo Tratado de Responsabilidade Civil.** 4. ed. São Paulo: Saraiva, 2019.

COVENTRY, Linne; BRANLEY, Dawn Beverley Branley. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. **Maturitas**. 22.abr.2018.

DALLARI, Analluza Bolivar. **Impactos da LGPD na saúde suplementar e a aprovação do parecer sobre MP 869/2018.** Disponível em: <ttps://www.conjur.com.br/2019-jan-03/analluza-dallari-anpd-protecao-bancos-dados-saude>.

Data is giving rise to a new economy. **The Economist.** 6.maio.2017.

DAVIS, Jessica. 30 Percent of Online Health Databases Expose Patient Data. Health it Security. 12. Dec. 2018. Disponível em: <https://healthitsecurity.com/news/30-percent-of-online-health-databases-expose-patient-data>.

_____. Telemedicine vendor breaches the data of 2.4 million patients in Mexico. **Healthcare It News.** 07 de Agosto de 2018. Disponível em: <https://www.bbc.com/news/technology-47292887>.

DECLARAÇÃO DE TEL AVIV, adotada pela 51ª Assembleia Geral da Associação Médica Mundial em Tel Aviv, outubro de 1999.

DRESCH, Rafael de Freitas Valle; FALEIROS JUNIOR, José Luiz de Moura. Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) In: BRAGA NETO, Felipe Peixoto. FARIAS, Cristiano Chaves e ROSENVALD, Nelson. **Novo Tratado de Responsabilidade Civil.** 4.ed. São Paulo: Saraiva, 2019.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thompson Reuters Brasil, 2019.

EUROPEAN COMMISSION. **Towards a thriving data-driven economy,** Communication from the commission to the European Parliament, the council, the

European economic and social Committee and the committee of the regions. Brussels, 2014.

EUROPEAN UNION. **Market study on telemedicine**. Luxembourg: Publications Office of the European Union, 2018.

FALEIROS JUNIOR, José Luiz de Moura., *et. al.* Telemedicina e Proteção de Dados: reflexões sobre a pandemia da covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais**, n. 1016, jun. 2020.

FARIA, Paula Lobato de; CORDEIRO, João Valente. Health data privacy and confidentiality rights: Crisis or redemption?. **Revista Portuguesa de Saúde Pública,** Lisboa, v. 32, n. 2, p. 123-133, dez. 2014. [consult. 24-09-19]. Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0870-90252014000200002&lng=pt&nrm=iso>.

GARCIA, Lara Rocha. **Inovação Tecnológica e Direito à Saúde:** Aspectos Jurídicos, Econômicos, Tecnológicos e de Políticas Públicas. Curitiba: Juruá, 2017.

GARCIA, Marcos Vinicius Fernandes; GARCIA, Marco Aurélio Fernandes. Telemedicina, segurança jurídica e COVID-19: onde estamos? **Jornal Brasileiro de Pneumologia**, São Paulo, v. 46, n. 4, e20200363, 2020.

GEDIEL, José Antônio Peres. Direito e Bioética. **Revista da Faculdade de Direito da UFPR**, Curitiba, a. 29, n. 29, 1996, p. 255-257.

_____. Tecnociência, dissociação e patrimonialização jurídica do corpo humano. In: FACHIN, Luiz Edson (coord.), **Repensando fundamentos do direito civil brasileiro contemporâneo.** Rio de Janeiro: Renovar, 2000. p. 57-85.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o Mercado. **Revista da Faculdade de Direito.** Universidade Federal do Paraná, v. 47, p. 141-153, 2008.

HALE, T. M., KVEDAR, J. C. Privacy and Security Concerns in Telehealth. **Virtual Mentor,** v. 16, 2014. p, 981-985.

HAVE, Ten. Cybermedicine and e-ethics Medicine**, Health Care and Philosoph**y, v, 5, n 2, 2001, p. 117-119.

IBGE. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2017**. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf>.

KFOURI NETO, Miguel. **Responsabilidade Civil do Médico.** 9 ed. rev, atual e ampl. São Paulo: Editora Revista dos Tribunais, 2018.

_____. **Responsabilidade Civil dos Hospitais.** 3 ed. rev, atual e ampl. São Paulo: Editora Revista dos Tribunais, 2018.

LEAO, Camila Furtado et al. **O uso do WhatsApp na relação médico-paciente**. Revista Bioética. Bioét. Brasília, v. 26, n. 3, p. 412-419, Dec. 2018.

LOVERLUCK, Benjamin. **Redes, Liberdades e Controle:** Uma Genealogia Política da Internet. Tradução de Guilherme João de Freitas Teixeira. Petropólis: Vozes, 2018.

MARESCAUX, Jacques, *et al.* **Transatlantic robot-assisted telesurgery.** Nature, v. 413, p. 379–380, set. 2001.

_____. et al. **Transcontinental Robot-Assisted Remote Telesurgery:** Feasibility and Potential Applications. Annals of Surgery, v. 235, n. 4, p. 487–492, set. 2002.

MINISTÉRIO DA SAÚDE. 2019. Brasília, Brasil. [consult. 11-05-19]. Disponível em <http://www.saude.gov.br/trabalho-educacao-e-qualificacao/gestao-da-educacao/qualificacao-profissional/telessaude>.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais:** uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, p. 159-180, 2018. p. 172.

O'FLAHERTY, Kate. **Why Cyber-Criminals Are Attacking Healthcare - And How To Stop Them**. Forbes, Oct 5, 2018.

ONU. DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948.

PARKINS, David. The World's Most Valuable Resource is no longer Oil, but Data. **The Economist.** 06.maio.2017. Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

PEREIRA, Alexandre Libório Dias. **Patient Safaty in e-Health and Telemedicine**. Lex Medicinae – Revista de Direito da Medicina, nº Especial (2014), p 95-106. Disponível em <http://hdl.handle.net/10316/28805>.

PEREIRA, André Gonçalo Dias. **O Consentimento Informado na Relação Médico Paciente:** Estudo de Direito Civil. Lisboa: Editora Coimbra, 2004.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5. ed rev. atual e ampl de acordo com as Leis n. 12.735 e 12.737/2012. São Paulo: Saraiva, 2013.

RAPOSO, Vera Lucia. **Você tem uma nova mensagem:** A prestação de cuidados de saúde na era da telemedicina, in Lex Medicinae, Revista Portuguesa de Direito da Saúde, ano 10, nº 20, 2013. P. 17 a 44.

_____. **Telemedicine:** The legal framework (or the lack of it) in Europe. GMS Health Technology Assessment, NCBI - NIH. 2016.

RIBEIRO, José Medeiros. **Saúde Digital:** um sistema de saúde para o século XXI. Fundação Francisco Manuel dos Santos: Lisboa, 2019

RODOTÀ, Stefano. **La "privacy" tra individuo e colletività.** In: Il diritto privatto nella Società Moderna. Bologna: Mulino, 1977.

_____. Data Protection as a Fundamental Right. In: GUTWIRTH, Serge. **Reinventing Data Protection**?. Springer, Dordrecht, 2009, p. 77-82.

SCHAEFER, Fernanda. **Procedimentos Médicos realizados à distância e o CDC.** 1ª reimpr. Curitiba: Juruá, 2009.

_____. **Proteção de Dados de Saúde na Sociedade de Informação:** Busca pelo Equilíbrio entre Privacidade e Interesse Social. Curitiba: Juruá, 2010.

_____. Telemedicina e Proteção de Dados de Saúde. p. 123-147. In: CORREA, Felippe Abu-Jamra. **Diálogos entre Direito e Medicina:** estudos em homenagem ao CRM/TO**.** Curitiba: Instituto Memória, 2019.

SCHAEFER, Fernanda; GONDIM, Glenda Gonçalves. Telemedicina e Lei Geral de Proteção de Dados Pessoais. In: ROSENVALD, Nelson; MENEZES, Joyceane Bezerra de; DADALTO, Luciana. **Responsabilidade Civil e Medicina.** Indaiatuba: Editora Foco, 2020.

SCHREIBER, Anderson. **Os Direitos da Personalidade.** 2. ed. São Paulo: Atlas, 2013.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Miranda. São Paulo: Edipro, 2016.

STEINMAN, Milton et al. **Impacto da telemedicina na cultura hospitalar e suas consequências na qualidade e segurança do cuidado**. Einstein: São Paulo, v. 13, n. 4, p. 580-586, Dec. 2015. [consult. 01-06-19]. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1679-45082015000400580&lng=en&nrm=iso>.

TAITSMAN, Julie K.; GRIMM, Christi Macrina; AGRAWAL, Shantanu Article**.** Protecting Patient Privacy and Data Security, **The New England Journal of Medicine Perspective**, v. 368, 14.03.2013, p. 977-979.

TIAGO, Ediane. Crise da covid acelera uso de big data e da telemedicina. Transformação digital ganha ritmo em todos os elos da cadeia. **Valor,** 30.09.2020.

TIDY, Joe. Police launch homicide inquiry after German hospital hack. **BBC,** 18.09.2020.

ZHOU, Leming. **A Telehealth Privacy and Security Self-Assessment Questionnaire for Telehealth Providers:** Development and Validation, International Journal of Telerehabiliation, v. 11, n 1, 2019.

WARREN, Samuel D., BRANDEIS Louis D., **The Right to Privacy**, Harvard Law Review, Vol. IV, No. 5. 1890. Disponível em <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>. Acesso em 02.02.2020.

World Health Organization (WHO). **Global Observatory for eHealth** [Internet]. Geneva: WHO; 2005. Disponível em <http://www.who.int/goe/en/>.

NOTA TÉCNICA OBSERVATÓRIO ANAHP, 3º trimestre, 2020, disponível em <https://conteudo.anahp.com.br/nt-observatorio-anahp-3a-edicao>