https://doi.org/10.11606/issn.2316-9044.rdisan.2022.176159
Artigo Original

Revista de Direito Sanitário

http://revistas.usp.br/rdisan

Telemedicina no Brasil: ameaças à proteção de dados pessoais em decorrência da flexibilização da pandemia e da regulamentação precária

Telemedicine in Brazil: threats to the protection of personal data due to both easing of pandemic measures and poor regulation

Diogo Luís Manganelli Oliveira[1]

[1] Universidade Federal de Juiz de Fora. Juiz de Fora/MG, Brasil.
https://orcid.org/0000-0002-0495-0519

RESUMO

O presente trabalho analisou os riscos envolvidos na utilização dos recursos de telessaúde e telemedicina, autorizados durante a pandemia de covid-19, sem um correspondente amadurecimento com relação aos requisitos necessários para garantir a segurança dos dados pessoais e dados pessoais sensíveis de seus usuários, seja pela recente entrada em vigor da Lei n. 13.709/2018, seja pela incipiente criação da Autoridade Nacional de Proteção de Dados, que ainda caminha no sentido de se estruturar organicamente. Sob o lume da metodologia civil-constitucional capitaneada por Perlingieri, o artigo destacou a necessidade de que os requisitos tecnológicos abarcados nas relações privadas sejam devidamente adequados aos valores intrínsecos àqueles delineados no texto constitucional, tendo as normas de direito civil como importante vetor na garantia de tal aplicação. A partir de pesquisa qualitativa, valendo-se de fontes indiretas, inclusive legislação estrangeira, e análise à luz da metodologia dedutiva, elencou-se uma série de considerações para a aplicação de recursos da telemedicina no Brasil de maneira adequada e em sintonia com a proteção de dados pessoais de seus cidadãos.

Palavras-Chave: Pandemia de Covid-19; Proteção de Dados Pessoais; Regulamentação; Telemedicina.

ABSTRACT

The present work analyzed the risks involved in the use of telehealth and telemedicine resources, authorized during the covid-19 pandemic, without a corresponding maturity in relation to the necessary requirements to guarantee the security of personal data and sensitive personal data of users, whether by the recent entry into force of Law no. 13,709/2018, or the incipient creation of the National Data Protection Authority, which is still moving towards an organic structure. Under the light of the civil-constitutional methodology led by Perlingieri, the article highlights the need for technological requirements encompassed in private relations to be duly adapted to the intrinsic values of those outlined in the constitutional text, with the norms of civil law as an important vector in guaranteeing such an application. Based on qualitative research, using indirect sources, including foreign legislation, and analysis in the light of deductive methodology, a series of considerations are listed for the application of telemedicine resources in Brazil in an adequate manner and in line with the protection of personal data of citizens.

Keywords: Covid-19 pandemic; Personal Data Protection; Regulation; Telemedicine.

Correspondência:
Diogo Luís Manganelli Oliveira
diogomanganelli@hotmail.com

Recebido: 14/10/2020
Revisado: 05/07/2021
Nova revisão: 04/10/2021
Aprovado: 06/10/2021

Conflito de interesses:
O autor declara não haver conflito de interesses.

Contribuição dos autores:
O autor é responsável por todo o desenvolvimento do artigo.

Introdução

A promoção do cuidado à saúde figura-se como um dos temas mais frequentes nos debates desenvolvidos em países constituídos como Estados Democráticos de Direito, principalmente a partir da segunda metade do século XX, após a promulgação da Declaração Universal dos Direitos Humanos (DUDH), que, por sua vez, consagra a saúde como uma das previsões que devem ser garantidas aos cidadãos. Conforme o artigo 25 da DUDH (ONU, 1948):

> 1. Toda a pessoa tem direito a um nível de vida suficiente para lhe assegurar e à sua família a saúde e o bem-estar, principalmente quanto à alimentação, ao vestuário, ao alojamento, à assistência médica e ainda quanto aos serviços sociais necessários, e tem direito à segurança no desemprego, na doença, na invalidez, na viuvez, na velhice ou noutros casos de perda de meios de subsistência por circunstâncias independentes da sua vontade.

O avanço tecnológico alcançado nas últimas décadas tem, cada vez mais, proporcionado substancial alteração no modo de vida da população mundial, modificando suas formas de relacionamento, trabalho e consumo. Nesse sentido, o percentual de domicílios brasileiros com acesso à internet era em 2018 cerca de 79,1% (PNAD..., 2020).

Seja no âmbito público, seja no privado, é certo que tais evoluções influenciam fortemente a maneira com que os serviços vêm sendo disponibilizados aos cidadãos, alterando, inclusive, a forma como as ciências médicas têm abordado as várias espécies de enfermidades que afligem a humanidade. Tais mudanças, por sua vez, são acompanhadas *pari passu* por uma ampliação na disponibilidade das tecnologias de informação digital e no acesso a elas por parte da população em geral. As ferramentas e soluções desenvolvidas facilitam a comunicação e podem ser utilizadas não só para o lazer, como também para a ampliação do acesso a determinados recursos e serviços antes possíveis apenas no mundo físico.

Em que pesem os debates acerca da implementação da telemedicina ao redor do globo remontem à segunda metade do século XX, no Brasil a discussão só toma fôlego na virada do milênio, com a popularização da internet e o avanço das tecnologias que permitem sua efetivação por meio da transmissão de informações em tempo real. Contudo, a própria conceituação de telemedicina ainda gera divergências, motivo pelo qual se adota aqui aquela atribuída pela Organização Mundial da Saúde (OMS):

> A prestação de serviços de saúde, onde a distância é um fator crítico, por todos os profissionais de saúde usando tecnologias de informação e comunicação para o intercâmbio de informações válidas para diagnóstico, tratamento e prevenção de doenças e lesões, pesquisa e avaliação, e para a educação contínua dos prestadores de serviços de saúde, tudo no interesse de promover a saúde dos indivíduos e suas comunidades (WHO, 2010; tradução nossa).

Definições similares são encontradas para os termos "telemática" e "telessaúde". Enquanto a telemática pode ser resumida como a simples junção da telecomunicação com a informação – inclusive, sendo utilizada para outros fins que não a própria aplicação da medicina por meio de tais recursos –, a telessaúde relaciona-se com a gestão da saúde pública de maneira geral (URTIGA; LOUZADA; COSTA, 2004).

Cumpre, ainda, destacar que algumas áreas das ciências médicas têm se destacado entre as demais na implementação de tal modalidade de atendimento, como radiologia, patologia, dermatologia e psiquiatria, além do próprio monitoramento de pacientes (WHO, 2016) .

Apesar de concebida há algumas décadas e de representar uma considerável evolução nos atendimentos médicos por facilitar o acesso a eles e possibilitar um contato mais

imediato com o profissional de referência, a incidência prática da telemedicina ainda era, até há pouco tempo e salvo em países desenvolvidos, negligenciada por parte dos profissionais e planos de saúde, sendo fomentada apenas por esparsas ações governamentais de promoção.

Foi a partir da pandemia de covid-19, que impingiu o isolamento social a toda a sociedade brasileira e mundial, que alternativas que propiciam o contato remoto entre médicos e pacientes vieram à tona mais intensamente, tornando a regulamentação da telemedicina ordem do dia para as autoridades de saúde pública (MESKÓ; GÖRÖG, 2020).

Nessa esteira, a Lei n. 13.989/2020 (BRASIL, 2020) foi publicada e, sem mais delongas, autorizou o uso da telemedicina no Brasil durante a crise causada pelo coronavírus.

Inobstante a praticidade conferida pela solução, é fundamental destacar que sua implementação inadequada – ou seja, sem observar as garantias fundamentais dos indivíduos insculpidas pela Constituição Federal de 1988 (CF/88) (BRASIL, 1988) e delineadas pela Lei n. 12.965/2014 (BRASIL, 2014) – Marco Civil da Internet – e, especialmente, pela Lei n. 13.709/2018 (BRASIL, 2018) – Lei Geral de Proteção de Dados (LGPD) – pode gerar severas consequências negativas tanto para os indivíduos quanto para a sociedade.

Assim, o presente trabalho debruçou-se sobre as possíveis implicações oriundas de tal implementação sem a devida atenção aos requisitos normalmente dispensados a sua melhor prática, bem como diante da recente entrada em vigor da LGPD (BRASIL, 2018) e da recente criação material da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), colocando em xeque o respeito a suas previsões.

Ao mesmo tempo, também se fez necessário tecer considerações acerca das influências que tais soluções informáticas podem ter nos direitos coletivos e individuais, ensejando maiores ou menores medidas de regulamentação por parte dos Estados. Logo, o presente trabalho buscou compreender se a utilização da telemedicina, em um contexto de pandemia e frente à ausência de maturidade legislativa nacional para a proteção de dados pessoais, gera riscos iminentes à privacidade de seus usuários e se a Lei n. 13.989/2020 teria o condão de mitigá-los.

Para tanto, a partir da metodologia civil-constitucional, cujo principal expoente é Pietro Perlingieri (2019), buscou-se compreender o Direito Civil como o responsável pela consagração dos valores enraizados no texto constitucional, especialmente por meio da efetivação dos direitos fundamentais, entre os quais está a privacidade insculpida no artigo 5º, inciso X, da CF/88 (BRASIL, 2018).

A metodologia qualitativa de pesquisa com emprego de fontes indiretas permitiu a elaboração das definições ora expostas. Já no que se refere à revisão de literatura, foram consultadas inúmeras fontes bibliográficas para o desenvolvimento do trabalho proposto, valendo-se também de legislações nacionais e internacionais referentes ao tema da proteção de dados pessoais, em especial a Lei n. 13.709/2018 e o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE, 2016).

I Privacidade e autodeterminação informativa

As inovações relacionadas às tecnologias de informação e comunicação (TICs) causaram uma revolução em toda a sociedade, alterando a maneira com que a comunidade se integra, interage e estabelece seu modo de vida. Segundo Rodotà (2008), por muito tempo a partir do fim da era feudal e da consolidação da Revolução Industrial na Europa (RODOTÀ, 2008, p. 27), o conceito de privacidade esteve vinculado aos desejos de uma sociedade burguesa em ascensão, culminando na

definição de Warren e Brendeis (1890) de que a privacidade seria o "direito a ser deixado só" – o que, conforme pontua Doneda (2019, p. 30), imprimiria um traço de individualismo exacerbado naquela sociedade.

Contudo, o avanço das TICs não só representou novas maneiras de interação social, como também gerou uma inédita concepção de tratamento das informações coletadas e trafegadas. Nesse sentido, Doneda (2019, p 33) esclarece que, frequentemente, existem duas justificativas básicas para a utilização de informações pessoais, quais sejam, a eficiência e o controle, tornando sua manipulação de interesse tanto do Estado quanto da iniciativa privada.

Bioni (2020, p. 12) salienta que, a partir de tais avanços, utilizados em conjunto com a inteligência desenvolvida pela ciência mercadológica, os dados pessoais dos cidadãos converteram-se em um fator essencial para o funcionamento do que chamou de "economia da informação". Assim, inserido em uma "economia de vigilância", o cidadão torna-se um mero espectador de suas informações.

Dada a inegável importância que os dados pessoais têm na sociedade moderna, torna-se necessário evoluir no debate sobre sua proteção em âmbito não só individual, como anteriormente destacado, mas também coletivo. Com relação a esse aspecto, Doneda (RODOTÀ, 2019 *apud* DONEDA, 2019, p. 42)) discorre acerca das diferentes concepções da proteção de dados pessoais em uma sociedade tão plural e desigual como o Brasil, já que a compreensão da importância de sua tutela encontra óbice na realização *a priori* de outras necessidades básicas dos indivíduos e varia, pois, conforme o padrão médio de consumo da população. Dado que tal tutela possui interdependência com o próprio livre desenvolvimento da personalidade, ressaltando sua importância coletiva, surge a definição contemporânea de privacidade, que se manifesta, exatamente, na proteção dos dados pessoais (DONEDA, 2019).

Trata-se do que a LGPD (BRASIL, 2018) conceituou, em seu artigo 2º, inciso II, como autodeterminação informativa, ou seja, não apenas a posse irrestrita das informações pessoais pelo indivíduo, em seu sentido patrimonial, mas o poder de controle acerca de sua circulação em face dos prejuízos que seu tratamento indiscriminado pode causar. Sobre tal definição, aponta novamente Doneda (2019, p. 169) que, concebido como um direito fundamental entre os direitos gerais de personalidade, a autodeterminação informativa proporciona ao sujeito o efetivo controle sobre suas informações.

Cabe ressaltar que o direito de acesso às informações tratadas por determinado ente é uma das principais garantias conferidas a seus titulares, proporcionando-lhes o conhecimento necessário sobre o tratamento de seus dados pessoais e possibilitando-lhes a promoção das medidas necessárias para a adequação do tratamento. Rodotà (2008, p. 47) destaca que o direito de acesso corrobora-se a partir da versão dinâmica dos poderes de controle sobre as informações, o que seria a melhor técnica utilizada pelas leis de proteção de dados pessoais. Tal previsão, por sua vez, encontra-se expressamente consagrada entre os princípios delineados pela LGPD (BRASIL, 2018), em seu artigo 6º, inciso IV.

Inobstante, Perlingieri (2019) pontua que a inovação tecnológica deve ser acompanhada pelos desenvolvimentos jurídicos no sentido de se consagrarem os valores constitucionalmente concebidos, não devendo situar-se apenas como refém dos desejos do mercado. Valendo-se da efetivação dos preceitos constitucionais nas relações privadas – exatamente o que se verifica na utilização de recursos de telemedicina para o atendimento de pacientes sem a devida cautela acerca das medidas técnicas de segurança para o tratamento de seus dados pessoais e dados pessoais sensíveis –, deve-se garantir que tais construções não coloquem em risco iminente a pessoa humana e seus direitos fundamentais, ou seja, sua privacidade.

Tepedino (2004), nesse sentido, enfatiza a necessidade de validar inovações tecnológicas diante das eventuais violações que podem causar aos valores basilares do ordenamento jurídico nacional.

Ante o exposto, torna-se essencial estender o debate ora delineado à aplicação das soluções de telemedicina no Brasil, uma vez que o tema tangencia necessariamente o tratamento de dados pessoais, muitas vezes sensíveis, para sua efetivação, e tem como condão gerar riscos tanto a seus titulares, de forma imediata, como à própria coletividade, em uma concepção mediata, dadas as sobreditas características que podem ser extraídas de seu mau uso. Nesse contexto, ressalta-se que tais soluções foram implementadas em um cenário em que a LGPD (BRASIL, 2018) ainda se encontrava em período de *vacatio legis*, aumentando ainda mais a necessidade das reflexões ora pontuadas.

Embora se tenha conhecimento de que tais permissões estejam sendo aplicadas em uma conjuntura de pandemia, e considerando que a autodeterminação informativa insere-se entre aqueles direitos tidos como fundamentais, inclusive conforme pretende fazer, literalmente, a Proposta de Emenda Constitucional (PEC) n. 17/2019 (BRASIL, PEC n. 17/2019), caso admitam-se mitigações temporárias de tais previsões com relação a outros direitos, como a saúde e/ou a liberdade, é necessário utilizar técnicas objetivas, como a ponderação, para que a matéria não seja subjugada indiscriminadamente. Vale destacar que Alexy (2008), ao elaborar a Teoria dos Direitos Fundamentais, definiu que, ante a colisão entre princípios, um terá precedência sobre o outro de acordo com a análise do caso concreto sem que, para tanto, algum deles seja considerado inválido ou afastado pela incidência de uma cláusula de exceção. Na verdade, o problema deverá ser resolvido a partir de um "sopesamento entre os princípios conflitantes" (ALEXY, 2008, p. 90).

II Telemedicina e o controle dos dados do titular

Conforme destacado outrora, o presente trabalho adota como definição de telemedicina aquela estipulada pela OMS (WHO, 2010), tendo em vista que a doutrina não é uníssona quanto ao tema.

A partir de tal especificação, telemedicina resume-se na utilização de TICs para conectar pacientes e profissionais de saúde que estejam separados pela distância, seja propriamente territorial, seja imposta por outros meios (como medidas de isolamento social), a fim de permitir a troca de informações e a realização do atendimento. Todavia, crucial compreender que, ao se permitir a realização de diagnósticos, tratamentos etc., faz-se referência a dados de saúde de seus titulares, que se inserem nas definições de "dados sensíveis" trazidas tanto pelo RGPD (EU, 2016) como pela própria LGPD, ensejando, pois, o cumprimento de requisitos específicos para a garantia da segurança de tais dados.

Tepedino e Teffé (2019, p. 170) afirmam que os dados pessoais sensíveis constituem o "núcleo duro" da privacidade e, por essa razão, mereceram atenção especial do legislador, que lhes imputou requisitos especiais para seu tratamento. Rodotà (2008, p. 248) destaca que os dados sobre saúde sempre exigem atenção particular, não somente pelas previsões contidas em lei, mas pelo fato de se referirem à "nua condição humana, colhendo as pessoas em seus momentos de maior fragilidade, [que] revelam a fraqueza do corpo".

Analisando o escopo da legislação brasileira, Monteiro (2018) define dados pessoais sensíveis como aqueles que podem, em razão de sua natureza, resultar em práticas discriminatórias a seu titular em caso de vazamentos ou acessos indevidos, já que fazem referência a informações de cunho étnico, racial, religioso, político, sexual e de

saúde, além de dados genéticos ou biométricos. Logo, devem ser tratados de maneira adequada, ensejando camadas de proteção mais robustas e hipóteses legais específicas para tanto.

Para que a implementação da telemedicina no Brasil se dê em atenção aos princípios referentes à proteção dos dados pessoais de seus titulares, garantindo não só a segurança do tratamento como, em última medida, a autodeterminação informativa dos cidadãos, deve, portanto, atentar-se a tais considerações.

Em parceria com a Universidade Federal do Rio Grande do Sul (UFRGS) e o Hospital Alemão Oswaldo Cruz (HAOC), o Ministério da Saúde (MS) desenvolveu e publicou, ainda em 2019, estudo acerca dos requisitos a serem considerados para a implementação de soluções referentes à prática da telemedicina no país, inclusive apresentando um *checklist* de apontamentos a serem observados. Em que pese tal documento faça importantes reflexões sobre os aspectos de segurança da informação e as melhores práticas internacionais, não faz referência expressa à legislação de proteção de dados pessoais no país, salvo breve menção a tais práticas na Europa.

Visando ao combate da covid-19, o governo federal promulgou a Lei n. 13.979/2020 (BRASIL, Lei n. 13.979/2020) para definir as ações a serem implementadas, tais como isolamento social, quarentena etc. Ato contínuo, promulgou a Lei n. 13.989/2020 (BRASIL, Lei n. 13.989/2020), que, por sua vez, autorizou a prática da telemedicina no país durante o tempo em que durar a crise da pandemia.

Inicialmente, tem-se que o conceito de telemedicina estipulado pelo legislador é consideravelmente restrito quando comparado àquele definido pela OMS. Igualmente, referida norma é silente quanto aos critérios técnicos a serem implementados e/ou respeitados para que o serviço seja disponibilizado à população no que diz respeito à segurança do tratamento de dados pessoais, sequer fazendo menção à LGPD (BRASIL, 2018) e/ou à Lei n. 12.965/2014 – Marco Civil da Internet (BRASIL, 2014). Por fim, utiliza-se de conceitos genéricos, como "crise", para delimitar o espectro temporal de sua aplicação, acarretando insegurança jurídica.

Nesse contexto e de modo a implementar a telemedicina no país como estratégia de combate à pandemia, o MS publicou, em março de 2020, a Portaria n. 467 (MS, 2020), que dispõe sobre a regulamentação e a operacionalização desse modelo de atendimento, mais uma vez não fazendo qualquer referência a legislações atinentes ao tema.

Por sua vez, o Conselho Federal de Medicina (CFM) encaminhou ao MS o Ofício CFM n. 1756/2020-COJUR (CFM, 2020), em que reconheceu, em caráter de excepcionalidade, a possibilidade e a eticidade da prestação de serviços médicos em modalidade remota, indo além das previsões já contidas na Resolução CFM n. 1.643/2002 (CFM, 2002).

Importante pontuar que a Resolução CFM n. 1.643/2002 (CFM, 2002) já havia sido revogada pela Resolução n. 2.227/2018 (CFM, 2018), do mesmo órgão, que, na esteira da legislação de proteção de dados pessoais, definiu inúmeras obrigações aos prestadores de tais serviços para a garantia da segurança dos pessoais dos pacientes. Todavia, no ano seguinte, esta última também foi revogada, agora pela Resolução n. 2.228/2019 (CFM, 2019) – que, na contramão do exposto, reestabeleceu a vigência daquela primeira, que, por sua vez, não prevê qualquer obrigação nesse sentido.

A Agência Nacional de Saúde Suplementar (ANS), autarquia responsável pela regulação do setor de saúde suplementar no país, publicou a Nota Técnica n. 3/2020/DIRAD-DIDES/DIDES (ANS, NT 3/2020), na qual estabeleceu critérios para que as operadoras de saúde suplementar disponibilizem a telemedicina a seus usuários. Novamente, nenhuma menção foi feita aos requisitos de segurança

e proteção de dados pessoais ou à legislação sobre o tema. Em seguida, a ANS publicou a Nota Técnica n. 4/2020/GGRAS/DIRAD-DIPRO/DIPRO (ANS, NT 4/2020) no intuito de estabelecer medidas para o combate à covid-19, reiterando as previsões acerca da telemedicina. Finalmente, emitiu a Nota Técnica n. 6/2020/GGRAS/DIRAD-DIPRO/DIPRO (ANS, NT 6/2020), na qual afirmou que a cobertura de atendimentos de telessaúde deverá ser garantida (BRASIL, 2020).

Sobreleva esclarecer que, apesar de o Decreto n. 10.747/2020 (BRASIL, Dec. N. 10.747/2020) ter constituído formalmente a ANPD, a agência ainda não iniciou sua atuação ostensiva. Conforme disposto pelo artigo 55-A e J, incisos I e III, da própria LGPD (BRASIL, 2018), uma de suas atribuições seria "zelar pela proteção de dados pessoais", de acordo com as respectivas normas, além de elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, o que significa dizer que tais práticas ainda são inexistentes no país.

Ressalta-se que, no período de *vacatio legis* da Lei n. 13.709/2018 (BRASIL, 2018), o Supremo Tribunal Federal (STF), ao apreciar as Ações Diretas de Inconstitucionalidade (ADI) n. 6.387, n. 6.388, n. 6389, n. 6390 e n. 6393 – todas propostas em face da Medida Provisória (MP) n. 954/2020 (BRASIL, MP n. 954/2020), que, naquela oportunidade, determinava que as empresas de telecomunicações compartilhassem dados pessoais de milhões de consumidores com o IBGE para o que denominou de "fins estatísticos", em decisão histórica –, as acatou liminarmente no sentido de suspender seus efeitos, tomando para si a responsabilidade pelo zelo da proteção dos dados pessoais. Para tanto, entre outros argumentos, afirmou que tal proteção possuiria *status* de direito fundamental e, como tal, deveria ser garantido.

Fato é que, em que pese a ausência de uma autoridade constituída e pronta para zelar por suas previsões naquele momento, a LGPD (BRASIL, 2018) encontra-se vigente desde sua devida publicação e, como tal, deve ser garantida, o que pode ainda ser exigido de outros órgãos igualmente responsáveis pelo zelo de sua obrigatoriedade por terem competência concorrente, como Ministério Público, Defensoria Pública, órgãos de proteção ao consumidor etc. Atualmente, importante salientar, a recém-criada ANPD já se organiza para enfrentar tais desafios.

Concomitantemente, cabe apontar que a primeira ação proposta no Brasil com fulcro no respeito aos ditames da LGPD foi ajuizada apenas dois dias após a entrada em vigor da sobredita legislação, justamente pelo Ministério Público do Distrito Federal e dos Territórios (MPDFT) perante o Tribunal de Justiça da mesma localidade (TJDFT). Trata-se de Ação Civil Pública ajuizada pelo *parquet* sob o argumento de que a parte ré, uma empresa de tecnologia sediada em Minas Gerais, realizaria a comercialização de dados pessoais de milhões de cidadãos brasileiros em seu sítio eletrônico, o que, de acordo com o previsto pela Lei n. 13.709/2018 (BRASIL, 2018) acerca do tratamento de dados pessoais, configurar-se-ia como ilegal.

1 Dados sensíveis, requisitos para seu tratamento e mitigação de riscos

Consoante as considerações desenvolvidas acerca dos dados pessoais que são tratados na telemedicina, tem-se como incontroverso o fato de que envolvem, majoritariamente, dados de saúde, que, por sua vez, foram classificados pelo legislador como sensíveis e, portanto, ensejam requisitos especiais.

Cumpre salientar que, diferentemente do que fez o RGPD europeu ao definir especificamente o que considera "dados de saúde" dentro do conceito de dados pessoais sensíveis, em seu Considerando n. 35 (UE, 2011), a LGPD brasileira, assim como a própria CF/88, foi omissa nesse sentido, abrindo margem para interpretações extensivas com relação à composição dos dados pessoais sensíveis. A partir da

definição europeia, tem-se que, para fins de proteção de dados pessoais, serão considerados como dados de saúde:

> Os dados pessoais relativos à saúde devem incluir todos os dados referentes ao estado de saúde de um envolvido que revelem informações relativas ao estado de saúde passado, atual ou futuro, físico ou mental do envolvido. 2 Isso inclui informações sobre a pessoa física coletadas durante a inscrição ou a prestação de serviços de saúde, conforme referido na Diretiva 2011/24/EU do Parlamento Europeu e do Conselho[1] a essa pessoa física; um número, símbolo ou particular atribuído a uma pessoa física para identificar de forma única a pessoa física para fins de saúde; informações derivadas do teste ou exame de uma parte do corpo ou substância corporal, inclusive de dados genéticos e amostras biológicas; e qualquer informação sobre, por exemplo, uma doença, deficiência, risco de doença, histórico médico, tratamento clínico ou o estado fisiológico ou biomédico do sujeito dos dados independentemente de sua fonte, por exemplo, de um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro. (OJ L 88, 4.4.2011, p. 45) (UE, 2011; tradução nossa)

Já com relação às hipóteses legais de tratamento de dados pessoais sensíveis, a LGPD (BRASIL, 2018) caminhou de maneira similar ao regulamento europeu ao estabelecer que, além da necessidade de consentimento, poderá ser realizado em hipóteses específicas e delimitadas, tais como para o cumprimento de obrigação legal ou regulatória, para a tutela da saúde e proteção à vida etc.

Ainda no que tange à necessidade de anuência do titular dos dados, a LGPD também trouxe a necessidade de que o consentimento seja obtido de maneira específica (art. 8º), além dos requisitos de ser livre, informado e inequívoco já delineados em seu artigo 5º, inciso XII. Para tanto, dedicou seção específica voltada à definição de critérios a serem observados, entre os quais está o consentimento do titular:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

Acerca das inúmeras questões que permeiam a tomada de decisão de um sujeito e a fim de compreender a efetividade do consentimento racional, Bioni (2020) salienta que os indivíduos dispõem de uma "racionalidade limitada", apontando barreiras psicológicas que os influenciam negativamente em tal processo. Denominada de "decisão da utilidade subjetiva", ater-se-ia aos benefícios imediatos, não vislumbrando as eventuais consequências negativas que poderiam ser geradas. Neste mesmo sentido, aponta que a "teoria prospectiva" ressalta que a tomada de decisão tende a ser efetivada no contexto de perdas maiores do que ganhos. Em resumo, afirma que o ser humano tende a procurar uma "zona de conforto" para não se preocupar com os prejuízos, o que denomina de "dissonâncias cognitivas".

Também com relação ao consentimento, Doneda (2019) afirma tratar-se que uma ficção para a finalidade a qual se pretende alcançar. Isso se deve não só à disparidade técnica de negociação entre as partes envolvidas, apresentando-se em uma espécie de "pegar ou largar" e "tudo ou nada", como também ao fato de apresentar-se de maneira "inócua", dada a obscuridade com que as consequências do consentimento podem ser identificadas no que diz respeito ao tratamento de dados pessoais. Ainda, ressalta que estaria relacionado com o "paradoxo da privacidade", ou seja, somente poderá ser invocado na satisfação de sua tutela após ter sido concedido e, consequentemente, ter havido a revelação dos dados. Acerca de sua natureza jurídica, disporia de natureza dúplice e, em referência a Messinetti (*apud* MESSINETTI, 1998), destaca que o consentimento estaria separado em dois diferentes aspectos: como "condição de acesso" na esfera privada, ligado ao poder de autodeterminação, e como "fonte da regra que confirma a legítima inserção de tais dados pessoais no mercado".

Em que pesem tais considerações, Tepedino e Teffé (2019) asseveram que, para a realização do tratamento de dados pessoais sensíveis, como são os dados de saúde, deve-se realizar a coleta do consentimento do titular dos dados de forma específica e destacada, para finalidades também específicas, o que significa dizer que devem ser esclarecidos pormenorizadamente os motivos pelos quais tais dados são necessários para os fins propostos.

De modo a mitigar eventuais impactos do tratamento de tais informações, além do consentimento, aconselha-se a elaboração de relatórios de impacto de proteção de dados (RIPD) para a operacionalização de tais ferramentas, por exemplo, as de telemedicina. Apesar de tal exigência ainda não existir pontualmente no Brasil, dado que caberá à ANPD estabelecer as hipóteses de sua incidência, a experiência internacional do RGPD revela que a avaliação de impacto da proteção de dados (AIPD) será necessária sempre que houver o tratamento das "categorias especiais de dados pessoais", entre as quais encontram-se os dados de saúde. Cabe esclarecer que, no que tange à utilização de dados de rastreamento remoto para o combate da covid-19 (*contact tracing*), o Comitê Europeu para a Proteção de Dados (CEPD) publicou, nas Diretrizes n. 04/2020, a obrigação de que, antes da implementação de tais ferramentas, sejam elaborados suas respectivas AIPDs (EDPB, 2000).

No tocante às outras bases legais previstas no artigo 11 da LGDP (BRASIL, 2018), merece especial atenção aquela que, fazendo exceção ao consentimento, trata da tutela da saúde. Especificamente no inciso II, F, dispõe que o consentimento não será necessário em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Considerando as características que permeiam a prática da telemedicina, pode-se vislumbrar que o consentimento seja desnecessário para o tratamento de dados de saúde nesse caso. Contudo, dadas as incertezas geradas tanto pelo contexto da pandemia como pela ausência de posicionamentos da recém-criada ANPD, além de se tratar de questão a ser avaliada a partir do caso concreto, tem-se que tal afirmação pode ser demasiadamente antecipada, motivo pelo qual ainda se considera o consentimento a melhor maneira de mitigação de riscos em sua aplicação.

2 Práticas Internacionais: *Health Insurance Portability and Accountability Act (HIPAA)*

Considerando-se que a implementação da telemedicina no Brasil tem sido marcada pela ausência de manifestação quanto aos requisitos técnicos relacionados à proteção de dados pessoais de seus usuários, faz-se necessário obter referência das melhores práticas internacionais. Para tanto, considerar-se-ão as previsões contidas na legislação norte-americana *Health Insurance Portability and Accountability Act* (HIPAA), que, debruçando-se sobre o tema, dispôs recomendações para soluções tecnológicas que sejam compatíveis com as regras de privacidades e proteção de dados pessoais estabelecidas.

A HIPAA volta-se à proteção de dados pessoais médicos de trabalhadores quando da mudança ou perda de emprego, tendo como objetivo a redução de fraudes ou abusos na assistência à saúde. Essa lei estabelece requisitos destinados tanto à garantia das regras de portabilidade como da confidencialidade e segurança quando envolver transferência, recebimento, manuseio ou compartilhamento de dados pessoais, assim como a mínima utilização de dados de saúde necessários. A HIPAA está dividida em questões de segurança e privacidade, enquanto a primeira parte abarca o tema a partir de questões como confidencialidade, integridade e disponibilidade dos dados de saúde, a segunda estabelece limites para a utilização e o acesso desses dados.

No que tange às regras de privacidade, concebidas a partir de 2002, têm como intuito salvaguardar a confidencialidade das informações de saúde, denominadas pela lei norte-americana de *Protected Health Information* (PHI) – informações de saúde protegidas. Tais regras aplicam-se a todas as organizações que tenham acesso a dados pessoais de saúde, estabelecendo penalidades pecuniárias para aquelas que violarem as previsões legais.

Com relação à telemedicina, a HIPAA dedicou-se a desenvolver orientações para a proteção das informações de saúde protegidas eletrônicas (*ePHI*). Essas diretrizes aplicam-se a qualquer profissional médico ou organização de saúde que adote tais práticas de atendimento remoto, determinando que: i) somente pessoas autorizadas devem ter acesso a *ePHI*; ii) deve ser implementado um sistema de comunicação seguro para proteger a integridade das *ePHI*; iii) deve ser implementando um sistema de monitoramento de comunicações contendo *ePHI*, de modo a prevenir vazamentos maliciosos ou acidentais (HIPAA..., [s.d.]).

Como ferramentas ideais, a lei norte-americana sugere a utilização de aplicativos de mensagens eletrônicas que cumpram tais requisitos de segurança, desenvolvidos exclusivamente para esta finalidade, proporcionando contato entre pacientes e seus profissionais de maneira adequada e em conformidade com a HIPAA. Ao mesmo tempo, desaconselha o uso de ferramentas populares, como *e-mail* e SMS, destacando o alto custo de sua implementação e a difícil negociação com seus fornecedores, essencial para a limitação de responsabilidade.

Nesse sentido, empresas privadas norte-americanas criaram certificações de conformidade com tal legislação. Em que pese não sejam oficialmente reconhecidas, conforme já

deixou claro o Departamento de Saúde e Serviços Humanos dos Estados Unidos (HHS, na sigla em inglês), tais certificações demonstram, ainda que de maneira preliminar, o cumprimento dos requisitos relacionados às previsões de segurança e privacidade, indicando que as empresas e soluções tecnológicas que delas dispõem estão, minimamente, em conformidade com a legislação.

Cumpre, ainda, assinalar que, de modo a enfrentar a pandemia de covid-19, o HHS flexibilizou suas regras de conformidade com a HIPAA. Para tanto, autorizou a utilização de outros recursos eletrônicos na telemedicina além daqueles já mencionados, mitigando os requisitos de segurança e privacidade e incluindo plataformas de comunicação utilizadas cotidianamente pelo público em geral. Todavia, diferentemente do Brasil – onde sequer existe menção à proteção de dados pessoais na implementação de ferramentas de comunicação nos serviços de saúde –, salientou que as regras mínimas ainda deverão ser adotadas, inclusive excluindo expressamente a utilização de determinados aplicativos que, sabidamente, têm problemas no que tange à privacidade de seus usuários (HIPPA..., 2020).

Considerações finais

É certo que a temática da implementação dos serviços de telessaúde e telemedicina ao redor do mundo enseja inúmeros debates nos campos ético, clínico e de privacidade, motivo pelo qual deve ser aprofundada cada vez mais. Dada a complexidade da questão, viu-se que os países encontram-se, atualmente, em diferentes estágios de sua implementação, motivo pelo qual necessitam de reflexões adequadas a suas realidades, principalmente com relação a aspectos acessórios que são de suma importância para sua efetivação, como desigualdade social, saúde pública, acesso a dispositivos eletrônicos e à internet, cultura de privacidade etc.

Da mesma forma, salienta-se que o contexto de pandemia é um fator extremamente relevante, que deve ser levado em consideração.

Em que pese o Brasil ter iniciado o debate acerca da implementação de recursos de atendimento médico remoto há algum tempo, considera-se que, para a adequada implementação dessa prática, ainda são necessários desenvolvimentos, principalmente no que se refere à segurança e à privacidade com que os dados pessoais de saúde serão tratados. Isso porque, dadas suas características e os riscos envolvidos em sua utilização inadequada, os dados de saúde são classificados como sensíveis, ensejando requisitos específicos para seu tratamento. Nesse contexto, reitera-se que a recém-constituída ANPD ainda não teceu qualquer manifestação quanto à questão.

Conforme delineado pelo marco teórico aplicado ao presente trabalho, é fundamental que os valores definidos pelo legislador originário não sejam postos de lado em prevalência da incorporação de requisitos técnicos sem uma robusta análise dos impactos na própria concepção da personalidade e dignidade humana (PERLINGIERI, 2019). De modo contrário, devem tais axiomas ser cada vez mais incorporados pelas normas aplicáveis do Direito Civil nas relações privadas, o que certamente pode ser obtido a partir da efetivação das definições carreadas na Lei Geral de Proteção de Dados para a garantia, em última instância, do direito fundamental à privacidade.

A partir do exposto, tem-se que a autorização da utilização de tais recursos no Brasil – ainda que, em tempos de pandemia, inicialmente pode-se tolerar a mitigação de tais garantias em prol da saúde pública – possui o condão de gerar riscos tanto aos titulares dos dados como a toda a coletividade.

Considera-se que tais flexibilizações, ainda que temporárias, podem gerar danos permanentes, motivo pelo qual se recomenda, desde já, a adoção dos requisitos mínimos atinentes tanto à segurança das informações como à proteção dos dados pessoais dos

usuários no desenvolvimento de soluções tecnológicas de telemedicina. Não em razão de exigências legais, mas principalmente com relação ao gerenciamento dos riscos que tal prática pode gerar se não realizada da maneira adequada, em observância a tais pressupostos.

Referências

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR – ANS. *Nota Técnica n. 3/2020/DIRAD-DIDES/DIDES*. Disponível em: https://www.ans.gov.br/images/stories/noticias/pdf/covid_19/Nota_Tecnica_n_3_2020_DIRAD-DIDES_DIDES.pdf. Acesso em: 05 jul. 2020.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR – ANS. *Nota Técnica n. 4/2020/GGRAS/DIRAD-DIPRO/DIPRO*. Disponível em: https://www.ans.gov.br/images/stories/noticias/pdf/covid_19/nota-tecnica-4-2020-ggras-dirad-dipro-dipro.pdf. Acesso em: 05 jul. 2020.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR – ANS. *Nota Técnica n. 6/2020/GGRAS/DIRAD-DIPRO/DIPRO*. Disponível em: https://www.sbp.com.br/fileadmin/user_upload/NT_TELESSAUDE.pdf.pdf.pdf.pdf.pdf.pdf. Acesso em 05 jul. 2020.

ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros Editores, 2008.

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

BRASIL, Cristina Índio do. ANS diz que atendimento terá cobertura obrigatória conforme contrato. *Agência Brasil*, Rio de Janeiro, 06 abr. 2020. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2020-04/beneficiario-de-plano-de-saude-pode-fazer-consulta-por-telemedicina. Acesso em: 01 jul. 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 jun. 2020.

BRASIL. *Decreto n. 10.474, de 26 de agosto de 2020*. Aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm#:~:text=1%C2%BA%20A%20Autoridade%20Nacional%20de,e%20privacidade%20e%20o%20livre. Acesso em 22 set; 2020.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 02 jul. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 jun. 2020.

BRASIL. *Lei n. 13.989, de 15 de abril de 2020*. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13989.htm. Acesso em 29 jun. 2020.

BRASIL. *Lei n. 13.979, de 6 de fevereiro de 2020*. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 13 jul. 2020.

BRASIL. *Medida Provisória n. 954, de 17 de abril de 2020*. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 27 jul. 2020.

BRASIL. Senado Federal - SF. *Proposta de Emenda à Constituição (PEC) n. 17, de 03 de julho de 2019*. Altera a Constituição para inserir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 27 jun. 2020.

CONSELHO FEDERAL DE MEDICINA - CFM. *Resolução n. 2.227, de 06 de fevereiro de 2019*. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227. Acesso em: 03 jul. 2020.

CONSELHO FEDERAL DE MEDICINA – CFM. *Ofício n. 1.756, de 19 de março de 2020*. Disponível em: https://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf. Acesso em: 06 jul. 2020.

CONSELHO FEDERAL DE MEDICINA -- CFM. *Resolução n. 1.643/2002, de 26 de agosto de 2002*. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643. Acesso em: 03 jul. 2020.

CONSELHO FEDERAL DE MEDICINA -- CFM. *Resolução n. 2.228/2019, de 06 de março de 2019*. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2019/2228. Acesso em 03 jul. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais:* elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN DATA PROTECTION BOARD – EDPB. *Guidelines 04/2020 on the use of location data contact tracing tools in the contexto of the COVID-19 outbreak*. Adopted on 21 April 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en. Acesso em: 25 jul. 2020.

HIPAA Guidelines on Telemedicine. *HIPAA Journal,* [s.d.]. Disponível em: https://www.hipaajournal.com/hipaa-guidelines-on-telemedicine/. Acesso em 04 jul. 2020.

HIPPA and COVID-19. *HHS.gov. Health Information Privacy*, 21 Oct. 2022. Disponível em: https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html. Acesso em: 27 ago. 2020.

MESKÓ, Bertan; GÖRÖG, Marton. A short guide for medical professions in the era of artificial intelligence. *npj Digital Medicine*, n. 126, p. 1-8, 2020. Disponível em: https://rdcu.be/cem3H. Acesso em: 28 ago. 2020.

MESSINETTI, David. Circolazione dei dati personali e dispositivi de regolazione dei poteri individuali. *Rivista Critica del Diritto Privato*, n. 3, p. 339-407, 1998.

MINISTÉRIO DA SAÚDE – MS. *Portaria n. 467, de 20 de março de 2020*. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996. Acesso em 05 jul. 2020.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *Jota*, 14 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 05 jul. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. *Declaração Universal dos Direitos Humanos*. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 07 jul. 2020.

PERLINGIERI, Pietro. Normas Constitucionais nas relações privadas. *Civilistica.com*. Rio de Janeiro, ano 8, n. 1, 2019. Disponível em: http://bit.ly/2TKUL8X. Acesso em: 27 jun, 2021.

PNAD Contínua TIC 2018: internet chega a 79,1% dos domicílios do país. *Instituto Brasileiro de Geografia e Estatística – IBGE*, Estatísticas Sociais, 29 abr. 2020. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27515-pnad-continua-tic-2018-internet-chega-a-79-1-dos-domicilios-do-pais#:~:text=O%20percentual%20de%20domic%C3%ADlios%20em,%25%20para%2019%2C0%25. Acesso em: 04 jul. 2020.

RODOTÀ, Stefano. A *vida na sociedade da vigilância*: a privacidade hoje. Org. Marina Celina Bodin Moraes; Trad. de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

TEFFÉ, Chiara Spadaccini; TEPEDINO, Gustavo. Consentimento e proteção de dados pessoais. *In*. FRAZÃO, Ana; TEPEDINO, Gustavo e OLIVA, Milena Donato (coord.). *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. Rio de Janeiro: Renovar, 2004.

UNIÃO EUROPEIA – EU. Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011.

UNIÃO EUROPEIA - UE. *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)*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 09 jul. 2020.

URTIGA, Keylla Sá; LOUZADA, Luiz A. C.; COSTA, Carmen Lúcia B. *Telemedicina:* uma visão geral do estado da arte. Faculdade de Medicina, Universidade de São Paulo/USP, 2004. Disponível em: https://telemedicina.unifesp.br/pub/SBIS/CBIS2004/trabalhos/arquivos/652.pdf. Acesso em: 02 jul. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review,* v. 4, n. 5, Dec. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 07 jul. 2020.

WORLD HEALTH ORGANIZATION – WHO. Analysis of third global survey on eHealth based on the report data by countries, 2016. *Global Health Observatory (GHO)*, 2016. Disponível em: https://www.who.int/publications/i/item/9789241511780. Acesso em: 08 jul. 2020.

WORLD HEALTH ORGANIZATION – WHO. Telemedicine: opportunities and developments in Member States: report on the second global survey in eHealth. *Global Observatory for eHealth Series*, n. 2, 2010. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/44497/9789241564144_eng.pdf?sequence=1&isAllowed=y Acesso em: 29 jun. 2020.