INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP

ESCOLA DE DIREITO DE BRASÍLIA – EDB

CURSO DE GRADUAÇÃO EM DIREITO

TAYNÁ GOUVEIA RAMOS

TELEMEDICINA EM TEMPOS DE PANDEMIA: ASPECTOS REGULATÓRIOS E OS DESAFIOS ASSOCIADOS À PROTEÇÃO DE DADOS PESSOAIS

BRASÍLIA

NOVEMBRO 2020

TAYNÁ GOUVEIA RAMOS

TELEMEDICINA EM TEMPOS DE PANDEMIA: ASPECTOS REGULATÓRIOS E OS DESAFIOS ASSOCIADOS À PROTEÇÃO DE DADOS PESSOAIS

Trabalho apresentado como requisito à obtenção da aprovação na disciplina de Metodologia da Pesquisa Jurídica no âmbito da graduação de Direito da Escola de Direito de Brasília – EDB/IDP.

Orientadora: Profa. Dra. Miriam Wimmer.

BRASÍLIA

NOVEMBRO 2020

TAYNÁ GOUVEIA RAMOS

TELEMEDICINA EM TEMPOS DE PANDEMIA: ASPECTOS REGULATÓRIOS E OS DESAFIOS ASSOCIADOS À PROTEÇÃO DE DADOS PESSOAIS

Trabalho apresentado como requisito à obtenção da aprovação na disciplina de Metodologia da Pesquisa Jurídica no âmbito da graduação de Direito da Escola de Direito de Brasília – EDB/IDP.

Brasília, 23 de novembro de 2020.

Profa. Dra. Miriam Wimmer

Professora Orientadora

Prof. Dr. Guilherme Pereira Pinheiro

Membro da Banca

Prof. Ma. Tainá Aguiar Junquilho

Membro da Banca

TELEMEDICINA EM TEMPOS DE PANDEMIA: ASPECTOS REGULATÓRIOS E OS DESAFIOS ASSOCIADOS À PROTEÇÃO DE DADOS PESSOAIS

TELEMEDICINE IN PANDEMIC TIMES: REGULATORY ASPECTS AND CHALLENGES IN PERSONAL DATA PROTECTION

Tayná Gouveia Ramos

RESUMO

Diante da situação de calamidade pública vivenciada pelo País em decorrência da epidemia causada pelo vírus Covid-19, a Telemedicina possibilita o começo de uma nova era no setor de saúde, uma vez que a prática auxilia no controle e no combate à doença. A entrada em vigor da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) tornou imprescindível o enfrentamento dos desafios da Telemedicina também à luz da adequação do tratamento de dados pessoais realizado, sobretudo no tocante aos dados pessoais sensíveis, aos quais compete regulamentação específica. Ainda, foram citadas outras normas regulamentadoras da matéria, como a Constituição Federal de 1988 e normas internacionais. Ao final, foram analisados os principais desafios e levantadas situações-problema hipotéticas no campo da proteção de dados pessoais aplicada à Telemedicina no cenário atual.

Palavras-chave: Covid-19. Telemedicina. e-Saúde. Direito à Saúde. Direito à Privacidade. Lei Geral de Proteção de Dados (LGPD).

ABSTRACT

Faced with the situation of public calamity experienced in Brazil due to an epidemic caused by Covid-19 virus, Telemedicine starts the beginning of a new era in the health area, since the practice contributes to this disease control. The entry into force of the Brazilian General Law of Personal Data Protection – LGPD (Brazilian law nº 13.709/2018) became essential to face Telemedicine challenges, especially when it comes to sensitive personal data, that have specific regulations. In addition, other regulatory standards, such as the Brazilian Federal Constitution and international norms, were mentioned. To conclude, the main challenges related to telemedicine were analyzed through the examination of hypothetical problems.

Keywords: Covid-19. Telemedicine. e-Health. Right to Health. Right to Privacy. General Data Protection Law (LGPD).

INTRODUÇÃO

A Constituição da República Federativa do Brasil garante a saúde como um direito corolário à vida, haja vista que se trata de um direito fundamental e social. O texto constitucional estabelece que:

> Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.[1]

O Direito à saúde é, portanto, direito de todos e dever do Estado. Além disso, as diretrizes de regulamentação e fiscalização desse direito foram fixadas nos artigos 196 e 197 da Carta da República, *in verbis*:

> Art. 196. A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação.
>
> Art. 197. São de relevância pública as ações e serviços de saúde, cabendo ao Poder Público dispor, nos termos da lei, sobre sua regulamentação, fiscalização e controle, devendo sua execução ser feita diretamente ou através de terceiros e, também, por pessoa física ou jurídica de direito privado.

A Organização Mundial da Saúde (OMS) é a agência da Organização das Nações Unidas (ONU) responsável pela agenda internacional dos assuntos referentes às áreas médicas e de saúde. A partir do Regulamento Sanitário Internacional[2], a OMS estabelece direitos e obrigações aos países integrantes, no intuito de defender a saúde pública global, a fim de

---

[1] BRASIL. **Constituição da República Federativa do Brasil de 1988**.

[2] ORGANIZAÇÃO DAS NAÇÕES UNIDAS – BRASIL (ONU-BRASIL). Organização Mundial da Saúde (OMS). **A ONU e a saúde**, 2020.

garantir o definido em seu preâmbulo, para o qual saúde é "estado de bem-estar físico, mental e social"[3].

Sob essa ótica, a OMS, em março de 2020, declarou que o surto causado pelo vírus SARS-CoV-2, também denominado de Covid-19 ou novo coronavírus, revelou um cenário de pandemia[4], ou seja, uma epidemia mundial, caracterizada como "evento extraordinário que pode constituir um risco de saúde pública para outros países devido à disseminação internacional de doenças e potencialmente requer uma resposta internacional coordenada e imediata"[5].

No Brasil, diante desse cenário excepcional, após a confirmação pelo Ministério da Saúde de 904 casos de contaminação no País[6], o Presidente da República buscou estratégias para o enfrentamento da doença. Em abril de 2020, mediante Despacho presidencial, enviou ao Congresso Nacional a Mensagem nº 93[7], no intuito de reconhecer a situação de calamidade pública até o dia 31 de dezembro de 2020, sob o fundamento de que as consequências do novo Covid-19 transcendem a questão de saúde pública ao afetarem a economia por um todo.

Em decorrência das medidas preventivas de controle da disseminação do vírus e levando em consideração a necessidade de auxílio médico no tratamento dos sintomas da doença, o Ministério da Saúde autorizou a prática provisória da Telemedicina, em caráter excepcional e enquanto durar a batalha de combate ao contágio da Covid-19[8]. A partir disso, em 2020 foi criado o TeleSUS, como "uma estratégia de disponibilização de serviço de atendimento pré-clínico de saúde, que visa amplo esclarecimento da população sobre a doença e quando procurar

---

[3] WORLD HEALTH ORGANIZATION (WHO). **Constitution of the world health organization**. 49. ed. 2020.

[4] OLIVEIRA, Pedro Ivo de. Organização Mundial da Saúde declara pandemia de coronavírus. **Agência Brasil (EBC)**, 11 mar. 2020.

[5] ORGANIZAÇÃO DAS NAÇÕES UNIDAS – BRASIL (ONU-BRASIL). *op. cit.*

[6] G1. Brasil tem 904 casos confirmados de novo coronavírus, diz ministério. **G1**, 20 mar. 2020.

[7] BRASIL. Presidência da República. Despacho do Presidência da República. **Mensagem n. 93, de 18 de março de 2020**.

[8] BRASIL. Ministério da Saúde. **Portaria n. 467, de 20 de março de 2020**. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19.

atendimento presencial”[9]. A intenção do governo foi a de informar a população sobre os sintomas e o que fazer em caso de sinais da doença, sem a necessidade de atendimento médico presencial, para manter o isolamento domiciliar.

Durante o ano de 2020, o Sistema Único de Saúde (SUS) desempenhou um papel fundamental no enfrentamento da pandemia. Além da criação do TeleSUS, o SUS contribuiu com o fornecimento de medicamentos, testes rápidos e tratamento adequado, seguindo informações atualizadas obtidas mediante a parceria com universidades públicas. Sobretudo tendo em conta a população mais vulnerável, maioria no cenário brasileiro, “sem o SUS, a pandemia teria instalado o caos social e o Estado contabilizaria um enorme prejuízo com muito mais vidas perdidas”[10]. Vale ressaltar que o sistema é internacionalmente reconhecido por suas ações-modelo na área de saúde, como cobertura universal, campanhas de prevenção, acesso a tratamentos de doenças incomuns, pesquisas públicas de saúde, dentre outras[11].

De outro lado, cabe mencionar os impactos da tecnologia no mundo moderno. A transformação digital causada pela popularização da tecnologia, como computadores, celulares e internet, é fato notório. No entanto, durante o ano de 2020, em razão das medidas preventivas de disseminação do vírus, que obrigam o distanciamento social, a procura por serviços disponíveis *online* aumentou exponencialmente.

Da mesma forma, o setor da saúde também foi afetado por esse movimento e a transformação tecnológica na área já é uma realidade incontornável, a nível mundial e nacional. Com isso, a sociedade vivencia um avançar tecnológico tanto na oferta, no que diz respeito aos hospitais, clínicas, médicos e planos de saúde, quanto na procura, pelo lado dos pacientes, produtos e serviços tecnológicos e digitais no setor de saúde. Associado a esse avançar tecnológico, surgem incertezas relacionadas ao uso indevido dos dados pessoais dos pacientes, sobretudo em relação aos dados pessoais sensíveis.

Os dados pessoais sensíveis são os que dizem respeito a informação de pessoa natural sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a

---

[9] BRASIL. Ministério da Saúde. **TeleSUS**. 2020.

[10] BRASIL. SERGIPE. Secretaria de Estado da Saúde. **SUS tem papel fundamental durante a pandemia**. 19 set. 2020.

[11] SILVA, Welison Matheus Fontes da. RUIZ, Jefferson Lee de Souza. A centralidade do SUS na pandemia do coronavírus e as disputas com o projeto neoliberal. **Physis: Revista de Saúde Coletiva**. v. 30 n. 3. Rio de Janeiro, set. 2020.

organização de caráter religioso, filosófico ou político, ou, ainda, seja referente à saúde ou à vida sexual, genético ou biométrico[12]. Em razão da matéria sensível e tendo em conta a situação de vulnerabilidade em que pode ser colocado o titular, esse tipo de dado passou a ter uma importância considerável no mercado e a ser utilizado para diversos fins, inclusive comerciais.

No que tange à proteção de dados pessoais, Doneda (2010) expõe que, com a experiência, demonstrou-se a necessidade de técnicas de tutela muito mais específicas do que as presentes no arcabouço clássico dos direitos à personalidade, seja pela complexidade técnica que exige a matéria, seja pelo fato de que o processamento de dados pessoais, quase sempre, se dá longe dos olhos do seu titular[13].

Dessa forma, observa-se a importância de um estudo mais aprofundado no tocante ao tratamento de dados pessoais realizado na Telemedicina, principalmente no que se refere ao tratamento dos dados pessoais sensíveis dos pacientes.

A atual situação de grave risco à saúde da população exige ações ágeis por parte do Estado, tornando-se imprescindível a tomada de decisões que observem a proteção à vida e à saúde dos cidadãos. Nesse sentido, dentre outros recursos, o reconhecimento do estado de calamidade pública no Brasil e as medidas preventivas de enfrentamento do vírus Covid-19, como o isolamento social, a realização compulsória de exames médicos, testes laboratoriais[14] e a aprovação do exercício da Telemedicina, inclusive mediante o TeleSUS, constituem um marco na política de enfrentamento à pandemia.

O presente artigo parte da premissa de que a Telemedicina é um serviço indispensável e essencial, que merece a devida notoriedade, não somente por possuir utilidade essencial para aqueles que habitam em regiões distintas, como também pelo fato de ser extremamente relevante em momentos de calamidade pública. A partir disso, este trabalho analisará este fato jurídico e como a Lei Geral de Proteção de Dados (LGPD) se relaciona com ele.

---

[12] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

[13] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE, 2010.

[14]BRASIL. **Decreto n. 7.257, de 4 de agosto de 2010**. Regulamenta a Medida Provisória no 494 de 2 de julho de 2010, para dispor sobre o Sistema Nacional de Defesa Civil - SINDEC, sobre o reconhecimento de situação de emergência e estado de calamidade pública, sobre as transferências de recursos para ações de socorro, assistência às vítimas, restabelecimento de serviços essenciais e reconstrução nas áreas atingidas por desastre, e dá outras providências.

A partir desse cenário, as novas regulamentações que surgiram este ano, elaboradas no intuito de assegurar a prestação de serviços de saúde em meio à pandemia, ilustram de forma clara essa essencialidade. No entanto, a área da saúde ainda carece de regras claras quanto à proteção de dados pessoais. Nesse sentido, este artigo pretendeu avaliar o aspecto regulatório da Telemedicina, em especial os efeitos da aplicação da recém-vigente LGPD. Assim, buscou-se compreender em que pé o Brasil se encontra atualmente e para qual direção caminhará, a fim de encontrar alternativas de adequação para a área de saúde.

Para tanto, foram utilizadas técnicas de pesquisa bibliográfica, à legislação, em reportagens e *sites* oficiais do Governo. Como principal referência bibliográfica, elegeu-se a obra de Danilo Doneda; dentre os diversos documentos consultados, inclui-se a General Data Protection Regulation (GDPR), norma europeia sobre proteção de dados pessoais.

Por fim, no intuito de exemplificar certos âmbitos de aplicação da LGPD no campo da saúde, levantaram-se, ainda, os principais desafios e situações-problema hipotéticas, referentes ao compartilhamento de dados pessoais de saúde, ao exercício de direitos do titular, à responsabilização pelo descumprimento da Lei e às melhores práticas de proteção de dados no campo da saúde.

1 A Regulamentação da Telemedicina no Cenário Epidemiológico Provocado pelo Vírus da Covid-19

Com o propósito de iniciar a discussão sobre o cenário epidemiológico atual do País, elencam-se as atualizações regulatórias da Telemedicina decorrentes da Covid-19, para, depois, detalhar os elementos mais importantes à luz da LGPD.

Desde a edição do decreto de calamidade pública, em março de 2020, é nítido que se está embarcando em uma nova era no setor da saúde. No século XXI, especificamente neste ano, os canais de busca na internet se tornaram um grande aliado daqueles que precisam se consultar, mas não podem se expor aos riscos da pandemia ou não têm tempo, saúde ou recurso para ir até um hospital.

Essa mudança comportamental se deve, em grande medida, ao amadurecimento do que se pode chamar de saúde digital. Esse desdobramento da atenção à saúde tradicional passa a

contar com instrumentos tecnológicos em benefício da saúde e do bem estar dos indivíduos. Tais ferramentas tecnológicas utilizam-se de Inteligência Artificial para que o paciente consiga trocar informações em tempo real a respeito de quaisquer suspeitas, sintomas ou respostas clínicas que envolvam um diagnóstico médico. Além disso, a tecnologia permite a interação entre médico e paciente de forma mais efetiva e acessível, influenciando, assim, na superação de barreiras financeiras e geográficas.

Tem-se que a aplicação de tecnologias no âmbito da saúde também impacta na medida em que abre uma porta considerável e relevante para a democratização do acesso ao conhecimento médico. A partir disso, é possível haver uma melhora no mapeamento das demandas da sociedade, tanto na identificação de tendências epidemiológicas quanto de indicadores pertinentes à temática da saúde.

Hoje, em meio a tantas incertezas sobre o que futuro reserva, é visto que a saúde no meio digital está desempenhando um papel estratégico e fundamental contra o Covid-19. A pandemia trouxe consigo enormes desafios aos sistemas de saúde de países de toda parte do mundo, o que requer novas perspectivas de entendimento a respeito da situação sanitária atual a nível mundial. Dessa forma, a Telemedicina apresenta um meio de auxiliar no controle da doença frente ao cenário de pandemia, uma vez que permite a prática da medicina à distância, por meio da tecnologia.

Em termos regulatórios, a Telemedicina é definida de forma ampla e abrangente como sendo o exercício de medicina através da utilização de metodologias interativas de comunicação audiovisual e de tratamento de dados, com o objetivo de assistência, educação e pesquisa em saúde[15].

Tendo em vista os obstáculos para a plena democratização do acesso à saúde, a Telemedicina pode ser considerada como um meio de permitir que mais indivíduos tenham oportunidade de acesso aos serviços médicos. Não somente o acesso, mas também a isonomia, a qualidade e as despesas são alguns dos desafios encontrados pelos sistemas universais de saúde, que podem ser reduzidos com a implementação instruída, capacitada e devidamente regulamentada da Telemedicina.

---

[15] BRASIL. Conselho Federal de Medicina. **Resolução nº 1.643/2002, de 26 de agosto de 2002**.

Espantosamente, até março de 2020, a Telemedicina entre médico e paciente era proibida, exceto em casos específicos de urgência ou emergência. A tentativa anterior de atualização da respectiva regulação setorial, em 2019, ensaiada pelo Conselho Federal de Medicina (CFM), foi revogada antes mesmo de entrar em vigor.

A legislação supracitada abordou o assunto de maneira rasa, possibilitando a aplicação da prática apenas em caso de suporte diagnóstico e terapêutico emergenciais ou quando solicitado pelo médico responsável. Nesse mesmo sentido, a Resolução nº 2.217/2018 do CFM dispõe ser proibido ao médico prescrever tratamentos sem examinar diretamente o paciente em casos que não sejam de urgência e emergência, ou com impossibilidade comprovada de realizá-lo[16].

A Resolução determina, ainda, que eventual inconformidade com a regulação ético-profissional, no âmbito do Conselho Federal de Medicina (CFM) e dos Conselhos Regionais de Medicina (CRM), sujeita os profissionais médicos às penalidades de: (I) advertência confidencial, (II) censura confidencial, (III) censura pública, (IV) suspensão, e (V) cancelamento do registro mediante a realização de sindicância e processo ético profissional, conduzidos pelo CRM de origem do médico[17].

Contudo, é importante ressaltar que eventual condenação em âmbito administrativo não exclui a possibilidade de discussão da penalidade aplicável pelo Conselho profissional em âmbito judicial, especialmente no que se refere aos aspectos formais do processo administrativo.

Ocorre que, de forma não premeditada, a partir de março de 2020 o País se viu frente a essa situação de pandemia e calamidade pública, cujas principais ações de defrontação podem implicar na restrição de liberdades individuais.

Deste modo, em 19 de março deste ano, o CFM publicou o Ofício nº 1.756/2020 para disciplinar, de forma igualmente superficial, o exercício na modalidade virtual de atividades,

---

[16] *Id*. **Resolução n. 2.227, de 13 de dezembro de 2018**.

[17] SILVA, Marco Antônio Medeiros e. Penalidades aplicadas pelos Conselhos de medicina. **Conselho Regional de Medicina do Distrito Federal (CRM-DF)**. 2020.

como Teleorientação, Telemonitoramento e Teleinterconsulta (auxílio diagnóstico e terapêutico), entre médicos e pacientes enquanto durasse a crise decorrente do Covid-19[18].

Na sequência, em 20 de março, o Ministério da Saúde publicou a Portaria MS nº 467/2020, que regula a Telemedicina em caráter excepcional e temporário para enfrentamento de emergência de saúde pública decorrente da pandemia, em âmbito público e privado. A referida norma permite a realização, à distância, de atendimento pré-clínico, suporte assistencial, consultas, e monitoramento e diagnóstico, inclusive entre médicos e pacientes[19].

A nova regulamentação autorizou expressamente a emissão de atestados e receitas médicas por meios digitais. Assim, durante a pandemia, os médicos poderão atender pela internet, bem como prescrever receitas e atestados. Contudo, para validar sua autenticidade, os documentos precisam de assinatura eletrônica, por meio de certificados digitais emitidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Nota-se o surgimento de uma nova era, repleta de diversos recursos tecnológicos e digitais. Além disso, é possível perceber que a Telemedicina oferece diversas vantagens, tanto para o médico quanto para o paciente. Todavia, na esfera da privacidade, deve-se atentar para aspectos relacionados à proteção dos dados pessoais dos pacientes, que certamente serão compartilhados, armazenados, acessados e processados com a prática. A falta de informação, transparência e segurança no tratamento dessas informações preocupa, com razão, os cidadãos.

A Lei Geral de Proteção de Dados (LGPD) estabelece que o tratamento de dados pessoais sensíveis precisa caminhar de acordo com a sua finalidade, ou seja, o tratamento somente será adequado quando for realizado para cumprir a finalidade informada ao titular ou que fundamente a base-legal em que pode ser enquadrado. Além disso, também prevê que os dados do paciente devem ser protegidos de forma rigorosa quanto à segurança da informação.

---

[18] BRASIL. Conselho Federal de Medicina. **Ofício n. 1.756/2020, de 19 de março de 2020**.

[19] BRASIL. Ministério da Saúde. **Portaria n. 467, de 20 de março de 2020**. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19.

Dessa forma, é notório que, para manter a segurança dos dados de saúde do paciente, é necessária a realização de mapeamento de dados e fluxo capaz de apontar as vulnerabilidades que podem surgir durante a prática de tratamento, bem como os planos de mitigação dos riscos previstos.

Segundo afirma Rodotà (2008), no tocante aos dados de saúde, "a proteção especial atribuída a estes dados não se justifica somente por referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provoca discriminações"[20]. Assim, fica evidente a preocupação com o uso indevido dos dados sensíveis de pacientes para os mais diversos fins, inclusive comerciais. O conhecimento desses dados por parte de companhias seguradoras ou planos de saúde poderá causar discriminações, bem como prejudicar futuras contratações. Dados de geolocalização, ainda que sejam considerados dados não sensíveis, podem ser utilizados de forma nociva a seu titular ou para a verificação de informações íntimas.

Entretanto, ainda que levados em consideração os perigos supracitados, o que se tem no momento é um cenário de incerteza e de grandes danos à saúde coletiva.

Schwab (2016) [21] destaca que as mudanças produzidas pela conectividade digital em nossa sociedade geram aspectos positivos e negativos, ressaltando que os pontos negativos se referem diretamente à perda de privacidade, uso indevido e diminuição da segurança de dados, por exemplo.

Dessa forma, fica evidente que os dados pessoais sensíveis requerem uma tutela diferenciada e especial, de forma a evitar que as informações de seus titulares sejam usadas indevidamente, em comercialização, no embasamento de discriminações ou outros prejuízos ao titular da informação[22].

---

[20] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. 1 ed. Rio de Janeiro: Renovar, 2008.

[21] SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016. p. 159.

[22] ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comissão Interamericana de Direitos Humanos (CIDH). **Resolución n. 1/2020, de 10 abr. 2020**. Pandemia y Derechos Humanos en las Américas.

2 A Aplicação da Lei Geral de Proteção de Dados (LGPD)

No plano internacional, o Regulamento Geral sobre a Proteção de Dados, conhecido pela sigla GDPR[23], editada pela União Europeia e em vigor desde maio de 2018, afetou não somente os países europeus, mas todos os outros que estabeleciam negócios com a Europa, inclusive o Brasil.

As primeiras normas europeias sobre privacidade emergiram sob um contexto de vigilância estatal sem precedentes, invadindo a vida privada durante o nazismo na Alemanha. Dessa forma, os direitos humanos associados à proteção de dados pessoais foram concebidos a partir do resultado do Holocausto e do abuso nazista, em que os dados pessoais obtidos pelo governo serviram para perseguição[24].

Ainda sob a ótica do direito à privacidade no contexto pós-Segunda Guerra Mundial, tem-se que os legisladores lutaram para responder a um tipo específico de violação de privacidade: a violação do direito à privacidade do lar. Surpreendentemente, o legado do governo de uso indevido de informações pessoais, infiltração de grupos políticos dissidentes ou interceptação de comunicações não se tornou o centro das atenções. Em vez disso, o parlamento estava preocupado em garantir o direito – um direito do homem, ou seja, masculino – de dirigir a família da forma como ele desejasse, em oposição a Políticas nazistas que colocavam o governo diretamente no comando de reprodução, família e casamento[25].

Diante da previsão legal de aplicação da lei em território estrangeiro, nos casos em que o país em questão participar de relações comerciais que envolvam dados de titulares europeus, a GDPR tornou-se modelo mundial. Em razão desse dispositivo, vários outros países se viram obrigados a elaborar uma legislação que assegure o tratamento de dados pessoais seguro e adequado.

---

[23] UNIÃO EUROPEIA (UE). **Regulation (EU) n. 2016/679**. General Data Protection Regulation (GDPR). 27 abr. 2016.

[24] CAREY, Sabine C. GIBNEY, Mark. & POE, Steven C. **The Politics of Human Rights: The Quest for Dignity**, 2010.

[25] Nesse sentido, BLOCK, Gisela. Racism and Sexism in Nazi Germany: Motherhood, Compulsory Sterilization, and the State *in* BRIDENTHAL, Renate. GROSSMAN, Atina. & KAPLAN, Marion. **When Biology Became Destiny: Women in Weimar and Nazi German**. 1984; e KOONZ, Claudia. **Mothers in The Fatherland**: Women, the Family, and Nazi Politics, 1987.

No mesmo sentido do ordenamento jurídico brasileiro, a GDPR reforça o caráter de que nenhum direito é absoluto e tampouco o é a proteção de dados pessoais. Para evidenciar esse ponto de conexão entre a privacidade e as questões sociais no uso de dados, o texto legal traz que "[...] o direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade" [26].

A legislação brasileira se insere nesse mesmo contexto histórico de evolução de normas de proteção de dados pessoais, tendo forte inspiração na legislação europeia. Antes de dar sequência à matéria, no cenário nacional, é importante mencionar a Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), que foi a primeira legislação voltada unicamente para um tema digital e contribuiu diretamente para a promoção da cultura de proteção de dados que a LGPD veio firmar. No entanto, enquanto a LGPD abrange a proteção de dados tratados em meio físico ou digital, o MCI trata apenas de meios digitais online.

No art. 1º do MCI é disposto que a lei "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria"[27]. Em decisão no STJ, a Ministra Maria Thereza de Assis comentou acerca dos princípios versados no MCI:

> 8. A Lei n. 12.965/2014, conhecida como Marco Civil da Internet, em seu art. 7º, assegura aos usuários os direitos para o uso da internet no Brasil, entre eles, o da inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de suas comunicações pela internet, bem como de suas comunicações privadas armazenadas.[28]

Adiante, na lei, é prevista a garantia da neutralidade da rede (art. 9º), a responsabilização dos agentes de acordo com suas atividades, a preservação da natureza participativa da rede e a liberdade dos modelos de negócios promovidos na internet. Aqui, cabe frisar que os princípios expressos no MCI não excluem outros previstos no ordenamento jurídico brasileiro.

---

[26] UNIÃO EUROPEIA (UE). **Regulation (EU) n. 2016/679**. General Data Protection Regulation (GDPR). 27 abr. 2016.

[27] BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[28] BRASIL. Superior Tribunal de Justiça. Habeas Corpus: HC 315220 RS. Relatora Ministra Maria Thereza de Assis Moura. Sexta Turma. DJe 9/10/2015. **STJ**, 2015.

Nesse sentido, Miriam Wimmer disserta sobre outras normas que são igualmente aplicáveis ao direito digital e à proteção de dados pessoais:

> Já antes da aprovação da LGPD, inúmeras normas veiculavam, a partir de uma ótica eminentemente setorial, regras acerca do tratamento de dados pessoais. Cite-se, a título exemplificativo, o Código de Defesa do Consumidor ((CDC) Lei nº 8.078, de 11 de setembro de 1990), a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), a Lei Geral de Telecomunicações ((LGT) Lei nº 9.472, de 16 de junho de 1997) e, no que tange especificamente aos dados custodiados pelo Poder Público, a Lei de Acesso à Informação ((LAI) Lei nº 12.527, de 18 de novembro de 2011).[29]

Assim como na GDPR, a LGPD coloca o titular dos dados como protagonista das relações jurídicas que envolvam o tratamento de seus dados[30], não somente por regular a proteção de dados pessoais, mas, sobretudo, porque elege como fundamento em seu art. 2º, inciso II, a "autodeterminação informativa", que significa o direto de escolher quais dados serão utilizados, como também os limites e o prazo dessa utilização[31]. Nesse sentido, a Lei brasileira define um conceito de suma importância, em especial no campo da saúde, que é o de dados pessoais sensíveis.

Dados sensíveis são os dados que acarretam maior risco ao titular, por serem passíveis de utilização para fins discriminatórios, necessitando, por isso, de medidas mais rigorosas para o seu tratamento. Para fins de diferenciação, é importante mencionar também o conceito de dados de saúde, que está dentro da categoria de dados sensíveis, incluídos os dados referentes à saúde ou à vida sexual, bem como dados genéticos e biométricos. Esse conceito integra também dados pessoais que podem não parecer ser de saúde, mas que, dentro de um contexto, podem possibilitar a leitura de dados de saúde, como a frequência de corridas de um indivíduo por meio da frequência cardíaca[32].

---

[29] WIMMER, Miriam. Proteção de Dados Pessoais no Setor Público: incidência, bases legais e especificidades. **Revista do Advogado**. v. 144, p. 126-133, 2019.

[30] Art. 5º, inciso X, da LGPD: "Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."

[31] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[32] Art, 5º, inciso II, da LGPD: "Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;"

Portanto, na seara de dados pessoais sensíveis, exige-se maior segurança e normas estritas no que se refere ao compartilhamento da informação. Nesse sentido, o art. 11, § 4º, incisos I e II, da LGPD limita as hipóteses do compartilhamento de dados sensíveis. Eis o que previsto no dispositivo:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> [...]
>
> § 4º 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 a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência
>
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)[33]

Em relação aos dados de saúde, é preciso deixar claro que são dados dotados de extrema sensibilidade e que o seu uso indevido pode gerar danos irreparáveis ao titular. Assim, deve haver uma atenção redobrada quanto a esse tipo de dado, a fim de evitar que sejam compartilhados indevidamente, vazados ou destinados a propósitos distintos de sua finalidade ou prejudiciais ao titular da informação[34]. Assim, verifica-se que a LGPD traz regras específicas e restritas para o tratamento desses dados, sejam eles dados pessoais ou dados pessoais sensíveis.

3 O Tratamento de Dados Pessoais Sensíveis no Contexto da Telemedicina

[33] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

[34] DIAS, Rodrigo dos Santos. BORTMAN, Roberto. ZANGARINO JÚNIOR, Sérgio. O Código de Defesa do Consumidor e sua Aplicação às Healthtechs. **UNISANTA Law and Social Science**, v. 7, n. 3, p. 605-620, 2018.

Para tratar dados pessoais, é exigido que o agente de tratamento se fundamente em uma base legal. Em vista disso, bases legais são tidas como as hipóteses fáticas em que o tratamento de dados deve se enquadrar para ser dotado de adequação, a depender da categoria do dado e da finalidade do tratamento. A LGPD traz 10 hipóteses para o tratamento dos dados pessoais[35], em sentido amplo, e 8 hipóteses para o tratamento dos dados pessoais sensíveis[36].

No tocante aos dados pessoais, o legislador optou por conferir às bases legais o mesmo peso, dessa forma, o consentimento vale como base legal tanto quanto a tutela da saúde ou o cumprimento de contrato, sendo necessário analisar qual a base legal mais adequada em cada contexto.

Já em relação aos dados pessoais sensíveis, o legislador optou por restringir as hipóteses de base legal, não podendo ser utilizadas nos casos de execução de contrato, legítimo interesse do controlador, proteção de crédito e prevenção à fraude. O que significa dizer que, no tocante à dados de saúde, usando-se como base legal a proteção da vida ou a tutela da saúde, por exemplo, o tratamento de dados pessoais sensíveis é permitido.

No tocante à base legal do consentimento, a Lei prevê regras específicas para que a coleta seja considerada adequada. É previsto que, no tratamento de dados pessoais sensíveis de saúde, o consentimento deve ser: (i) informado; (ii) livre; (iii) para finalidades determinadas; e (iv) específico. Ou seja, no momento da coleta, o titular deve manifestar-se expressa e livremente no sentido de que consente que os seus dados pessoais sensíveis sejam tratados para uma certa finalidade, determinada e específica.

Conforme o que já foi exposto, tem-se que a LGPD foi fortemente influenciada pela regulação da União Europeia. Dessa forma, é interessante observar como a ideia de consentimento adequado tem sido abordada pelos países do bloco. Carolan (2016)[37] revela falar em ‘consentimento ativo’, sugerindo a impossibilidade de obter-se o consentimento de forma subentendida, mencionando a mera inatividade do titular, a não oposição ao tratamento e o uso reiterado de determinado serviço.

---

[35] Art. 7º, incisos I a X, da LGPD. Ver: BRASIL, 2018, *op. cit*.

[36] Art. 11, incisos I e II, da LGPD. Ver: BRASIL, 2018, *op. cit*.

[37] CAROLAN, Eoin. The continuing problems with online consent under the Eus emerging data protection principles. **Computer Law and Security Review**. V. 32. Ed. 3, jun. 2016.

Também é prevista em lei a obrigação do responsável de comprovar que obteve consentimento da forma adequada, sob pena de ser considerado inválido. Para mais, caso haja alguma alteração das finalidades de tratamento, deve-se informar o titular previamente, a fim de ser coletado um novo consentimento. Por fim, deve ser garantido ao titular dos dados, de forma facilitada, o direito de revogação de seu consentimento ou de exclusão de seus dados pessoais.

São notórias as vantagens, assim como os perigos, riscos e inseguranças decorrentes da coleta e do tratamento de dados pessoais, especialmente quando se trata de dados pessoais sensíveis de saúde, como os tratados em sede da Telemedicina. Alguns autores consideram que esse risco é tão evidente que pode chegar a impactar o livre arbítrio e a dignidade humana daqueles que estão sujeitos a essa coleta[38].

Nesse ponto, Doneda (2006) destaca o princípio da autodeterminação informativa, que possibilita ao titular impor condições de acesso à sua esfera privada. Ademais, há o aspecto da legitimação propriamente dita no tocante à comercialização de dados pessoais[39]. Fica claro, então, a relevância do consentimento, da autodeterminação e da legitimação no âmbito da proteção de dados pessoais, devendo-se buscar sempre harmonia, razoabilidade e equilíbrio entre todos.

Nessa perspectiva, independentemente das inseguranças e incertezas, deve-se acreditar que a aplicação da LGPD será adequada e trará clareza ao cidadão em relação à forma com que o detentor do dado irá tratar as informações coletadas.

4 Proteção de Dados Pessoais Sensíveis de Saúde no Contexto da Telemedicina: Principais Desafios

[38] CUKIER, Kenneth. MAYER-SCHONBERGER, Viktor. **BIG DATA**. New York, 2014. p. 170.

[39] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

São evidentes os benefícios da Telemedicina, como ajudar a conter custos, evitar idas desnecessárias ao hospital e encaminhar o paciente à especialidade médica mais adequada para tratar a sua enfermidade, facilitando o processo de prestação de serviço[40].

Ademais, observa-se que o tratamento de dados pessoais sensíveis de saúde deve se dar no sentido de evitar possível acesso não autorizado às informações, por meio de protocolos de segurança da informação adequados e plataformas atualizadas constantemente, a fim de evitar ataques virtuais.

Dessa forma, a partir da análise de situações-problema hipotéticas, serão analisados os principais desafios relacionados à aplicação da LGPD: (i) hipóteses legais que permitem o compartilhamento de dados pessoais sensíveis de saúde; (ii) direitos dos titulares dos dados; (iii) responsabilização por descumprimento da LGPD; e, por fim, (iv) melhores práticas de proteção dos dados pessoais sensíveis de saúde.

4.1 Primeiro Desafio: O Compartilhamento de Dados Pessoais Sensíveis a Empresas de Plano de Saúde

O primeiro desafio a ser analisado é a situação descrita na sequência. Durante a pandemia, diversas empresas do ramo da saúde passaram a tratar dados sensíveis de pacientes que optaram por fazer uso da Telemedicina. Partindo da situação de comercialização de informações de saúde dos pacientes, contidas nos registros do médico ou outro profissional com acesso ao dado, para planos de saúde, de maneira a permitir a avaliação da saúde dos clientes, e, ao mesmo tempo, a cobrança de tarifas diferenciadas, com base nos riscos avaliados. Que base legal poderia autorizar o compartilhamento de tais dados?

Ao examinar o caso em questão, é importante rememorar que o tratamento de dados pessoais, especialmente no tocante aos dados sensíveis, deve ser compatível com as finalidades informadas ao titular para as quais foram coletados inicialmente. De acordo com o princípio da finalidade[41], o tratamento de dados pessoais deve ser realizado com finalidades legitimas e

[40] WEN, Chao Lung. **Telemedicina e Telessaúde**: Inovação e Sustentabilidade. GoldBook: Inovação Tecnológica em Educação e Saúde, p. 86-104, 2011.

[41] Art. 5º, inciso I, da LGPD. Ver: BRASIL, 2018, *op. cit*.

específicas, sempre informadas ao titular dos dados. Já o princípio da adequação[42] determina que o processamento dos dados deve ser congruente com as finalidades informadas ao titular. Vale dizer, ainda, que os princípios da proteção de dados estão expressamente previstos no art. 6º da Lei Geral de Proteção de Dados (LGPD).

Para mais, não há dúvida quanto à sensibilidade dos dados pessoais tratados no contexto da Telemedicina, uma vez que a partir de informações médicas privilegiadas é possível inferir diversas suposições referentes à saúde do titular do dado. Levando em consideração que os dados coletados numa Teleconsulta, por exemplo, sejam referentes a eventual enfermidade que o paciente sofra e tenham sido coletados com o fim de acessar as informações em consultas futuras, o tratamento secundário dos dados narrado, com o fim de comercialização e avaliação dos ricos de seus titulares por seguradoras de planos de saúde, pode não ser compatível com a finalidade estipulada na época da coleta dos dados do titular.

No que se refere às hipóteses legais que permitem o compartilhamento de dados pessoais de saúde, a LGPD autoriza o compartilhamento desses dados com o objetivo de obter vantagem econômica somente em determinadas situações, vejamos:

> § 4º 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 de: (Redação dada pela Medida Provisória nº 869, de 2018)
>
> I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)
>
> II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)[43]

Dessa forma, a lei dispõe que será permitido o compartilhamento de dados pessoais de saúde nos casos de (a) portabilidade dos dados, quando solicitada pelo titular, e de (b) transações financeiras relacionadas a assistência farmacêutica e de saúde, serviços auxiliares de terapia e diagnose.

Nesse sentido, em relação ao caso fictício supracitado, dificilmente o compartilhamento de dados na forma pretendida seria considerado legítimo, ainda que com o consentimento do

[42] Art. 5º, inciso II, da LGPD. Ver: BRASIL, 2018b, op. cit.

[43] Art. 5º, § 4º, da LGPD. Ver: BRASIL, 2018b, op. cit.

titular. Possivelmente, haveria uma violação aos princípios da finalidade e da adequação. Contudo, seria possível utilizar tais dados de forma anonimizada, ou seja, sem estarem ligados a indivíduos identificados ou identificáveis, visando analisar os hábitos gerais de seus clientes.

4.2 Segundo Desafio: Direitos do Titular, Portabilidade e Exclusão de Dados Pessoais de Saúde

Para fins de análise dos direitos dos titulares envolvidos no contexto das Telemedicina, em particular o direito à eliminação de dados pessoais, ilustra-se a seguinte situação-problema. Um paciente utilizou-se de Teleconsultas, durante a pandemia, para fazer acompanhamento psiquiátrico e tratar a depressão, com um médico especializado. Acontece que, ao mudar de convênio de saúde, o paciente perdeu a cobertura na clínica ao qual o profissional é vinculado. Com isso, o paciente optou por trocar de médico e passou a fazer o seu acompanhamento em outra clínica, também na modalidade virtual. Tendo em vista que a LGPD dispõe sobre os direitos de portabilidade e exclusão dos dados pessoais, o paciente solicitou, junto à antiga clínica, a portabilidade de seus dados para a nova, além da exclusão de seus dados do banco de dados da empresa.

O caso em questão envolve direitos do titular, a saber, o direito de portabilidade e de eliminação dos dados, garantidos pela LGPD no art. 18, incisos V e VI:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> [...]
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;[44]

Neste ponto, é importante ter em mente que, conforme já mencionado neste trabalho, nenhum direito é absoluto. Existem hipóteses, previstas na LGPD, em que a empresa é

[44] Art. 18, incisos V e VI, da LGPD. Ver: BRASIL, 2018b, op. cit.

legitimada a não eliminar os dados[45]. Assim, é permitida a manutenção das informações, desde que para cumprir uma das seguintes finalidades: (a) cumprimento de obrigação legal; (b) estudo por órgão de pesquisa, garantida a anonimização dos dados pessoais; (c) transferência a terceiro, desde que sejam respeitados os requisitos de tratamento dispostos na lei; ou (d) uso exclusivo do controlador, vedado seu acesso por terceiro e desde que anonimizados os dados.

Quanto ao direito de portabilidade solicitado pelo paciente, a antiga clínica terá que transferir os dados do paciente para a nova empresa. Neste ponto, vale realçar que não há obrigação de transferência em relação aos dados porventura anonimizados[46].

No que se refere ao direito de exclusão dos dados, também requerido pelo paciente, os dados do prontuário médico, estejam eles disponibilizados em meio físico ou eletrônico, obtidos durante todo o período de tratamento, não poderiam ser excluídos pela clínica. Isso porque os dados de prontuários médicos com até 20 anos devem ser guardados, em razão de obrigação legal imposta pela Lei nº 13.787/2018, em seu artigo 6º:

> Art. 6º Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados.
>
> § 1º Prazos diferenciados para a guarda de prontuário de paciente, em papel ou digitalizado, poderão ser fixados em regulamento, de acordo com o potencial de uso em estudos e pesquisas nas áreas das ciências da saúde, humanas e sociais, bem como para fins legais e probatórios.
>
> § 2º Alternativamente à eliminação, o prontuário poderá ser devolvido ao paciente.
>
> § 3º O processo de eliminação deverá resguardar a intimidade do paciente e o sigilo e a confidencialidade das informações.
>
> § 4º A destinação final de todos os prontuários e a sua eliminação serão registradas na forma de regulamento.
>
> § 5º As disposições deste artigo aplicam-se a todos os prontuários de paciente, independentemente de sua forma de armazenamento, inclusive aos microfilmados e aos arquivados eletronicamente em

[45] Art. 16, incisos I a III, da LGPD. Ver: BRASIL, 2018b, op. cit.

[46] Art. 18, § 7º, da LGPD. Ver: BRASIL, 2018b, op. cit.

> meio óptico, bem como aos constituídos por documentos gerados e mantidos originalmente de forma eletrônica.[47]

Aqui, mostra-se relevante o destaque para o princípio da necessidade, disposto no art. 6º, inciso III, da LGPD. No mesmo sentido, na Regulamentação europeia, a GDPR, exige-se que o tratamento dos dados envolva apenas dados necessários para o objetivo da respectiva finalidade, ou seja, nem para mais nem para menos. Fica, portanto, a indagação: quais dados têm de ser excluídos e quais dados devem ser mantidos?

Não há uma resposta clara e objetiva para tal questão, tornando o cumprimento do direito controverso. Ainda, há os obstáculos naturais decorrentes da novidade da matéria, uma vez que há a previsão de regulamentação adicional pela Autoridade Nacional de Proteção de Dados (ANPD), o que ainda não ocorreu, já que a Diretoria do órgão foi recentemente nomeada.

Conclui-se, por fim, que, ainda que os direitos dos titulares não sejam absolutos, é necessário que as empresas do setor de saúde desenvolvam estratégias para garanti-los, sobretudo no tocante aos dados sensíveis. É preciso deixar clara também a importância do mapeamento e fluxo dos dados tratados no modelo de negócio da empresa, bem assim da indispensável identificação das bases legais para a adequação do tratamento realizado.

Assim, mostra-se necessária a conformidade das empresas aos novos padrões legais, buscando meios eficientes de cumprir com os pedidos de requisição de direitos.

4.3 Terceiro Desafio: Vazamento de Dados e Responsabilização por Descumprimento da LGPD

Como terceiro desafio, apresenta-se a situação hipotética de uma clínica privada de oncologia e genética de Brasília, que detectou atividades suspeitas em sua rede. Após análises, foi comprovada uma invasão em seu banco de dados, na qual foram acessados laudos e prontuários contendo diversos dados pessoais sensíveis de pacientes, incluídos testes genéticos de familiares de pacientes. Nesse cenário, a clínica precisa buscar apoio profissional para encontrar soluções de segurança da informação para o problema.

---

[47] BRASIL. **Lei n. 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Um dos maiores tormentos do mundo atual consiste no vazamento de dados, comumente causados por falhas de segurança. Diversos casos são expostos todos os dias, os vazamentos abrangem desde dados bancários[48] até dados biométricos[49].

Quando as normas referentes ao tratamento de dados pessoais são descumpridas, como a violação do princípio da segurança, que obriga a empresa a utilizar-se de "medidas técnicas e administrativas aptas a proteger dados pessoais de acessos não autorizados e situações acidentais ou ilícitas"[50]., é possível a aplicação de sanções de cunho administrativo. Na Lei, também é prevista a regulamentação de implemento dessas sanções pela Autoridade Nacional de Proteção de Dados (ANPD), o que não impede a condenação judicial no âmbito do direito civil ou direito penal.

O artigo 52 da Lei Geral de Proteção de Dados (LGPD) dispõe sobre as sanções aplicáveis pela ANPD para infrações ao tratamento de dados pessoais:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;

[48] TOZZATO, Luiza. Vazam quase 250GB de dados bancários: saiba como se proteger. **Olhar Digital**, 22 jul. 2019.

[49] LIMA, Bruna. Falha de segurança na rede expõe dados biométricos de 1 milhão de pessoas. **Olhar Digital**, 15 ago. 2019.

[50] Art. 6º, inciso VII, da LGPD. Ver: BRASIL, 2018b, op. cit.

> [...]
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)[51]

Caso comprovada a existência do ato ilícito gerador da infração, será dado início a um processo administrativo pela ANPD. O acusado possuirá direito à ampla defesa, porém, conforme os incisos do § 1º do mesmo art. 52, exige-se que sejam considerados, em todo caso, os seguintes elementos:

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;

[51] Art. 15 da LGPD. Ver: BRASIL, 2018b, op. cit.

> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.[52]

Além de levar em conta os elementos mencionados, a ANPD deverá criar um regulamento próprio, estabelecendo critérios para a aplicação das sanções administrativas, o qual deverá ser objeto de consulta pública.

Deste modo, no caso exemplificado de vazamento dos prontuários médicos da clínica, a LGPD exige, ainda, que o ocorrido seja informado aos pacientes afetados, tendo em vista que um vazamento dessa dimensão possui alto potencial de dano ao titular.

Outrossim, uma vez definida a sanção a ser aplicada, a ANPD avaliará se a clínica adotava medidas de segurança adequadas, bem como se armazenava os dados sensíveis dos pacientes criptografados, por exemplo, dificultando, assim, a utilização e a identificação do titular em caso de vazamento.

Os pacientes lesados poderão exigir indenizações. O Código de Defesa do Consumidor estabelece que o dano causado deve ser indenizado, independente de comprovação de culpa do prestador dos serviços.

Conclui-se, então, que a adoção de medidas de segurança da informação adequadas é um elemento de suma importância, uma vez que pode servir como atenuante na aplicação da sanção pela ANPD, ainda que isso não signifique a absolvição por eventuais indenizações.

4.4 Melhores Práticas de Proteção de Dados de Saúde

Com a LGPD em vigor desde 18 de setembro de 2020, diversas empresas estão em processo de conformidade à nova lei. Para analisar as melhores práticas nesse campo, ilustra-se a situação de uma empresa fictícia, cujo modelo de negócio inclui também a comercialização de testes genéticos.

[52] Art. 52 da LGPD. Ver: BRASIL, 2018b, op. cit.

O caso supracitado revela o grau de preocupação e cautela que uma empresa deste porte deverá ter para atender às exigências da LGPD. Como articulado em tópicos anteriores, o tratamento de dados sensíveis envolve riscos superiores àqueles relacionados ao tratamento de dados pessoais gerais. O caso trata sobre a comercialização de teste genéticos e é importante pressupor que existem riscos inerentes à essa atividade, como a possibilidade de identificar predisposições e riscos de doenças e a de fornecer informações sobre os membros da família, ou seja, situações que envolvem pessoas além do indivíduo que realiza o teste[53].

Como abordado nos arts. 46 e seguintes da LGPD, capítulo dedicado a segurança e boas práticas, um dos objetivos de normas de segurança e sigilo ou anonimização é a proteção de dados pessoais contra acessos não autorizados e, ainda, contra situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado.[54].

Ocorre que as normas de segurança da informação não trazem padrões específicos que devem ser seguidos, e nem poderia, se considerar que a lei deve ser atemporal e novas tecnologias surgem a cada dia. O papel de regulamentar a lei, ou seja, estabelecer as regras do jogo, será da ANPD em conjunto à participação ativa dos entes regulados.

Dessa forma, hoje, a recomendação das melhores práticas para o tratamento de dados genéticos conforme o caso supracitado seria com base nas regras e princípios de proteção de dados, assim como em opiniões irradiadas no plano internacional sobre o referido tema.

Nesse diapasão, sugere-se medidas de boas práticas de segurança que podem ser recomendadas à empresa em tela, ou seja, sob a ótica do tratamento de dados genéticos.

A primeira delas diz respeito à anonimização de dados, que é o processo pelo qual os dados não mais permitem identificar o titular a quem originalmente diziam respeito. Esse processo envolve técnicas complexas, mas traz mais segurança para o consumidor, além de abrir outras possibilidades de uso dos dados, tendo em vista que dados anonimizados não permitem a identificação, direta ou indireta, do titular dos dados.

---

[53] FUTURE OF PRIVACY FORUM (FPF). **Privacy Best Practices for Consumer Genetic Testing Services**. Washington, jul. 2018.

[54] Art. 46 e seguintes da LGPD. Ver: BRASIL, 2018b, op. cit.

Como segunda medida sugerida, o consentimento do titular do dado, conforme abordado previamente, deve ser logrado a partir de uma manifestação livre, informada e inequívoca, deixando claro para o titular a finalidade determinada do tratamento de seus dados pessoais. É importante ressaltar, ainda, que, em se tratando de dados genéticos, caso a empresa venha a utilizar esses dados para outras finalidades, torna-se indispensável a obtenção de novo consentimento para as novas finalidades específicas.

É recomendável também, como terceira medida, a aplicação de políticas de segurança da informação adequadas, sejam elas no tocante a base de dados, criptografia ou controle de acesso, tendo em vista que dados pessoais sensíveis de saúde exigem um alto nível de segurança e confidencialidade.

Por fim, como quarta sugestão, a adoção e disponibilização da política de privacidade é medida que se impõe, devendo ser observadas clareza e objetividade por ocasião da redação do documento, por exemplo, evitando-se termos técnicos para que as informações sobre o tratamento de dados pessoais sejam compreendidas pelo titular dos dados.

CONCLUSÃO

Em tempos de crise, como a vivenciada neste ano de 2020, com a atual pandemia ocasionada pelo vírus Covid-19, os dados pessoais são elementos que ganham destaque. Além do aumento pela procura de serviços virtuais, os dados pessoais são essenciais para executar políticas públicas de contenção e controle do vírus, bem como para tornar possibilitar que a pesquisa científica proporcione os melhores resultados possíveis em curto prazo[55].

Neste trabalho foram especificadas, por meio de uma abordagem teórica e mediante a análise de situações-problema, como o setor da saúde poderá ser afetado pela nova legislação, a Lei Geral de Proteção de Dados (LGPD).

[55] DONEDA, Danilo. **A proteção de dados em tempos de coronavírus**. 26 mar. 2020.

Primeiro, depreende-se que, apesar da sensibilidade inerente dos dados de saúde, o setor carece de regras claras de proteção de dados pessoais.

Com a LGPD em vigor, tornam-se evidentes os efeitos no setor da saúde e áreas afins, como a Telemedicina. Um caso de vazamento de dados pessoais provoca, com toda a razão, a desconfiança dos titulares em relação à empresa que os deixou vazar. O uso da tecnologia traz inseguranças quanto ao sigilo das informações e, ao mesmo tempo, é um desafio técnico e organizacional para as empresas que tratam um grande volume de dados pessoais e que precisarão se adequar à nova legislação[56].

A LGPD dispõe de recursos apropriados para atender às demandas decorrentes da pandemia por qual passamos, por isso foi tão importante a entrada em vigor da Lei. Para mais, por certo será também um elemento fundamental para a reestruturação do País no cenário de pós-pandemia.

Ainda, espera-se que a Telemedicina, em se tratando de uma plataforma integradora, interessante e importante, possa ser implementada principalmente com o intuito de promover a democratização do acesso à saúde.

Será que, após o exposto, pode-se imaginar que a regulação da Telemedicina evitaria desperdícios, diante de um direcionamento mais claro para a realização de consultas e procedimentos? Será que o acesso aos dados de saúde, bem como a integração dos sistemas, poderia trazer maior transparência e segurança aos pacientes?

A Telemedicina, devidamente regulamentada e somada a estratégias que ampliam o seu potencial, pode fortalecer e complementar os serviços de saúde. Além disso, a Telemedicina pode auxiliar a fornecer cuidados médicos a regiões inacessíveis, popularizando o acesso aos serviços de saúde, desafogando as demandas do sistema de saúde brasileiro e, ainda sim, redirecionando de forma mais efetiva as demandas do setor.

O presente artigo teve como objetivo trazer uma ampla visão quanto à importância e necessidade da proteção de dados, especialmente no âmbito da Telemedicina, no que se refere a dados pessoais sensíveis de saúde. Ainda, visou apresentar um panorama geral de como está a atual legislação vigente no País, diante da presente situação de pandemia. Por todo o exposto,

---

[56] *Id*. **O vazamento de dados pessoais na iminência de regulação**. 10 maio, 2017.

conclui-se que a LGPD é dotada de grande relevância, afinal a relação dos indivíduos em face das empresas que coletam os seus dados é de hipervulnerabilidade. Talvez esse momento de pandemia e de dificuldade seja também o momento de despertar o melhor dos seres humanos.

REFERÊNCIAS

BLOCK, Gisela. Racism and Sexism in Nazi Germany: Motherhood, Compulsory Sterilization, and the State *in* BRIDENTHAL, Renate. GROSSMAN, Atina. & KAPLAN, Marion. **When Biology Became Destiny: Women in Weimar and Nazi German**. 1984.

BRASIL. Conselho Federal de Medicina. **Resolução n. 2.227, de 13 de dezembro de 2018**. 2018a. Disponível em: <https://abmes.org.br/legislacoes/detalhe/2694>. Acesso em: 8 jul. 2020.

_____. Conselho Federal de Medicina. **Resolução nº 1.643/2002, de 26 de agosto de 2002**. 2002. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643>. Acesso em: 8 jul. 2020.

_____. Conselho Federal de Medicina. **Ofício n. 1.756/2020**, de 19 de março de 2020. 2020a. Disponível em: <https://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf>. Acesso em: 8 jul. 2020.

_____. Conselho Regional de Medicina do Estado do Mato Grosso. **Resolução n. 2, de 24 de março de 2020**. Dispõe sobre a assistência médica a partir de ferramentas de telemedicina e telessaúde, com base no Decreto Federal de Estado de Calamidade Pública, importando epidemias onde as orientações médicas incluem quarentena, isolamento e distanciamento social extenso. 2020b. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-n-2-de-24-de-marco-de-2020-249806129>. Acesso em: 8 jul. 2020.

_____. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 13. jun. 2020.

_____. **Decreto n. 7.257, de 4 de agosto de 2010**. Regulamenta a Medida Provisória no 494 de 2 de julho de 2010, para dispor sobre o Sistema Nacional de Defesa Civil - SINDEC, sobre o reconhecimento de situação de emergência e estado de calamidade pública, sobre as transferências de recursos para ações de socorro, assistência às vítimas, restabelecimento de serviços essenciais e reconstrução nas áreas atingidas por desastre, e dá outras providências. 2010. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/Decreto/D7257.htm>. Acesso em: 5 maio, 2020.

_____. **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: 24 dez. 2020.

_____. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 nov. 2020.

_____. **Lei n. 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. 2018c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm>. Acesso em: 10 nov. 2020.

_____. Ministério da Saúde. **Portaria n. 467, de 20 de março de 2020**. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. 2020c. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996>. Acesso em: 30 ago. 2020.

_____. Ministério da Saúde. **TeleSUS**. 2020. Disponível em: <https://aps.saude.gov.br/ape/corona/telesus>. Acesso em: 24 dez. 2020.

_____. Presidência da República. Despacho do Presidência da República. **Mensagem n. 93, de 18 de março de 2020**. 2020d. Disponível em: <http://www.in.gov.br/en/web/dou/-/despacho-do-presidente-da-republica-248641738>. Acesso em: 5 jul. 2020.

_____. Sergipe. Secretaria de Estado da Saúde. **SUS tem papel fundamental durante a pandemia**. 19 set. 2020. Disponível em: <https://www.saude.se.gov.br/sus-tem-papel-fundamental-durante-a-pandemia/>. Acesso em: 23 dez. 2020.

_____. Superior Tribunal de Justiça. Habeas Corpus: HC 315220 RS. Relatora Ministra Maria Thereza de Assis Moura. Sexta Turma. DJe 9/10/2015. **STJ**, 2015.

CAREY, Sabine C. GIBNEY, Mark. & POE, Steven C. **The Politics of Human Rights: The Quest for Dignity**, 2010.

CAROLAN, Eoin. The continuing problems with online consent under the Eus emerging data protection principles. **Computer Law and Security Review**. V. 32. Ed. 3, jun. 2016.

CUKIER, Kenneth. MAYER-SCHONBERGER, Viktor. **BIG DATA**. New York, 2014.

DIAS, Rodrigo dos Santos. BORTMAN, Roberto. ZANGARINO JÚNIOR, Sérgio. O Código de Defesa do Consumidor e sua Aplicação às Healthtechs. **UNISANTA Law and Social Science**, v. 7, n. 3, p. 605-620, 2018.

DONEDA, Danilo. **A proteção de dados em tempos de coronavírus**. 26 mar. 2020. Disponível em: <http://www.doneda.net/2020/03/26/a-protecao-de-dados-em-tempos-de-coronavirus/>. Acesso em: 11 nov. 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE, 2010.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **O vazamento de dados pessoais na iminência de regulação**. 10 maio, 2017. Disponível em: <http://www.doneda.net/2017/05/10/o-vazamento-de-dados-pessoais-na-iminencia-de-regulacao/>. Acesso em: 9 nov. 2020.

FUTURE OF PRIVACY FORUM (FPF). **Privacy Best Practices for Consumer Genetic Testing Services**. Washington, jul. 2018. Disponível em: < https://fpf.org/2018/07/31/privacy-best-practices-for-consumer-genetic-testing-services/> Acesso em: 22 nov. 2020.

G1. Brasil tem 904 casos confirmados de novo coronavírus, diz ministério. **G1**, 20 mar. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/03/20/brasil-tem-904-casos-confirmados-de-novo-coronavirus-diz-ministerio.ghtml. Acesso em: 20 maio, 2020.

KOONZ, Claudia. **Mothers in The Fatherland**: Women, the Family, and Nazi Politics, 1987.

LIMA, Bruna. Falha de segurança na rede expõe dados biométricos de 1 milhão de pessoas. **Olhar Digital**, 15 ago. 2019. Disponível em: <https://olhardigital.com.br/noticia/violacao-encontrada-no-sistema-da-biostar2-divulga-dados-biometricos/89194>. Acesso em: 10 nov. 2020.

OLIVEIRA, Pedro Ivo de. Organização Mundial da Saúde declara pandemia de coronavírus. **Agência Brasil (EBC)**, 11 mar. 2020. Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/organizacao-mundial-da-saude-declara-pandemia-de-coronavirus>. Acesso em 05 de julho de 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – BRASIL (ONU-BRASIL). Organização Mundial da Saúde (OMS). **A ONU e a saúde**. Disponível em: <https://nacoesunidas.org/acao/saude/>. Acesso em: 5 jun. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comissão Interamericana de Direitos Humanos (CIDH). **Resolución n. 1/2020, de 10 abr. 2020**. Pandemia y Derechos Humanos en las Américas. Disponível em: <https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>. Acesso em: 15 out. 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. 1 ed. Rio de Janeiro: Renovar, 2008.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

SILVA, Marco Antônio Medeiros e. Penalidades aplicadas pelos Conselhos de medicina. **Conselho Regional de Medicina do Distrito Federal (CRM-DF)**. Disponível em: <http://www.crmdf.org.br/index.php?option=com_content&view=article&id=21592:das-penalidades-aplicadas-pelos-conselhos-de-medicina&catid=3>. Acesso em: 30 ago. 2020.

SILVA, Welison Matheus Fontes da. RUIZ, Jefferson Lee de Souza. A centralidade do SUS na pandemia do coronavírus e as disputas com o projeto neoliberal. **Physis: Revista de Saúde Coletiva**. v. 30 n. 3. Rio de Janeiro, set. 2020. Disponível em: < https://www.scielo.br/scielo.php?pid=S0103-73312020000300301&script=sci_arttext>. Acesso em: 24 dez. 2020.

TOZZATO, Luiza. Vazam quase 250GB de dados bancários: saiba como se proteger. **Olhar Digital**, 22 jul. 2019. Disponível em: <https://olhardigital.com.br/noticia/vazam-quase-250-gb-de-dados-bancarios-saiba-como-se-proteger/88263>. Acesso em: 10 nov. 2020.

UNIÃO EUROPEIA (UE). **Regulation (EU) n. 2016/679**. General Data Protection Regulation (GDPR). 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN> . Acesso em: 10 nov. 2020.

WEN, Chao Lung. **Telemedicina e Telessaúde**: Inovação e Sustentabilidade. GoldBook: Inovação Tecnológica em Educação e Saúde, p. 86-104, 2011. Disponível em: <http://www.telessaude.uerj.br/resource/goldbook/pdf/5.pdf>. Acesso em: 15 out. 2020.

WIMMER, Miriam. Proteção de Dados Pessoais no Setor Público: incidência, bases legais e especificidades. **Revista do Advogado**. v. 144, p. 126-133, 2019. Disponível em: < https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/2/index.html>. Acesso em: 24 dez. 2020.

WORLD HEALTH ORGANIZATION (WHO). **Constitution of the world health organization**. 49. ed. 2020. Disponível em: <https://apps.who.int/gb/bd/pdf_files/BD_49th-en.pdf>. Acesso em: 5 jul. 2020.