Diretora de Conteúdo e Operações Editoriais
JULIANA MAYUMI ONO

Gerente de Conteúdo
MILISA CRISTINE ROMERA

Editorial: Aline Marchesi da Silva, Diego Garcia Mendonça, Karolina de Albuquerque Araújo Martino e Quenia Becker

Gerente de Conteúdo Tax: Vanessa Miranda de M. Pereira

Direitos Autorais: Viviane M. C. Carmezim

Analista de Conteúdo Editorial: Juliana Menezes Drumond

Analista de Operações Editoriais: Alana Fagundes Valério

Analista de Conteúdo Editorial Júnior: Bárbara Baraldi

Estagiárias: Ana Amalia Strojnowski, Mariane Cordeiro e Mirna Adel Nasser

Produção Editorial
Gerente de Conteúdo
ANDRÉIA R. SCHNEIDER NUNES CARVALHAES

Especialistas Editoriais: Gabriele Lais Sant'Anna dos Santos e Maria Angélica Leite

Analistas de Operações Editoriais: Caroline Vieira, Damares Regina Felício, Danielle Castro de Morais, Mariana Plastino Andrade, Mayara Macioni Pinto, Patrícia Melhado Navarra e Vanessa Mafra

Analistas de Qualidade Editorial: Ana Paula Cavalcanti, Fernanda Lessa e Victória Menezes Pereira

Estagiárias: Bianca Satie Abduch, Gabrielly N. C. Saraiva, Maria Carolina Ferreira e Sofia Mattos

Capa: Linotec

Líder de Inovações de Conteúdo para Print
CAMILLA FUREGATO DA SILVA

Equipe de Conteúdo Digital
Coordenação
MARCELLO ANTONIO MASTROROSA PEDRO

Analistas: Gabriel George Martins, Jonatan Souza, Maria Cristina Lopes Araujo e Rodrigo Araujo

Gerente de Operações e Produção Gráfica
MAURICIO ALVES MONTE

Analistas de Produção Gráfica: Aline Ferrarezi Regis e Jéssica Maria Ferreira Bueno

Assistente de Produção Gráfica: Ana Paula de Araújo Evangelista

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Compliance e Política de Proteção de Dados / Ricardo Villas Bôas Cueva, Ana Frazão, coordenação. -- São Paulo : Thomson Reuters Brasil, 2021.

Vários autores.
Bibliografia.
ISBN 978-65-5991-540-8

1. Compliance 2. Direito à privacidade 3. Direito à privacidade - Brasil 4. Programas de compliance 5. Proteção de dados - Leis e legislação 6. Proteção de dados pessoais 7. Risco - Avaliação I. Cueva, Ricardo Villas Bôas. II. Frazão, Ana.

21-88641 CDU-342.721

Índices para catálogo sistemático:
1. Compliance : Proteção de dados pessoais : Direito 342.721

Cibele Maria Dias - Bibliotecária - CRB-8/9427

ANA FRAZÃO
RICARDO VILLAS BÔAS CUEVA
COORDENAÇÃO

COMPLIANCE E POLÍTICAS DE PROTEÇÃO DE DADOS

THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

COMPLIANCE E POLÍTICAS DE PROTEÇÃO DE DADOS

ANA FRAZÃO E RICARDO VILLAS BÔAS CUEVA
Coordenação

THOMSON REUTERS BRASIL CONTEÚDO E TECNOLOGIA LTDA.

JULIANA MAYUMI ONO
Diretora Responsável

Av. Dr. Cardoso de Melo, 1855 – 13º andar – Vila Olímpia
CEP 04548-005, São Paulo, SP, Brasil

CENTRAL DE RELACIONAMENTO THOMSON REUTERS SELO REVISTA DOS TRIBUNAIS
(atendimento, em dias úteis, das 9h às 18h)
Tel. 0800-702-2433

e-mail de atendimento ao consumidor: sacrt@thomsonreuters.com

e-mail para submissão dos originais: aval.livro@thomsonreuters.com

Conheça mais sobre Thomson Reuters: www.thomsonreuters.com.br

Acesse o nosso *eComm*

www.livrariart.com.br

Impresso no Brasil [12-2021]

Profissional

Fechamento desta edição [25.10.2021]

ISBN 978-65-5991-540-8

Apresentação

É com muita alegria que apresento ao público o livro *Compliance e Políticas de Proteção de Dados*, cuja coordenação eu compartilho com o querido e admirado Ministro Ricardo Villas Bôas Cueva que, não obstante todos os compromissos profissionais, sempre encontra tempo para se dedicar a projetos editoriais da mais alta importância, como é o caso do presente.

Com efeito, o tema tratado pelo livro não poderia ser mais atual e oportuno, pois a entrada em vigor da LGPD veio acompanhada de inúmeros desafios, considerando não apenas a importância, como também o alcance e a transversalidade do regime de proteção de dados por ela instituído. Assim, tornou-se urgente densificar os aspectos principais da LGPD e oferecer aos agentes de tratamento diretrizes confiáveis para as adaptações organizacionais e comportamentais que precisarão ser feitas para a adequação à legislação.

Trata-se de esforço que está longe de ser trivial, considerando a grande heterogeneidade dos agentes de tratamento, os quais precisarão encontrar soluções para se adaptar à lei de acordo com o seu porte, a sua atividade e também o risco do tratamento de dados a que se submete. A dificuldade é maior porque a ANPD ainda não conseguiu regulamentar vários dos aspectos controversos da LGPD, o que gera desafios adicionais para a estruturação dos programas de *compliance*.

Foi da necessidade prática de encontrar caminhos para orientar a conformidade dos agentes de tratamento que surgiu a ideia do presente livro, que reuniu doutrinadores de escol para tratar dos principais temas que têm intrigado as comunidades científica e empresarial.

Ao contrário do que costuma ocorrer em livros coletivos, a presente obra não foi uma reunião aleatória de artigos. Houve uma organização cuidadosa

REFLEXÕES SOBRE *COMPLIANCE* DE DADOS PESSOAIS DOS PACIENTES E A PRESTAÇÃO DE SERVIÇOS MÉDICOS NA ERA DIGITAL

PAULA MOURA FRANCESCONI DE LEMOS PEREIRA[1]

Sumário: 1. Notas introdutórias: a prestação de serviços médicos na era digital; 2. Da proteção dos dados pessoais dos pacientes; 3. O *compliance* de dados dos pacientes e a prevenção de riscos; Considerações finais; Referências.

1. NOTAS INTRODUTÓRIAS: A PRESTAÇÃO DE SERVIÇOS MÉDICOS NA ERA DIGITAL

A sociedade contemporânea utiliza amplamente a tecnologia da informática em um crescente processo de digitalização, o que propicia uma grande circulação de dados pelas redes eletrônicas e, em especial, o uso da Internet das Coisas em diversas áreas do saber, entre elas, a Medicina.

1. Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em Advocacia Pública pela PGE-CEPED-UERJ. Especialista em Direito Médico pela Universidade de Coimbra-PT. Professora do Instituto de Direito da PUC-Rio. Membro da Comissão da OAB-RJ de Direito Civil e de Órfãos e Sucessões. Coordenadora Adjunta de Direito Civil da ESA-RJ. Advogada. E-mail: paula@francesconilemos.com.br, Lattes: http://lattes.cnpq.br/5276030017603037.

Na era digital a relação médico-paciente é fortemente afetada, o que acarreta um grande impacto na esfera de alguns direitos humanos fundamentais, entre os quais, o direito à proteção de dados pessoais e sensíveis dos pacientes. Isso porque os dados sensíveis, em especial os dados de saúde, estão mais expostos, mais vulneráveis à ocorrência de incidentes com as diversas formas de circulação (ex. nuvem), além de integrar o *Big Data*.

Na área da saúde, o avanço da inteligência artificial, as novas ferramentas tecnológicas de comunicação e biotecnológicas oferecem aos médicos diversos meios para melhor atender seus pacientes, principalmente com a Internet, o uso de aplicativos, *software*, mídias sociais, *sites*, flexibilizando todas as barreiras geográficas, otimizando o tempo e garantindo maior acesso à população. Além disso, existem novos tratamentos, dispositivos médicos e equipamentos que utilizam a inteligência artificial,[2] algoritmos que se alimentam de dados pessoais sensíveis dos pacientes, contribuindo para facilitar tanto a atuação dos profissionais de saúde quanto o cuidado com os pacientes.

Os avanços na informática conferem maior facilidade no acesso às informações dos dados de saúde, científicos, de pesquisas e inovações tecnológicas, e permitem a troca de informações com outros médicos à distância (teleinterconsulta) e o envio de dados do paciente, até mesmo, em grande volume. Isso facilita a identificação de doenças, o diagnóstico por meio de recursos mais velozes e eficazes, e uma maior socialização dos dados médicos.

Todavia, surgem algumas indagações: como garantir que o acesso às informações de saúde, dados pessoais sensíveis dos pacientes veiculados na Internet, em aplicativos, e outros veículos de comunicação ocorra de maneira segura? Como compatibilizar a circulação de imagens, exames, atestados, prescrição médica, prontuário, dados clínicos do paciente sem causar lesão à intimidade, à privacidade, à confidencialidade e ao sigilo desses dados sensíveis? Quais são os deveres dos médicos diante dessa nova realidade tecnológica, do uso da inteligência artificial no que diz respeito ao tratamento dos dados sensíveis dos pacientes?

Esses questionamentos estão relacionados com a nova forma de prestação de serviços médicos, inclusive, com o aumento da prática da medicina, da

2. Para um aprofundamento a respeito da inteligência artificial na saúde e a importância do estabelecimento de guias de boas práticas, cabe citar o artigo: PEREIRA, Paula Moura Francesconi de Lemos; SCHULMAN, Gabriel. Futuro da saúde e saúde do futuro: impactos e limites reais da inteligência artificial. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Org.). *O Direito Civil na era da Inteligência Artificial*. São Paulo: Thomson Reuters, 2020, p. 165-182.

terapia *on-line* e das consultas médicas à distância (telemedicina), que se desenvolveram de forma mais célere com a pandemia da Covid-19, declarada pela Organização Mundial de Saúde (OMS).[3]

O uso da informática no campo da Medicina, da Biomedicina e nos serviços de saúde, apesar de considerado, hoje, indispensável, pode acarretar diversos riscos e danos aos pacientes, tais como os danos decorrentes da violação de seus dados pessoais e sensíveis, que podem ser de ordem patrimonial ou extrapatrimonial. Esses danos são causados diretamente à personalidade do paciente, ao seu direito à saúde, à igualdade, à não discriminação e à liberdade.

A Constituição Federal (art. 5º, incisos X e LXXII) assegura, mesmo que de forma implícita[4] e, em breve, expressa, a proteção dos dados pessoais,[5] juntamente com algumas normas infraconstitucionais,[6] ganhando relevo a Lei Geral

3. Portaria nº 188, de 3 de fevereiro de 2020 – Declara Emergência em Saúde Pública de importância Nacional (ESPIN) em decorrência da Infecção Humana pelo novo Coronavírus (2019-nCoV). Disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-188-de-3-de-fevereiro-de-2020-241408388. Acesso em: 25 mai. 2021.
Decreto nº 46.973, de 16 de março de 2020: Reconhece a situação de emergência na saúde pública do estado do Rio de Janeiro em razão do contágio e adota medidas para enfrentamento da propagação decorrente do novo coronavírus (Covid-19); e dá outras providências. Disponível em: https://pge.rj.gov.br/comum/code/MostrarArquivo.php?C=MTAyMjI%2C. Acesso em: 25 mai. 2021.
Lei nº 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: https://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735. Acesso em: 27 mai. 2021.

4. No tocante à natureza do direito à proteção de dados, merece leitura o artigo: SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo (et al.). *Tratado de proteção de dados pessoais*. 2. reimp. Rio de Janeiro: Forense, 2021, p. 21-59.

5. No dia 20/10/2021 foi aprovada no Senado Federal a Proposta de Emenda à Constituição nº 17/2019, que torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental previsto na Constituição, agora o texto segue para promulgação, em sessão do Congresso Nacional, ainda a ser marcada. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao. Acesso em: 08 nov. 2021.

6. Código de Defesa do Consumidor (nº 8.078/1990), Código Civil (nº 10.406/2002), Lei de Interceptação Telefônica e Telemática (nº 9.296/1996), Lei Geral de Telecomunicações (nº 9.472/1997), Lei Complementar sobre o sigilo das operações de instituições financeiras (nº 105/2001), Lei do *Habeas Data* (nº 9.507/1997), Lei nº 12.414/2011, que disciplinou o cadastro positivo, Marco Civil da Internet (Lei nº 12.965/2014), Lei de Acesso à Informação (nº 12.527/2011), entre outras.

de Proteção de Dados – LGPD, Lei nº 13.709/2018.[7] Essa lei sistematiza e apresenta elementos, princípios próprios, bases legais para regular as atividades, públicas e privadas, que tratam de dados pessoais, interferindo em várias áreas de atuação da sociedade, que passa a incorporar seus valores, com reflexo direto na adoção de novas medidas, novas políticas necessárias para a readaptação ao perfil da regulação protetiva dos dados.[8]

O médico, pela interpretação da LGPD, pode ser enquadrado como agente de tratamento de dados,[9] seja na posição de controlador[10] ou de operador de dados[11]

7. A LGPD recebeu forte influência do direito comunitário europeu, desde a Diretiva de Proteção de Dados de 1995 até o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor a partir de maio de 2018.
8. Cf. DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (et al.). Tratado de proteção de dados pessoais. 2. reimp. Rio de Janeiro: Forense, 2021, p. 03-20.
9. Em 28 de maio de 2021, a Autoridade Nacional de Proteção de Dados – ANPD publicou o Guia Orientativo para a Definição dos Agentes de Tratamento e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf Acesso em: 31 maio 2021.
10. "Daí decorre que não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD. [...] Uma pessoa natural poderá ser controladora nas situações em que é a responsável pelas principais decisões referentes ao tratamento de dados pessoais. Nessa hipótese, a pessoa natural age de forma independente e em nome próprio – e não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta. 31. É o que ocorre, por exemplo, com os empresários individuais, os profissionais liberais (como advogados, contadores e médicos) e os responsáveis pelas serventias extrajudiciais." Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/ 2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 31 maio 2021.
11. "O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. [...] Cabe destacar, ainda, algumas das obrigações do operador: (i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador." Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/ 2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 31 maio 2021.

(arts. 5º, VI, VII e IX; e 39, LGPD),[12] já que realiza a operação de dados pessoais dos pacientes, inclusive de dados sensíveis (art. 5º, I e II, LGPD), em qualquer de suas etapas previstas no art. 5º, X, LGPD:

> coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A interdisciplinaridade da Informática, da Medicina e do Direito acaba por atrair a aplicação de normas jurídicas, éticas, técnicas e administrativas, que permitem um diálogo entre a regulação legal e a autorregulamentação, a exemplo dos Códigos Deontológicos e de outras Resoluções do Conselho Federal de Medicina – CFM, Conselhos Regionais de Medicina – CRMs, caminhando para o que hoje se chama de corregulação.[13] Esse conjunto de normas vai cooperar com o arcabouço legislativo já concebido pelo Direito para regular as relações privadas afetadas pelas novas tecnologias.

Caberá aos operadores do Direito, em um diálogo multidisciplinar, guiados pelo pluralismo e pela cientificidade, estudar os instrumentos necessários

12. "Para essa análise, é fundamental verificar o âmbito do tratamento. Quando o tratamento é restrito a um profissional pessoa física – como uma médica profissional liberal atendendo seus pacientes ou um contador autônomo prestando serviços a seus clientes –, então essa pessoa física será enquadrada como 'controladora' ou 'operadora' desses dados pessoais. Nos exemplos citados, a médica seria definida como controladora e o contador, como operador dos dados pessoais, conforme parâmetros definidos ao longo deste texto." Disponível em: https://www.migalhas.com.br/depeso/326741/descomplicando--agentes-de-tratamento. Acesso em: 29 maio 2021.
13. FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. "Sobre o assunto, não é demais lembrar as lições de Diane Rowland, Uta Kohl e Andrew Charlesworth de que o problema da regulação, especialmente no ambiente digital, não é, na prática, uma escolha rígida entre o modelo 'comando-controle' e a autorregulação, até porque os dois não são polos extremos que se excluem mutuamente. Daí a discussão atual sobre um terceiro gênero – o da corregulação – que combinaria diferentes categorias de práticas regulatórias e exigiria o envolvimento central dos agentes privados e dos governos, a fim de propiciar muitas vantagens da autorregulação sem as mesmas desvantagens". *Compliance* de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 685.

para garantir maior proteção e segurança dos dados pessoais e sensíveis dos pacientes, considerados consumidores[14] com vulnerabilidade potencializada (arts. 5º, XXXII, e 170, V, ambos da CF; arts. 2º, 17, e 29, todos do Código de Defesa do Consumidor – CDC).

Torna-se, portanto, indispensável, para além da obtenção do consentimento livre e esclarecido para legitimar o ato médico, a autorização para o tratamento dos dados do paciente, ressalvadas as exceções legais;[15] a adoção de medidas de segurança, de boas práticas, de governança, de um sistema de gestão de *compliance*.[16] Para isso, os médicos devem valer-se de alguns instrumentos para garantir a proteção quanto aos apurados riscos atrelados à violação de privacidade de dados, ao sigilo, à confidencialidade dos dados sensíveis e à imagem dos pacientes, que circulam nas redes, em observância à LGPD.

O objetivo do presente artigo é, diante da nova realidade tecnológica da atuação dos médicos, profissionais liberais e pequenos empresários, que são controladores de dados pessoais, traçar algumas medidas que precisam ser implementadas de forma a salvaguardar os interesses dos pacientes.[17] Tudo com foco na proteção de dados pessoais e sensíveis dos pacientes, calcada nos princípios da dignidade humana (art. 1º, inciso III, da CF), do livre desenvolvimento

14. A relação médico-paciente é considerada de consumo pela maioria da doutrina e jurisprudência pátria, apesar das críticas feitas à aplicação do Código de Defesa do Consumidor a esta relação. Nesse sentido: SOUZA, Eduardo Nunes de. *Do Erro à culpa*: Na responsabilidade civil do médico. Rio de Janeiro: Renovar, 2015. p. 95-96.

15. Cita-se como exemplo de uma exceção a permissão de acesso à base de dados sensíveis de saúde a realização de estudos em saúde pública (art. 13, LGPD).

16. A respeito do tema: SAAVEDRA, Giovani Agostini. *Compliance* de dados. In: DONEDA, Danilo (et al.). Tratado de proteção de dados pessoais. [2. reimp.]. Rio de Janeiro: Forense, 2021, p. 727-741.

17. Cabe ressaltar que, em outubro de 2021, a ANPD, em observância ao disposto no art. 55-J, XVIII da LGPD, publicou o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, bem como um checklist. A ANPD considera agentes de pequeno porte as microempresas e empresas de pequeno porte (sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário), bem como as iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, além de outras categorias de organizações. O objetivo do guia é proteger os dados pessoais sob a guarda dos agentes de pequeno porte, no qual é possível enquadrar os médicos que utilizam estruturas de pequeno porte para o exercício de suas atividades. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdfhttps://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf. Acesso em: 08 nov. 2021.

da personalidade, da igualdade, da não discriminação, da liberdade, da autonomia informacional, da privacidade e da intimidade.

2. Da proteção dos dados pessoais dos pacientes

O médico pode exercer sua atividade de diversas formas e por diferentes vínculos, seja como empregado de instituição hospitalar/clínica; servidor público; militar; sócio de sociedade; profissional liberal; empresário individual; constituir empresa de responsabilidade limitada; sociedade unipessoal, entre outras. Essas posições ocupadas pelo médico podem interferir em sua qualificação como agente de tratamento de dados, seja no papel de controlador, seja no de operador, ou, até mesmo, se ele não se enquadrar como agente.[18]

Em todas as formas de atuação, o profissional médico mantém os seus direitos e deveres decorrentes da relação médico-paciente, que constituem uma via de mão dupla, pautados no princípio da confiança e da boa-fé objetiva. Ganham destaque os deveres do médico de cuidado, de assistência, de informar, de sigilo e de confidencialidade (Capítulo I, IX, XI, art. 34, CEM)[19] e, hoje, com destaque para o dever de proteção dos dados dos pacientes (art. 17, LGPD), este

18. "A seguir, alguns exemplos que demonstram quem pode assumir o papel de controlador a depender do cenário. Exemplo 1 – Médica profissional liberal. Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. A médica, pessoa natural, é a controladora dos dados pessoais. Exemplo 2 – Médica empregada de um hospital. Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes. O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese. A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento". Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 31 maio 2021.

19. "O caráter existencial da relação médico-paciente faz nascer diversos direitos e deveres tanto para o médico quanto para o paciente (direito do paciente ao sigilo, à recusa do tratamento médico, direito à informação e de não ser informado, seu dever de informar ao médico, o dever do médico de informar, de manter sigilo, de se abster, de dar cuidado, de não agir de forma abusiva, o direito do médico de exercer sua autonomia, entre outros). Esses direitos ganham especial proteção por se tratar da saúde, da vida humana, do poder de autodeterminação do paciente, sua autonomia privada, suas escolhas em relação à disposição de seu próprio corpo". In: PEREIRA, Paula Moura Francesconi de Lemos. *Relação médico-paciente*: o respeito à autonomia do

último quando atua como agente de tratamento de dados, entre outros deveres. E o direito do médico de exercer de forma autônoma sua atividade (Resolução nº 2.217/2018, capítulo I, inciso VII, VIII, XVI – Código de Ética Médica). Da mesma forma, o paciente também tem deveres que decorrem do autocuidado, como o dever de observar as prescrições médicas; e no que diz respeito aos seus dados pessoais, o de evitar incidentes com maior guarda e segurança dos dados, não compartilhando senhas, não entrando em *links* desconhecidos, além de verificar determinadas fontes em busca de vazamento dos dados.

A inobservância pelo médico desses deveres pode acarretar responsabilidade (arts. 186 e 927 do CC, art. 14, parágrafo 4º, do CDC, arts. 42, 43, 44, LGPD[20-21]) pelos danos patrimoniais ou extrapatrimoniais causados ao paciente em várias esferas (integridade psicofísica, personalidade, privacidade, liberdade etc.), a despeito da responsabilidade ético-disciplinar que será apurada por seu órgão de classe (Resolução CFM nº 2.145/2016, Capítulo II, XIX, XX, CEM), aplicação de sanções administrativas, entre elas, a publicização da infração após devidamente apurada e confirmada sua ocorrência, a proibição parcial ou total do exercício de atividades relacionadas de dados[22] (art. 12, Lei nº 12.965/2014,

paciente e a responsabilidade civil do médico pelo dever de informar. Rio De Janeiro: Lumen Juris, 2011. v. 1. 304p.

20. Cf. FILHO, Eduardo Tomasevicius. *Responsabilidade civil na LGPD na área da saúde*. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). LGPD na Saúde [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

21. A responsabilidade do médico, profissional liberal, à luz da LGPD deve ser subjetiva, já que a relação médico-paciente é considerada relação de consumo pela maioria da doutrina e jurisprudência. Logo, é possível interpretar o disposto no art. 45 da LGPD com o art. 14, parágrafo 4º, do CDC. No entanto, essa interpretação não tem sido feita, cabendo trazer à baila um posicionamento mais amplo quanto à aplicação do regime objetivo de responsabilidade civil na LGPD. "Quanto à responsabilidade civil, a despeito de parte da doutrina sinalizar pela adoção de regime de responsabilidade subjetiva decorrente da inobservância de deveres expressamente tratados na lei, parece preponderar a constatação de que a responsabilidade civil trabalhada pela LGPD é de natureza objetiva e contempla o risco como núcleo essencial para a delimitação de critérios próprios de imputação advindos da violação dos deveres estabelecidos pela legislação protetiva, e que podem sofrer, ainda, a incidência dos efeitos da existência de eventuais políticas de governança e programas de integridade." MARTINS, G. M.; FALEIROS JUNIOR, J. *Compliance* digital e responsabilidade civil na Lei Geral de Proteção de Dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (org.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 263-297.

22. A ANDP publicou a Resolução CD/ANPD nº 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo

art. 52, 55-J, IV, LGPD), e a responsabilidade criminal (ex. crime de inviolabilidade dos segredos, tipificados no art. 153, 154 e 325 do Código Penal).

A dinâmica da relação médico-paciente vem sofrendo ao longo dos anos profundas mudanças decorrentes de novos paradigmas que afastam o perfil autoritário-vertical para um perfil dialógico-horizontal, ao mesmo tempo em que ocorre a massificação do serviço, e o crescimento acelerado da tecnologia, da biotecnologia, que implica no surgimento de situações jurídicas, com formatos de prestação de serviços diversos, trazendo novos desafios. As novas situações jurídicas, os novos métodos de atendimento médico decorrentes do progresso científico e tecnológico, não subtraem os deveres já inerentes, ao revés, acabam por trazer novos ônus para os profissionais médicos, que, embora se beneficiem da celeridade no atendimento; do maior acesso à informação, do auxílio no tratamento e diagnóstico, criam riscos e outras hipóteses de danos causados a bens jurídicos merecedores de tutela, tais como os dados pessoais.

Nesse contexto, dá-se ênfase aos dados pessoais dos pacientes, chamados de dados sensíveis, definidos pela LGPD como: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]" (art. 5º, II), e cuja proteção constitui direitos humanos[23] fundamentais de natureza[24] existencial, embora reflitam potencial valor econômico, mas cuja fruição encontra limite legal (art. 11, parágrafo 4º, LGPD).[25]

Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 09 nov. 2021.

23. A Carta dos Direitos Fundamentais da União Europeia no art. 8º prevê expressamente o direito à proteção de dados: "Artigo 8º – Protecção de dados pessoais – 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

24. "Portanto, a opção legislativa, manifestada no *caput* do art. 17 da LGPD, de tratar a pessoa física a quem os dados se vinculam como seu titular, denota a intenção de refletir que o exercício do direito ali descrito se dará de modo direto e imediato, empregando-se termo que corresponde ao gênero do qual a propriedade é espécie. Tal passagem da lei evidencia, ainda, a preocupação em demonstrar que a tutela ali conferida tem dupla natureza, restando contemplados os aspectos patrimoniais decorrentes

Os dados dos pacientes são de diversos conteúdos, desde os pessoais, atinentes a sua qualificação (art. 5°, I, LGPD),[26] até dados de saúde, de vida sexual, genéticos, biométricos e que são considerados dados sensíveis. O dado sensível, ao mesmo tempo em que representa a extensão da personalidade da pessoa e é fundamental para a construção de sua identidade, e integra sua vida privada (art. 21 do Código Civil), possui um alto nível discriminatório,[27] que pode afetar em vários setores da vida pessoal e social (dificuldade de contratação para emprego, seguro etc.), o que fez com que o ordenamento jurídico dispensasse um tratamento especial (arts. 5°, II, e 11, da LGPD).[28]

É de grande importância a proteção das informações sobre o paciente, o que atrai maior atenção quanto aos veículos utilizados pelos profissionais médicos

da disposição dos dados – atribuída ao seu titular – e os extrapatrimoniais. Portanto, o referido dispositivo legal serve de exemplo da constatação, por parte do legislador, de que a distinção mais relevante para o direito civil, hoje, não é a que aparta direitos reais e obrigações, mas sim as que separam as relações jurídicas absolutas das relativas e as patrimoniais daquelas extrapatrimoniais". MAIA, Roberta Mauro Medina. A titularidade de dados pessoais, prevista no art. 17 da LGPD: direito real ou pessoal? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato Oliva (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 153.

25. A respeito do valor econômico atribuído aos dados: PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: Interpretação do artigo 11, § 4°, da LGPD. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

26. "Portanto, podemos classificar os dados, de acordo com a LGPD, da seguinte forma: Dados pessoais diretos: identifica diretamente uma pessoa natural, sem a necessidade de outras informações, como CPF, título eleitoral, nome (se não houver homônimos)". VAINZOF, Rony. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD*: Lei Geral de Proteção de Dados Pessoais comentada. 3. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021, p. 96.

27. Stefano Rodotà, ao tratar de dados sensíveis, traz um exemplo de tratamento discriminatório em razão do uso indevido de dados pessoal sensível: "não há dúvida de que o conhecimento, por parte do empregador ou de companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado." A vida na sociedade de vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 70.

28. Cf. MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitlin (org.). *LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago Editorial, 2020, v. 1, p. 121-156.

para coleta, armazenamento, transmissão dos dados para o próprio paciente, para terceiros e para outros profissionais. Por isso, nessa seara, para além de toda a normativa já existente que regula a atividade médica; das leis como a que dispõe sobre o exercício da Medicina, Lei n° 12.842/2013; o Código de Defesa do Consumidor; e normas éticas, aplica-se a Lei Geral de Proteção de Dados, que traz novos contornos de proteção e que vão além dos deveres já existentes de sigilo e confidencialidade dos dados dos pacientes. Deve-se, portanto, melhor compreender os dados pessoais envolvidos, as normativas éticas e jurídicas aplicáveis de forma a garantir os direitos em relação à proteção, à confidencialidade, à privacidade e ao sigilo dos dados dos pacientes. Novos cuidados devem ser tomados a fim de proteger a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a intimidade, a honra e a imagem; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2° da LGPD). Devem-se observar os princípios e bases legais expressamente previstos na LGPD como o da finalidade e seus corolários, o da adequação, da necessidade, da garantia do acesso e controle do titular de dados, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização (art. 6°) e as bases legais, tal como a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (arts. 7°, VII e VIII, e 11, II, "e" e "f", LGPD).

As informações acerca de dados clínicos dos pacientes podem circular por diversos meios, físico ou eletrônico, na forma de: i) cadastros, prontuários físicos e eletrônicos,[29] marcação de consultas, fichas médicas, prescrição, receita,

29. No Brasil ainda não foi implantado um prontuário único para o paciente com acesso geral, mas no âmbito público há o RES. "O conceito mais básico a esse respeito é o de Registro Eletrônico em Saúde (RES). Trata-se de um repositório de informação referente à saúde de um ou mais indivíduos, processável por meios informáticos, transmitida com segurança para um conjunto de múltiplos usuários. Caracteriza-o, também, a estruturação lógica da informação. Em outros termos, pode ser definido como uma 'coleção longitudinal de informações eletrônicas sobre a saúde de pacientes individuais e populações'; o conceito cobre tanto a noção paradigmática de uma 'construção de amplo espectro, transinstitucional e, até mesmo, nacional', quanto estruturas mais fragmentadas, distribuídas e menos formais". COSTA, José Augusto Fontoura. Tratamento de dados de saúde na LGPD: Obrigações, limites e responsabilidade dos agentes. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

exames, atestados médicos; ii) envio por e-mail, troca de mensagens do médico com o próprio paciente ou com outros profissionais de saúde e terceiros fornecedores de produtos e serviços atrelados ao atendimento médico, tais como farmácias[30] e planos de saúde; além do iii) armazenamento dessas informações. Esses documentos, por conterem dados considerados sensíveis, impõem um maior controle, pois dizem respeito diretamente à privacidade e à intimidade do paciente, ao sigilo profissional das informações e à confidencialidade, aumentando a responsabilidade daqueles que utilizam e realizam o tratamento dos dados, como as clínicas, laboratórios, planos de saúde, os próprios médicos e os outros agentes que tratam dados.

Entre os diversos meios de circulação de dados dos pacientes, ganha destaque o prontuário. Mas o que seria o prontuário? Quais são as normas já existentes que traduzem sua importância e mecanismos de proteção dos dados dos pacientes neles contidos?

O prontuário do paciente é definido pela Resolução CFM nº 1.638/2002, como:

> o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo.

A Resolução nº 1.821/2007 do CFM, modificada pela Resolução nº 2.218/2018 do CFM, estabeleceu normas técnicas para elaboração, guarda e manuseio dos documentos que instruem o prontuário eletrônico, permitindo, inclusive, que se elimine o papel e a troca de informação, mas ressalvando a necessidade de que a prescrição no prontuário seja feita diariamente. E, para

30. Devem-se observar as restrições éticas referentes à prestação de serviços médicos, atrelada a parcerias com outros prestadores de serviços, cabendo citar as proibições previstas no Código de Ética Médica:
"Art. 68 Exercer a profissão com interação ou dependência de farmácia, indústria farmacêutica, óptica ou qualquer organização destinada à fabricação, manipulação, promoção ou comercialização de produtos de prescrição médica, qualquer que seja sua natureza.
Art. 69 Exercer simultaneamente a medicina e a farmácia ou obter vantagem pelo encaminhamento de procedimentos, pela prescrição e/ou comercialização de medicamentos, órteses, próteses ou implantes de qualquer natureza, cuja compra decorra de influência direta em virtude de sua atividade profissional."

segurança dos prontuários eletrônicos, deve-se observar o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, as normas de digitalização e prévia análise da Comissão de Revisão de Prontuários e as normas da Comissão de Avaliação de Documentos da unidade médico-hospitalar geradora do arquivo (arts. 1º e 2º).

Os prontuários ficam sob os cuidados do médico ou da instituição em que o paciente é assistido, como clínicas, hospitais, prontos-socorros, sanatórios, casas de saúde, laboratórios e empresas que prestam serviços médico-hospitalares, devidamente registradas (art. 87, §2º, do CEM), enquadráveis como controladores de dados (arts. 5º, VI, 37, LGPD). Esses agentes estão sujeitos não só às normas previstas no Código de Ética Médica (inciso I e II do preâmbulo), na Res. CFM nº 1.642/2002 (art. 1º), mas também à LGPD. Devem, portanto, observar todos os princípios legitimadores do tratamento de dados, a política de segurança e instrumentos estabelecidos na LGPD (art. 11, parágrafo primeiro), juntamente com a legislação própria. Em 27 de dezembro de 2018 foi publicada a Lei nº 13.787, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente, que deve ocorrer de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital (arts. 1º e 2º), e que se soma ao emaranhado de normas aplicáveis à relação médico-paciente.

Os dados contidos nos prontuários são exclusivamente do paciente e considerados sensíveis por englobar dados de saúde e genéticos (art. 5º, II, LGPD), pelo que a ele deve-se assegurar total acesso (art. 88 do CEM, arts. 6º, IV, e 9º, LGPD); garantir a possibilidade de retificação (art. 18, III, LGPD), sendo restritas as formas de divulgação e transmissão para terceiros (arts. 77, 85, CEM). E, mesmo que o prontuário esteja na forma de papel ou em meio eletrônico, devem ser assegurados o sigilo profissional e a privacidade do paciente, que configuram direito personalíssimo do paciente e dever do médico, calcado na confiança que surge na relação médico-paciente somado aos mecanismos de proteção legal.

O paciente tem o direito de que seus informes médicos sejam tratados com confidencialidade, com total sigilo profissional sobre suas condições, seus dados pessoais sensíveis, as alternativas de tratamento, com fundamento nos princípios constitucionais da proteção da dignidade da pessoa humana, fundamento da República Federativa do Brasil (art. 1º, III, da Constituição Federal), da tutela da honra, da imagem e da intimidade e da privacidade (art. 5º, inciso X, da Constituição Federal; art. 21 do Código Civil). Esse direito não cessa, mesmo que o fato seja de conhecimento público ou que o paciente venha a óbito. No entanto, caso isso ocorra, o Conselho Federal de Medicina editou a

Recomendação nº 03/2014, indicando, nos termos do seu art. 1º, que os médicos e as instituições de saúde forneçam, quando solicitado pelo cônjuge/companheiro sobrevivente do paciente morto, e sucessivamente pelos sucessores legítimos do paciente em linha reta, ou colaterais até o quarto grau, os prontuários médicos do paciente falecido.[31]

Ao lado desse direito ao sigilo, o médico e as sociedades prestadoras de serviços médico-hospitalares têm o dever de guardar segredo acerca dos fatos dos quais teve ciência em razão de sua atividade profissional (arts. 73 a 79 do CEM), e de proteção dos dados pessoais e sensíveis do paciente, dos resultados de exames realizados com finalidade terapêutica, diagnóstica ou prognóstica e das informações contidas no prontuário, arquivo ou boletim médico (art. 19, parágrafo 1º, LGPD). Além do dever de se abster de abusos, já que a relação médico-paciente está fundada na confiança, no respeito mútuo, na discrição e na reserva.

Ao profissional da área médica é vedado liberar cópias do prontuário que estão sob sua guarda, salvo quando: i) autorizado, por escrito, pelo paciente, ou seu representante legal; ii) para atender ordem judicial; iii) para a sua própria defesa; iv) por dever legal ou justa causa; v) se houver a anuência do Conselho Regional de Medicina da jurisdição. Tudo em conformidade com o art. 89 do CEM e a Resolução nº 1.605/2000 do CFM, e que também encontra respaldo no art. 7º, VI, da LGPD.

Questão relevante diz respeito à eliminação do prontuário que guarda relação direta com o prazo durante o qual os prontuários médicos devem ser guardados.

A Lei nº 13.787/2018 assegura o prazo de 20 (vinte) anos, a partir do último registro, para guarda dos prontuários, tanto em suporte de papel quanto de forma digitalizada, salvo previsão diversa em regulamento; após esse período, poderão ser eliminados ou devolvidos aos pacientes (art. 6º). A Resolução nº 1.821/2007 do CFM, modificada pela Resolução nº 2.218/2018 do CFM, artigo 8º, também prevê o prazo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmados ou digitalizados.[32]

31. Ação Civil Pública nº 26798-86.2012.4.01.3500, movida pelo Ministério Público Federal, em trâmite na 3ª Vara Federal da Seção Judiciária do Estado de Goiás.

32. Algumas leis e normas deontológicas estabelecem prazos diversos da Lei nº 13.787/2018, como o Estatuto da Criança e do Adolescente, Lei nº 8.069/90, que, em seu artigo 10, I, estabeleceu o prazo de 18 anos para os hospitais manterem os registros das atividades desenvolvidas por meio de prontuários; e a Lei nº 9.434/97, referente à remoção de órgãos, tecidos, e partes do corpo humano para fins de transplantes e tratamento, que, em seu artigo 3º, § 1º, prevê o prazo mínimo de cinco anos para guarda de prontuários.

A LGPD define a eliminação de dados como a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado" (art. 5º, XIV, da LGPD), podendo ocorrer quando: i) alcançada sua finalidade; ii) pelo fim do tratamento; iii) por vontade do próprio titular; ou iv) por determinação da autoridade nacional. Mas a própria lei ressalva a possibilidade de sua manutenção, como no caso de cumprimento de obrigação legal (arts. 15, 16, 17, 18, VI). Em se tratando de prontuários deve-se interpretar as leis aplicáveis de forma sistemática, cabendo a observância da legislação especial e do direito do paciente, titular dos dados, merecendo diretrizes da Autoridade Nacional de Dados a respeito da matéria.

Nesse contexto, não se pode deixar de ressaltar os avanços tecnológicos e biotecnológicos que ganharam maior visibilidade nesta fase pandêmica da Covid-19, afetando diretamente a relação médico-paciente e aumentando os riscos em relação aos dados pessoais dos pacientes. Ocorre o recrudescimento da telemedicina em razão do aumento da busca por serviços à distância, do alto índice de contaminação da doença, dos riscos hospitalares, das situações de isolamento social, entre outros.[33]

A telemedicina já era utilizada na prática há muitos anos devido à dificuldade de locomoção nos grandes centros urbanos; à ausência de profissionais em determinadas localidade; à falta de tempo, somada ao crescimento das novas tecnologias de comunicação que facilitaram o contato não presencial, mesmo que de forma mais tímida no Brasil.[34] Isso porque o uso da telemedicina

33. Observa-se, também na fase da pandemia da Covid-19, a circulação e divulgação de dados de saúde das pessoas que contraíram a Covid-19 e seus familiares, já que se trata de uma doença de notificação compulsória (Lista Nacional de Notificação Compulsória contida no anexo da Portaria nº 204, de 17 de fevereiro de 2016 – item 43) e que deve ser comunicada pelos médicos (Lei nº 6.259/75 e Decreto nº 49.974-A/61). A Lei nº 13.979/2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública decorrente do coronavírus, prevê expressamente a obrigatoriedade de compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal dos dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, (art. 6º), o que também tem respaldo na Lei nº 12.527/11 (art. 31, § 1º, II, § 3º, V), e na Lei Geral de Proteção de Dados (arts. 7º, VIII, 10, 11, II, *f*). A inobservância pelo médico desse dever se enquadra no tipo penal – omissão de notificação de doença (art. 269 do Código Penal).

34. Cf. TERRA, Aline de Miranda Valverde; PEREIRA, Paula Moura Francesconi de Lemos. *Telemedicina no sistema privado de saúde:* quando a realidade se impõe. Migalhas,

foi restrito pelo CFM (art. 37 do Código de Ética Médica, art. 3º da Resolução nº 1.643/2002 do CFM), possibilitado para certas modalidades (telerradiologia regulada pela Resolução nº 2.107/2014 do CFM, e telepatologia pela Resolução nº 2.264/2019 do CFM), mas limitado para o modelo assistencial, seja pelo risco da despersonalização da relação médico-paciente, seja pela exposição do paciente, pelo comprometimento do diagnóstico, do tratamento ministrado, seja pelas instruções mal interpretadas, pelo que só era cabível em situações emergenciais, de urgência.

Um dos problemas apresentados acerca do exercício da telemedicina é a ausência de normas deontológicas uniformes, de lei, que acarretam diversas incertezas, entre elas, as modalidades cabíveis, os veículos que serão utilizados, a forma de proteção dos dados dos pacientes e que geram, para os profissionais médicos e pacientes, insegurança do ponto de vista ético e jurídico. Todavia, o vácuo legislativo por si só não afasta a legalidade da prestação de serviços médicos à distância, e, na fase de emergência pública decorrente da Covid-19, diversas resoluções, ofícios e portarias foram expedidos pelo CFM, CRMs e Ministério da Saúde, tais como a Resolução CREMERJ 305/2020;[35] o Ofício CFM nº 1756/2020 – COJUR; a Portaria nº 467/2020 – MS e a edição da Lei nº 13.989/2020, que dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2).

A prestação de serviço médico presencial ou por meio da telemedicina que lida com dados dos pacientes, coletados de forma física, analógica ou digital, deve ocorrer de maneira segura, utilizando a infraestrutura tecnológica apropriada, seguindo as normas de coleta, guarda, manuseio, transmissão de dados, diretamente relacionados à tutela dos direitos do paciente, sob pena de o médico assistente do paciente e demais envolvidos responderem de forma solidária.

Um dos grandes dilemas dos profissionais médicos é o uso de determinadas mídias sociais, seja no que diz respeito à publicidade médica,[36] ao uso de

2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/322083/telemedicina-no-sistema-privado-de-saude--quando-a-realidade-se-impoe. Acesso em: 31 maio 2021.

35. Cabe ressaltar acerca do tema a leitura: PEREIRA, Paula Moura Francesconi de Lemos. O uso da internet na prestação de serviços médicos. In: SOUZA, Allan Rocha de (et al.). *Direito digital:* direito privado e internet. 4. ed. Indaiatuba: Editora FOCO, 2021.

36. Para aprofundar sobre a publicidade médica, merece a leitura: PEREIRA, Paula Moura Francesconi de Lemos; MILDEMBERGER, C. S. Publicidade médica nas mídias sociais: proposta de um modelo contemporâneo no Brasil. In: NOGAROLI, Rafaella; NETO, Miguel Kfouri (org.). *Debates contemporâneos em direito médico e da saúde*. São Paulo: Thomson Reuters, 2020, p. 399-428, e PEREIRA, Paula Moura Francesconi de Lemos; MILDEMBERGER, C. S. Publicidade médica em tempos de pandemia do novo coronavírus. *Revista dos Tribunais*, 2020, v. 1017, p. 385-391.

imagem dos pacientes,[37] seja no tocante ao uso de plataformas, aplicativos,[38] inclusive os de comunicação[39] instantânea, como *WhatsApp* e *Telegram*.

A respeito do *WhatsApp*, esse tem sido utilizado não só entre os profissionais médicos como entre estes e os seus pacientes, já que permite um diálogo mais célere e um fácil acesso às informações. Entretanto, questiona-se acerca da segurança desse veículo quanto à possibilidade de vazamento dos dados pessoais e sensíveis dos pacientes, mesmo que as conversas sejam criptografadas, pois é possível o acesso por terceiros, encaminhamentos de mensagens de forma indevida, entre outros riscos, o que pode acarretar problemas quanto ao sigilo de dados, à confidencialidade. Além disso, há os riscos quanto ao correto diagnóstico dos casos médicos analisados à distância, erro de prescrição de condutas terapêuticas, entre outros.

37. Aos médicos é vedado expor os pacientes, exibir seus retratos em anúncios profissionais ou em assuntos médicos em qualquer meio de comunicação, incluindo as redes, como se depreende do disposto no art. 75 do Código de Ética Médica, e regulado pela Resolução nº 1.974/2011 do CFM, alterada pelas Resoluções nºs 2.126/2015 e 2.133/2015, ambas do CFM, referentes à propaganda em Medicina.
Parecer nº 126/2020 do CRM-MG - Ementa: A formação de um grupo fechado de médicos para discussão de casos é permitida, sendo para tanto necessário um administrador médico, com garantia da segurança do sistema e da privacidade dos pacientes. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/MG/2020/126. Acesso em: 31 maio 2021.

38. A Resolução CFM nº 2.178/2017 regulamenta o funcionamento de aplicativos que oferecem consulta médica em domicílio, tratando, inclusive, da cobrança de honorários, em que veda a divulgação de valores em anúncios promocionais em razão de poder configurar forma de angariar clientela ou concorrência desleal.

39. A ANPD ressalta, em seu guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte, a importância da segurança das comunicações frente à vulnerabilidade nos processos de transmissão de dados e informações, sugerindo algumas medidas para evitar incidentes. A título de exemplo, utilizar conexões cifradas (com o uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim; tráfego de rede deve ser gerenciado, podendo instalar e manter um sistema de firewall13; caso utilize serviços web, dar preferência a firewalls de aplicação web (Web Application Firewall – WAF); utilizar ferramentas para proteger serviços de e-mail, tais como antivírus integrados, ferramentas anti-spam e filtros de e-mail; remover dados desnecessários em sites da empresa e criar canais de acesso restritos para clientes quando envolver dados sensíveis. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 08 nov. 2021.

O Conselho Federal de Medicina e alguns Conselhos Regionais[40] já se pronunciaram acerca da questão, sendo que não há entre os órgãos de classe uma uniformidade, pois, ao mesmo tempo em que o parecer nº 14/2017 se pronunciou favorável ao uso do WhatsApp[41] e de plataformas similares para a comunicação entre os médicos e seus pacientes para envio de dados e como meio para sanar dúvidas, inclusive, em grupos fechados de especialistas e corpo clínico de instituição, fazendo a ressalva quanto ao caráter confidencial das informações trocadas,[42] o Conselho Regional de Medicina do Estado do Amazonas expressou opinião contrária.[43].

Outra preocupação é a forma de envio de exames,[44] prescrições, atestados médicos, marcação de consultas,[45] que deve ocorrer por meios seguros, com o

40. Parecer nº 212/2020 CRM-MG, Ementa: "As plataformas que atendem ao nível de segurança NGS2, estabelecido pela Portaria 467 do Ministério da Saúde, bem como a Lei 13.898/2020, podem ser utilizadas no exercício da Telemedicina". Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/MG/2020/212 Acesso em: 31 maio 2021. Parecer 08/2020, CRM-MG, Ementa: "É permitido o uso do WhatsApp e plataformas similares para comunicação entre médicos e seus pacientes; em caráter privativo, para enviar dados ou tirar dúvidas em absoluto caráter confidencial; sendo opcional esta via de comunicação entre o médico e o paciente". Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/MG/2020/8. Acesso em: 31 maio 2021.
41. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2017/14. Acesso em 31 maio 2021.
42. O Conselho Regional de Medicina do Estado do Paraná, no ano de 2015, em resposta à consulta formulada acerca do uso do aplicativo WhatsApp por representantes legais de menores com envio de fotos para receber atendimento médico via telefone, não proibiu o seu uso, mas esclareceu que não se trata de ato médico completo, e que não prescinde da realização da anamnese e exame físico prévio, ficando a critério do médico e em acordo com o paciente ou representante legal combinar o envio de exames ou novas informações por meio eletrônico, considerando o disposto nos arts. 5º, 32, 37, 87, todos do Código de Ética Médica e art. 1º da Resolução 1.958/2010 do CFM. Ressalvou, ainda, que o profissional médico não poderá receber remuneração por suas orientações/prescrições via WhatsApp por não se tratar de ato médico completo.
43. Parecer nº 6/2018, CREMAN, Ementa: "Telerradiologia. Prática por meio de Whatsapp, e-mail e afins. Impossibilidade. Registro nos Regionais onde estão ocorrendo a transmissão. Obrigatoriedade. Deve atender aos requisitos obrigatórios do 'Nível de Garantia de Segurança 2 (NGS2)', estabelecida no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde vigente, editado pelo CFM e Sociedade Brasileira de Informática em Saúde (SBIS). O médico também deve estar registrado em ambos os regionais". Disponível em: https://sistemas.cfm.org.br/normas/ visualizar/pareceres/AM/2018/6. Acesso em: 31 maio 2021.
44. O Conselho Regional do Paraná, por meio do Parecer nº 1931/2008, referente ao envio pela Internet de exame de Termometria Cutânea (medida da temperatura cutânea de alguma parte do corpo) conclui pela possibilidade, desde que seguidas às normas técnicas de segurança em transmissão de dados via Internet para garantir o sigilo e a privacidade do paciente.

uso de ferramentas que protejam o acesso por pessoas não autorizadas, seja com o uso de senha, *firewall*, cópias de segurança, filtros, dados biométricos, entre outros, o que nem sempre conseguem proteger contra ataques cibernéticos,[46] vazamentos, acessos indevidos. Caberá ao controlador de dados comunicar, em caso de incidentes, à Autoridade Nacional e ao titular dos dados (art. 48 da LGPD e art. 10, do CDC).[47]

Toda fragilidade à qual os dados sensíveis dos pacientes estão sujeitos impõe aos médicos, aos profissionais liberais e aos que constituíram pessoa jurídica o dever de observar os valores e princípios da LGPD, como a finalidade; a adequação; a necessidade; o livre acesso; a qualidade dos dados; a transparência; a segurança; a prevenção; a não discriminação; e a responsabilização e a prestação de contas (art. 6º da LGPD).

A LGPD impõe aos agentes de tratamento o dever de adotar medidas de segurança[48] técnicas e administrativas capazes de proteger os dados pessoais de "acessos não autorizados e de situações acidentais ou ilícitas de destruição,

45. Resolução nº 97/2001 do CREMESP, que, ao se referir às consultas médicas e orientações pela Internet, concluiu: "As clínicas, hospitais e consultórios podem usar a Internet para agendamento e marcação de consultas via e-mail."
46. Em 2017, foi noticiado crime praticado no Hospital de Câncer de Barretos por *hackers* que interrompem até quimioterapia em sequestros virtuais. Disponível em: https://www.bbc.com/portuguese/brasil-40870377 Acesso em 31 maio 2021. Na Alemanha, ataque de *ransomware* em hospital leva paciente à morte. Disponível em: https://olhardigital.com.br/2020/09/18/seguranca/ataque-de-ransomware-em-hospital-leva-paciente-a-morte-na-alemanha/?gfetch=2020%2F09%2F18%2Fseguranca%2Fataque-de-ransomware-em-hospital-leva-paciente-a-morte-na-alemanha%2F. Acesso em: 31 maio 2021.
"Ataques cibernéticos em hospitais aumentam 45% em todo o mundo. A Check Point Research (CPR) relatou um aumento de 45% nos ataques cibernéticos a organizações de saúde em todo o mundo nos últimos dois meses, tornando a saúde o setor mais visado por criminosos cibernéticos." Disponível em; https://minutodaseguranca.blog.br/ataques-ciberneticos-em-hospitais-aumentam-45-em-todo-o-mundo/. Acesso em: 31 maio 2021.
47. Quanto à comunicação de incidentes de segurança com dados pessoais à ANPD acessar: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 08 nov. 2021.
48. ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", desde a concepção do serviço até a sua execução (*privacy by design e privacy by default*), e após seu término (arts. 15, 16, 46 e 47), sob pena de responsabilidade e cominação de sanções administrativas[49] (arts. 44 e 52).

Para além do dever de segurança da informação que abrange a confidencialidade, a disponibilidade e a integridade,[50] a LGPD dispõe sobre a adoção de boas práticas e programas de governança em privacidade para o tratamento de dados pessoais que, a despeito de a lei não estabelecer uma obrigatoriedade, considera sua utilização quando da imposição de sanções administrativas (arts. 50 e 52).

Aos profissionais médicos é aconselhável que formulem suas regras de boas práticas e de governança de dados[51] para as quais devem seguir alguns passos planejados de acordo com sua atividade, sua estrutura, sua finalidade de atuação, os riscos envolvidos em relação à possibilidade de ocorrer incidentes e os benefícios decorrentes do tratamento de dados.

No entanto, indaga-se: quais políticas de segurança[52] e de governança estabelecidas na própria LGPD poderiam ser utilizadas pelos médicos profissionais

49. "Centro Hospitalar Barreiro Montijo foi multado em 400.000 euros por violar o Regulamento Geral de Proteção de Dados. A autoridade de supervisão do país, a Comissão Nacional de Proteção de Dados, constatou que houve três violações do GDPR". Disponível em: https://www.lgpdbrasil.com.br/em-portugal-centro-hospital-e-multado-em-400-mil-euros-por-violar-gdpr/. Acesso em: 31 mai. 2021.

50. ABNT NBR ISO/IEC 27001:2003 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos, ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes.

51. Decreto nº 10.046/2019 – Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados: "Art. 2º Para fins deste Decreto, considera-se: [...] XV – governança de dados – exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos; [...]."

52. As medidas administrativas de segurança de dados pessoais, como ressaltado pela ANPD, devem abranger: i) política de segurança da informação; ii) conscientização e treinamento; iii) gerenciamento de contratos; as medidas técnicas: i) controle de acesso; ii) segurança dos dados pessoais armazenados; iii) segurança das comunicações; e iv) manutenção de programa de gerenciamento de vulnerabilidades; além de medidas relacionadas ao uso de dispositivos móveis e medidas relacionadas ao serviço em nuvem. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 08 nov. 2021.

liberais que são controladores de dados, que atuam em seus consultórios de forma autônoma ou que constituíram pequenas clínicas? Para responder é fundamental a interpretação de cada atuação médica profissional a fim de averiguar que instrumentos devem ser utilizados para se adaptarem à LGPD, bem como os que propiciam um sistema de *compliance* de dados pessoais, o que atrai uma atuação multidisciplinar.

3. O *COMPLIANCE* DE DADOS DOS PACIENTES E A PREVENÇÃO DE RISCOS

No exercício da atividade médica, nos termos da Lei nº 12.842/2013, que dispõe sobre o exercício da Medicina, o alvo é a promoção, a proteção, a recuperação da saúde, a prevenção, o diagnóstico, o tratamento das doenças, a reabilitação dos enfermos e das pessoas com deficiências, devendo o médico agir em prol da saúde do ser humano e da coletividade, sem qualquer discriminação e viés mercantilista (Capítulos I, II, Capítulo II, IX, art. 58, Código de Ética Médica).

Entre os direitos dos pacientes e os deveres dos médicos sempre foi ressaltado o direito do paciente ao sigilo de seus dados e, consequentemente, o dever do médico de mantê-lo como preceituam as normas deontológicas (Capítulo I, IX, arts. 73 a 79, 85 e 89), assim como o direito do paciente de decidir de forma autônoma sobre o tratamento médico, o que resulta no dever do médico de obter o consentimento livre e esclarecido do paciente (art. 22 do CEM, arts. 13 e 15 do Código Civil).

Todavia, não basta o médico manter o sigilo dos dados e observar a autonomia do paciente no que diz respeito às disposições acerca do próprio corpo. A LGPD asseverou o direito do paciente[53] ao sigilo, à informação, com ênfase no tratamento dos seus dados pessoais e sensíveis abrangendo o seu acesso facilitado, claro e ostensivo às informações; as formas de acesso; a disponibilidade; o

53. Cabe ressaltar que o paciente pode ser criança e adolescente, o que atrai normativa mais protetiva diante da vulnerabilidade que fica ainda mais potencializada, nos termos do art. 14 da LGPD, independentemente das especificidades na seara médica quanto à disposição de seu próprio corpo, sua autonomia existencial, a figura do assentimento livre e esclarecido. A respeito do tema, merece leitura: TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. In: A LGPD e o novo marco normativo no Brasil / organização Caitlin Mulholland. Porto Alegre: Arquipélago, 2020.

local de armazenamento; a recuperação; a retificação, correção ou atualização; a portabilidade; o compartilhamento; a ocultação, a anonimização e pseudonimização;[54] o bloqueio ou eliminação, apagamento, esquecimento; a limitação do tratamento; a revogação do consentimento; a revisão de decisões etc. (arts. 9º, 12, 18, 19 e 20, LGPD).[55]

Desses direitos nascem deveres que são atribuídos ao médico-controlador, como o de obter o consentimento livre e esclarecido do paciente para esse fim específico, salvo exceção legal (arts. 7º, 8º e 11, LGPD),[56] que vai além do consentimento referente ao tratamento médico; e o dever de garantir a segurança dos dados por meio de determinadas medidas e instrumentos, sendo de grande valia a utilização de um sistema de governança e *compliance* digital, agindo com transparência, integridade, responsabilidade e prestação de contas na sua atuação.

De acordo com Ana Frazão,[57] *compliance*[58] refere-se

> ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

54. "A pseudonimização é um instrumento utilizado para dificultar a identificação das pessoas quando no tratamento de dados pessoais. Essa técnica se efetiva pela criação de pseudônimos, isto é, pela substituição de um atributo de um registro por outro. Para essa substituição, pode-se recorrer à encriptação, ou seja, os dados encriptados, por meio de uma cifra, denominada chave criptográfica e conhecida apenas por quem está realizando o tratamento dos dados. [...] Já a anonimização consiste na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos. Aplicam-se técnicas que pretendem tornar impraticável, ou razoavelmente impossível, a reidentificação, inclusive pelo próprio técnico que realizou a operação inicial." EHRHARDT JR., Marcos; MODESTO, Jéssica Andrade. Breves Notas Sobre Anonimização e Proteção De Dados Pessoais. *Revista Magister de Direito Civil e Processual Civil*, Porto Alegre, v. 17, n. 99, p. 67-100, nov./dez. 2020.

55. Está previsto no Capítulo III do GDPR os direitos do titular dos dados.

56. A respeito do tema, os ensinamentos de Caitlin Mullholland em artigo: O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020, p. 121-156.

57. FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Grunspun. *Governança corporativa*: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42.

58. "O termo *compliance* é sabidamente oriundo da Língua Inglesa. Sua origem está na etimologia do verbo 'to comply', que não possui tradução exata, mas revela a expectativa de uma postura de conformidade e adesão a parâmetros regulatórios". MARTINS, G. M.; FALEIROS JUNIOR, J. *Compliance* digital e responsabilidade civil na Lei Geral de Proteção de Dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (org.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 274.

E, no que tange ao sistema de *compliance* de dados pessoais, o programa se destina a garantir a observância das normas de proteção dos dados pessoais, em especial as diretrizes da Lei Geral de Proteção de Dados, independentemente de outras normas existentes, já que os dados pessoais deixaram de ser tratados como ativos próprios, livremente comercializados e utilizados, para serem tratados por determinados agentes sem que se desprendam dos seus titulares, trazendo novos deveres de guarda, armazenamento, retificação de informações, entre outras medidas de segurança.

A política de *compliance* de dados auxiliará os médicos na adoção de padrões uniformes de conduta e estratégias para manter os dados pessoais e sensíveis dos pacientes protegidos dentro dos parâmetros legais de forma a minimizar os incidentes que geram violação dos direitos dos titulares quando ocorre o desvio, o vazamento dos dados. Esses incidentes devem ser evitados, pois acabam por violar os direitos dos pacientes, reduzindo sua capacidade de escolha, sujeitando-os a discriminações, suprimindo sua privacidade, o que a LGPD visa combater.

Mas como o médico deve proceder para cumprir seu dever de proteção dos dados pessoais e sensíveis do paciente? O objetivo não é onerar ainda mais os profissionais da saúde, mas trazer uma nova cultura de cidadania digital de maneira a assegurar o uso legítimo dos dados dos pacientes e conferir proteção, evitando responsabilidades, principalmente como o aumento da circulação dos dados, do uso da telemedicina.

Inicialmente, é importante estabelecer algumas etapas a seguir para que o profissional se adapte às novas exigências legais, a fim de legitimar sua atuação profissional não só no que diz respeito ao ato médico, mas diante de seu novo papel de controlador de dados pessoais. Isso porque cabe aos médicos, como agentes de tratamento, agirem de forma transparente quanto ao uso dos dados, cuja finalidade principal é a tutela da saúde humana, prestando contas integralmente e se responsabilizando pelos resultados alcançados.

No caso dos profissionais médicos, é oportuno identificar que medidas organizacionais precisam ser adotadas para se construir um programa de

compliance digital, tendo como base a finalidade da coleta dos dados dos pacientes, a estrutura e os direitos assegurados aos titulares de dados (arts. 2°, 7°, 11 e 18, LGPD).

O primeiro passo é identificar os riscos decorrentes do fluxo de dados existentes no exercício da atividade médica, o que deve ser feito de forma periódica (gerenciamento de riscos). Para isso, deve-se verificar o momento em que ocorre a coleta dos dados, de que forma (cadastros, físicos ou digitais, presencial ou virtual etc.); qual é a qualidade e a quantidade de dados (tipos de dados – pessoais e/ou sensíveis, observado o princípio da necessidade (art. 6°, III, da LGPD); as características dos dados; quem faz a coleta dos dados (funcionários, secretárias ou o próprio médico) e em que momento; quem tem acesso; qual é o prazo de conservação e a forma de acessibilidade.

O médico deve esclarecer ao paciente a finalidade da coleta dos dados (tutela da saúde do titular), especificar caso utilize para outros fins como eventualmente publicitários (ex. envio de informações sobre tratamentos por e-mail), pesquisa científica (Resolução n° 466/20212 do Conselho Nacional de Saúde), eventual compartilhamento com terceiros, outros profissionais da área da saúde (teleinterconsulta), com empresas de apoio de diagnóstico, laboratórios, serviços médicos e de saúde terceirizados, operadoras de planos de saúde/seguro saúde,[59] quando o serviço prestado ao paciente tenha sido realizado por meio de convênio médico. Ressalta-se que o médico poderá utilizar os dados pessoais do paciente em casos em que serão necessários para o cumprimento de obrigação legal ou regulatória; para o exercício regular de direito de defesa em processos judiciais, administrativos ou arbitrais e para a própria tutela da saúde do paciente; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis, entre outras hipóteses previstas no art. 7° referente aos dados pessoais e art. 11 da LGPD para os dados pessoais sensíveis.

Far-se-á, portanto, um mapeamento dos dados envolvidos para, em seguida, implementar um procedimento eficaz que, apesar de não poder assegurar integralmente a não utilização indevida por terceiros, o vazamento, pode minimizar os riscos a que os dados dos pacientes estão expostos, fechando as brechas dos canais de comunicação, tanto internamente quanto externamente, observando, com isso, o princípio da prevenção (art. 6°, VIII, LGPD).

59. NOTA TÉCNICA N° 3/2019/GEPIN/DIRAD-DIDES/DIDES. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf. Acesso em: 31 maio 2021.

O segundo passo é a elaboração, a título de exemplo, de documentos como: i) termo de consentimento livre e esclarecido; ii) código de ética e de conduta (boas práticas) contendo procedimentos do tratamento dos dados, instruções gerais, valores que devem guiar os funcionários, as pessoas que trabalham na clínica, no consultório, parceiros, colaboradores, especificar a finalidade do uso dos dados, as medidas de segurança a serem adotadas para proteger e recuperar os dados; iii) o desenvolvimento de política de privacidade; iv) termo de sigilo e confidencialidade para os funcionários (Non-Disclosure Agreement – NDA) para que estes se comprometam a não divulgar informações confidenciais que envolvam dados pessoais[60]; v) relatório de impacto; vi) canal de reclamações, de denúncias para o paciente, a fim de interromper práticas irregulares; vii) eleger um encarregado pelo tratamento de dados – canal de comunicação – interno e externo; viii) adotar medidas técnicas como anonimização ou pseudonimização de dados pessoais para impossibilitar a reconexão de dados pessoais a seus titulares;[61] ix) promoção de interação entre vários profissionais; x) utilizar tecnologias seguras, verificar os sistemas utilizados pelas empresas de tecnologia que fornecem os aplicativos, as plataformas, os locais de armazenamento, se possuem certificações, acreditações e procedimentos de controle;[62] xi) utilizar ferramentas de prevenção, consultas prévias; xii) comunicação de incidentes – incidentes de segurança; xiii) treinar periodicamente a equipe; xiv) realizar monitoramento dos dados, fazer relatórios; xv) manter registros das operações de tratamento de dados; xvi) realizar contratações com fornecedores que observam a LGPD e legislações atinentes, e que tenham certificações, acreditações por entidades especializadas; xvii) elaborar regulamento interno, entre outros instrumentos.

60. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 08 nov. 2021.

61. Cf. ALMEIRA, Mariana de Moraes. A segurança e as boas práticas no tratamento de dados pessoais. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020, p. 319-342.

62. "[...] empresas de tecnologia que trabalham com *cloud computing* têm uma preocupação muito grande e procuram certificações e procedimentos de controle, até mesmo internacionais como o *Health Insurance Portability and Accountability Act* (HIPAA – Lei de portabilidade e responsabilidade de provedores de saúde)." As maiores preocupações em *compliance* na saúde com empresas de tecnologia. Por Iomani Engelmann em 26 de maio de 2020. Disponível em: https://www.pixeon.com/blog/compliance-na-saude/#:~:text=As%20maiores%20preocupa%C3%A7%C3%B5es%20em%20compliance%20na%20sa%C3%BAde%20com%20empresas%20de%20tecnologia&text=Compliance%20na%20sa%C3%BAde%2C%20de%20forma,controles%20acordados%20com%20as%20empresas. Acesso em: 31 maio 2021.

E, por fim, será necessário o auxílio dos operadores de TI para implementar várias medidas já apontadas, de forma a utilizar veículos e ferramentas seguras, uso de senhas, *firewall*, criptografia etc.

A obtenção do consentimento livre e esclarecido do paciente é fundamental para o tratamento dos dados do paciente, salvo nas hipóteses de dispensa prevista em lei (arts. 7º e 11, LGPD), e, uma vez coletados os dados, identificar quem, porventura, poderia ter acesso, como restringir no ambiente do trabalho o acesso por secretárias, outros profissionais da clínica e terceiros não parceiros ou não autorizados. É importante definir, com suporte técnico, quais veículos de comunicação, plataformas, software, aplicativos, mídias sociais, serão utilizados com os pacientes para troca de informações, envio de pedidos médicos para a realização de exames, a manipulação de medicamentos, receitas, atestados, observados os limites de segurança para salvaguarda dos dados pessoais dos pacientes desde a concepção e a proteção por defeito.

As regras de boas práticas de governança e o desenvolvimento de mecanismos de *compliance* facilitarão o processo de adaptação à LGPD, modificando a cultura de proteção de dados pessoais desde a base organizacional da atividade médica. É por meio da atuação proativa dos médicos, controladores de dados dos pacientes, que será possível dar efetividade ao exercício dos direitos dos titulares/pacientes e ao livre desenvolvimento de sua personalidade.

Considerações finais

O elevado volume de circulação de dados pessoais e de dados clínicos (sensíveis) pelas redes, pelas mídias sociais, torna os pacientes cada vez mais vulneráveis, sendo alvos fáceis de incidentes que expõem seus dados de forma indevida, podendo comprometer sua saúde, seu convívio em sociedade, restringindo seu campo de contratações, sua atividade laborativa, seu acesso a seguros, planos de saúde, afetando diretamente sua capacidade de escolha, sendo alvo de discriminações e supressão da sua privacidade. São esses riscos e a forte probabilidade de danos extrapatrimoniais e patrimoniais a que estão sujeitos os titulares de dados pessoais e sensíveis que a Lei Geral de Proteção de Dados visa combater por meio de uma regulação sistemática e sancionatória, que, somada a outras normas existentes, pretendem tutelar determinados bens merecedores de tutelas.

A relação médico-paciente é pautada na confiança estabelecida entre eles, no princípio da transparência e da boa-fé, e vai além dos cuidados com a saúde e o corpo do paciente, alcançando a sua personalidade com um todo, que se completa nos seus dados pessoais e sensíveis. Os grandes desafios da era digital

relevam também no setor da saúde um grande despertar da urgente necessidade de tutelar os dados sensíveis dos pacientes pelo seu forte potencial de causar danos quando violados.

O fato de os médicos atuarem de forma autônoma ou de constituírem pessoas jurídicas de pequeno porte não os afasta da importância de desenvolver uma cultura de governança de dados. O que implica na adoção de medidas técnicas, administrativas, éticas, na área de segurança da informação, com suporte de uma consultoria jurídica, de TI, para manter íntegros os dados pessoais dos pacientes durante toda a atividade de tratamento.

A integridade da prestação de serviços médicos tem em um de seus pilares a adoção de práticas de *compliance* de dados indissociáveis dos padrões éticos de conduta, da autorregulação, da autovigilância. Portanto, caberá ao médico agir de forma diligente na implementação, no desenvolvimento e monitoramento dos programas de *compliance*. Essa tarefa depende de uma iniciativa de conteúdo multidisciplinar, em que será possível assegurar o cumprimento não só das leis de proteção de dados, mas também das normas deontológicas, dos guias de boas práticas. Tudo tendo como principal objetivo proteger os interesses dos pacientes vulneráveis em sua integralidade, abrangendo não apenas sua integridade psicofísica como o livre desenvolvimento da sua personalidade, o exercício da sua dignidade.

Referências

ALMEIRA, Mariana de Moraes. A segurança e as boas práticas no tratamento de dados pessoais. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020, p. 319-342.

CABELLA, Daniela Monte Serrat; FERREIRA, Raissa Moura. *Descomplicando: Agentes de tratamento*. Disponível em: https://www.migalhas.com.br/depeso/326741/descomplicando-agentes-de-tratamento. Acesso em: 29 maio 2021.

COSTA, José Augusto Fontoura. Tratamento de dados de saúde na LGPD: Obrigações, limites e responsabilidade dos agentes. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de proteção de dados pessoais comentada*. 3. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.). *Tratado de proteção de dados pessoais*. [2. reimp.]. Rio de Janeiro: Forense, 2021, p. 03-20.

FILHO, Eduardo Tomasevicius. Responsabilidade civil na LGPD na área da saúde. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. In: FRAZÃO, Ana Frazão; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.) *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 677-715.

FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Grunspun. *Governança corporativa:* avanços e retrocessos. São Paulo: Quartier Latin, 2007, p. 23-57.

MAIA, Roberta Mauro Medina. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal?. In: FRAZÃO, Ana Frazão; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 131-156.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). In: LGPD: *Lei Geral de Proteção de Dados Pessoais comentada*. 3. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

MARTINS, G. M.; FALEIROS JUNIOR, J. *Compliance* digital e responsabilidade civil na Lei Geral de Proteção de Dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (org.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 263-297.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitlin (org.). *LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago Editorial, 2020, v. 1, p. 121-156.

PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: Interpretação do artigo 11, § 4º, da LGPD. In: DALARRI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2021.

PEREIRA, Paula Moura Francesconi de Lemos; MILDEMBERGER, C. S. Publicidade médica em tempos de pandemia do novo coronavírus. *Revista dos Tribunais*, 2020, v. 1017, p. 385-391.

_____. Publicidade médica nas mídias sociais: proposta de um modelo contemporâneo no Brasil. In: NOGAROLI, Rafaella; NETO, Miguel Kfouri (org.). *Debates contemporâneos em direito médico e da saúde*. São Paulo: Thomson Reuters, 2020, p. 399-428.

_____. O uso da internet na prestação de serviços médicos. In: *Direito digital: direito privado e internet* / Allan Rocha de Souza [et al.]. 4. ed. Indaiatuba: Editora Foco, 2021.

_____. *Relação médico-paciente:* o respeito à autonomia do paciente e a responsabilidade civil do médico pelo dever de informar. Rio de Janeiro: Lumen Juris, 2011.

_____; SCHULMAN, Gabriel. Futuro da saúde e saúde do futuro: impactos e limites reais da inteligência artificial. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Org.). *O Direito Civil na era da Inteligência Artificial*. São Paulo: Thomson Reuters, 2020, p. 165-182.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAAVEDRA, Giovani Agostini. *Compliance* de dados. In: DONEDA, Danilo (et al.). *Tratado de proteção de dados pessoais*. [2. reimp.]. Rio de Janeiro: Forense, 2021, p. 727-741.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo (et al.). *Tratado de proteção de dados pessoais*. [2. reimp.]. Rio de Janeiro: Forense, 2021, p. 21-59.

TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020, p. 157-177.

TERRA, Aline de Miranda Valverde; PEREIRA, Paula Moura Francesconi de Lemos. *Telemedicina no sistema privado de saúde: quando a realidade se impõe*. Migalhas, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/322083/telemedicina-no-sistema-privado-de-saude--quando-a-realidade--se-impoe Acesso em 31 maio 2021.