ANÁLISE DOS DESAFIOS DA ÁREA MÉDICA EM VIRTUDE DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

ANALYSIS OF CHALLENGES IN THE MEDICAL AREA IN VIRTUE OF THE GENERAL DATA PROTECTION LAW – LGPD

***Hamilton Staichok*[1]**

RESUMO

Trata-se de análise na qual se pretende apontar alguns cuidados e deveres dos profissionais da saúde, os quais terão que se reinventar administrativamente, principalmente ao manipularem os dados considerados sensíveis de seus pacientes. Uma espécie de reengenharia deverá ser colocada em prática por este segmento para fazer frente às exigências impostas pela Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Neste aspecto, procura-se indicar questões relevantes relacionadas à segurança das informações, inevitável uso da tecnologia e possíveis sanções, que certamente ocorrerão, caso não se use de cautela na guarda de dados de seus pacientes. A pesquisa teve como base, em especial, a LGPD, sites acadêmicos, dissertações, teses, entre outros.

PALAVRAS-CHAVE: lgpd; privacidade; dados sensíveis; saúde.

ABSTRACT

This is an analysis, in which it is intended to point out some care and duties of health professionals, who will have to reinvent themselves administratively, especially when they manipulate considered sensitive data about their patients.

A kind of reengineering should be put into practice by this segment to be compatible with what the law brings in its contente, since its approval and validity in 2018, and especially now, when the foreseen sanctions can already be applied. In this aspect, we look for to indicate relevant issues related to information security, the inevitable use of technology and the possible sanctions, which will certainly occur, if caution is not used in the data storage of patients. The research was based on LGPD, websites, theses, dissertations and others still.

KEYWORDS: lgpd; privacy; sensitive data; health

1 Pós-graduado em Direito Médico na Universidade Curitiba. Graduado em Direito na Universidade Curitiba. (hamilton.staichok@gmail.com). Este artigo foi apresentado e avaliado com graduação 9,5, em 2022.

O presente trabalho teve orientação da Professora Pós-Doutora Fernanda Schaefer Rivabem. Advogada. Pós-Doutorado no Programa de Pós-Graduação Stricto Sensu em Bioética da PUC-PR, bolsista CAPES. Doutorado em Direito das Relações Sociais na Universidade Federal do Paraná, curso em que realizou Doutorado Sanduíche nas Universidades do País Basco e Universidade de Deusto (Espanha) como bolsista CAPES. Professora da Universidade Curitiba. Coordenadora do Curso de Especialização em Direito Médico e da Saúde da PUC-PR. Contato: (ferschaefer@hotmail.com)

INTRODUÇÃO

Muito se tem falado sobre a Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709/18), parcialmente em vigor desde 2018 e que desde agosto do ano passado já está tendo sua eficácia testada, pois a possibilidade de aplicação de sanções nas possíveis infrações cometidas é fato consumado. Embora objeto de muita controvérsia, trata-se de caminho sem volta e de aplicação imperiosa, uma vez que não se admite mais a utilização de dados pessoais de maneira aleatória e irresponsável, como vinham sendo manipulados em fase anterior à lei.

É de se esperar que, de agora em diante, com o advento da norma sancionadora, novos rumos com relação ao tratamento dos dados pessoais dos cidadãos sejam tomados, pois o uso indevido, a divulgação, a guarda e o compartilhamento podem significar prejuízo ao usuário desavisado.

Se a manipulação de dados pessoais, por qualquer pessoa ou empresa, já pode ser considerada como um fator de risco, esta situação alcança um grau máximo de preocupação quando envolve os dados sensíveis de pacientes na área da saúde.

A própria lei em sua Seção II, artigo 11, define como deve ser conduzido o tratamento dos dados sensíveis, no que tange às informações pertinentes ao paciente, seu estado de saúde, suas comorbidades, enfim, os dados singulares e íntimos, cujos direitos só a ele pertence.

A referida norma não deixa dúvidas, quanto ao manuseio dos dados, tanto por parte dos profissionais médicos, quanto dos planos de saúde, bem como esclarece quanto às exceções, previstas no artigo 4.º e seus incisos, que independem da autorização específica do paciente.

Este estudo objetiva trazer um melhor entendimento da problemática apresentada pela nova Lei Geral de Proteção de Dados, no que tange aos profissionais da saúde e sua readequação na manipulação e tratamento dos dados sensíveis de seus pacientes.

A pesquisa teve como base a LGPD, sites acadêmicos, dissertações, teses, publicações em periódicos, entre outros, capturando as melhores práticas que vêm sendo adotadas em clínicas, hospitais e pelos próprios profissionais da saúde no tocante ao tratamento de dados sensíveis de pacientes. O objetivo final era conseguir uma base sólida de informações, para permear as dificuldades de manter sob guarda tais dados, conforme a lei impõe.

Para tanto, optou-se por subdividir em etapas esta jornada, iniciando-se por tentar esclarecer as diferentes interpretações relativas aos conceitos de dados sensíveis. Na sequência, faz-se breve contemplação dos recursos da informática, de utilização imperiosa, que serão de fundamental importância no quesito de segurança da informação. Em seguida, passa-se pela documentação utilizada para o registro dos citados dados, destacando-se o prontuário. E ao final objetiva-se demonstrar, a responsabilidade civil dos profissionais da saúde em caso de não observância dos dispositivos normativos.

1 LEI GERAL DE PROTEÇÃO DE DADOS

O objetivo da LGPD é o de proteger os direitos fundamentais de liberdade e de privacidade e

o livre desenvolvimento da personalidade da pessoa natural (artigo 1.º).

Visando alcançar esses anseios, a referida norma traça uma caminhada, num primeiro plano, de esclarecer pontos importantes, que contribuirão sobremaneira para entender-se o seu verdadeiro propósito. Dentre tantos, um dos que têm gerado mais dúvidas, indubitavelmente, é o comparativo entre os dados pessoais e os dados sensíveis.

Em seu artigo 5.º, incisos I e II, foram conceituados de maneira sucinta os dados pessoais e os dados pessoais sensíveis:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - 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;

Sem dúvidas, um primeiro passo para que todos os profissionais da área da saúde possam começar a entender o que realmente a LGPD vai impactar, principalmente no que tange ao tratamento/manipulação dos dados dos pacientes, bem como nas precauções necessárias para que este manuseio seja efetuado da maneira correta e segura, evitando, enfim, qualquer represália da norma em questão.

1.1 Os dados sensíveis dos pacientes

Para que se possa entrar definitivamente no assunto, inicialmente é necessário que se faça uma análise do que realmente se pode considerar como dados sensíveis. Embora pareça de definição fácil, existem muitas controvérsias por tratar-se de assunto abrangente e muitas vezes se misturam as conceituações envolvendo dados pessoais, dados médicos ou sensíveis.

Em verdade os dados médicos ou os dados sensíveis são oriundos dos dados pessoais que são mais abrangentes, sendo os dados sensíveis muito mais específicos e é justamente por isso que a LGPD tenta protegê-los de maneira singular. Neste sentido ensina Schaefer (2010, p. 48) que:

> Dados médicos são aqueles que abarcam dois elementos: o elemento material (é a sua base física, tudo que dá suporte físico à informação, como os exames e as amostras biológicas); e o elemento imaterial (formado pelo conjunto de informações basicamente obtido da história clínica do paciente e de documentos médicos diversos e que pode assumir diferentes funções – inclusive política e econômica – dependendo do destino que se pretende dar a eles). São elementos que devem ser igualmente considerados bens da personalidade (pois detentores de informação pessoal – atributo da personalidade), uma vez que compõem parte do indivíduo, e, por isso, protegidos pelo direito à privacidade e pela autodeterminação informativa, observadas as singularidades de seu objeto.

É baseado no direito à privacidade e pela autodeterminação informativa que os dados sensíveis merecem uma proteção especial, pois como envolvem dados que muitas vezes revelam a intimidade do paciente, são cobertos por esse manto, como bem define Schaefer (2010, p. 51):

> Por estarem compostos por uma gama muito grande de informações pessoais especialmente qualificadas (pois capazes de revelar íntimos segredos), os dados referentes à saúde gozam de particular proteção, uma vez que afetam os aspectos mais íntimos da personalidade e forçam o indivíduo a lidar com sua própria individualidade (relacionada diretamente à própria personalidade). Por isso,

> à história clínica do paciente se impõe o dever de confidencialidade, obrigação que, por sua própria natureza, não pode ser considerada absoluta, podendo, em alguns casos (doenças infectocontagiosas, epidemias etc.), ser relativizado por questões de necessidade pública.

Na mesma linha, colabora com a definição de dados sensíveis Faleiros *et al* (2019 - p. 214 e 215):

> Mister ressaltar que são consideradas dados sensíveis as informações que estejam relacionadas a características da personalidade do indivíduo e às suas escolhas pessoais, a exemplo de sua origem racial ou étnica, de sua convicção religiosa, de sua opinião política, da filiação a sindicato ou a organização religiosa, filosófica ou a partido político, bem como os detalhes referentes à sua saúde ou à sua vida sexual, além dos dados genéticos, da biometria, da geolocalização.

Já Tepedino e Teffé (2021 – p. 108) acrescentam sobre a necessidade de consentimento no tratamento de dados sensíveis, porém advertem sobre a excepcionalidade com que se deve tratar o assunto, devido à relevância das informações:

> A mera proibição do tratamento de dados sensíveis mostra-se inviável, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, além de existirem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como exemplo, algumas entidades de caráter político, religioso ou filosófico. Dessa forma, entende-se que o tratamento de dados sensíveis é possível e, inclusive, necessário em determinadas circunstâncias. Contudo, deverá ser considerado excepcional, pela relevância dos valores em questão, e autorizado quando não houver utilização discriminatória das informações coletadas.

As condicionantes para o tratamento de dados sensíveis dos pacientes estão contempladas na LGPD com mais veemência em seu artigo 11, que contempla que tais dados podem ser tratados com ou sem o consentimento do paciente, dependendo da finalidade:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Diante da positivação detalhada, Faleiros *et al* (2019 - p. 227) pede a reflexão sobre em que condições há o fornecimento dos dados pessoais, e se realmente essa entrega é efetuada de maneira responsável. Aponta, ainda, que o assunto merece estudos mais aprofundados:

> Se os fluxos de dados são incessantes e se tornam cada vez mais imprescindíveis para o exercício de inúmeras atividades cotidianas, também os riscos advindos dessa nova realidade passam a gerar

> efeitos que o direito precisa enfrentar. Vale dizer: não basta que se tenha legislações detalhadas e repletas de conceitos! Para que seja efetivamente aplicável a abrangência de proteção da LGPD, impõe-se um repensar sobre o modo como a entrega de dados pessoais ocorre.

É de se esperar que, de agora em diante, toda e qualquer manipulação de dados sensíveis de pacientes, estejam sob o olhar das autoridades fiscalizadoras, muito mais em virtude das possíveis sanções que possam ser aplicadas, porém de qualquer forma, neste momento, é preciso que todos os envolvidos reflitam sobre a seguinte pergunta: quais cuidados os profissionais da área da saúde deveriam adotar para mitigar estes riscos?

Resta claro que uma espécie de reengenharia deverá ser colocada em prática por este segmento para fazer frente às exigências que a lei traz em seu conteúdo e principalmente agora, quando as sanções previstas já podem ser aplicadas. Esta necessidade está cada vez mais latente, pois conforme Schaefer (2010, p. 61):

> Por sua natureza, portanto, os dados de saúde considerados sensíveis não podem ser tratados (recolhidos, elaborados, transmitidos e conservados) automaticamente, a menos que sejam previstas garantias legais para essas situações ou consentimento expresso e específico de seu titular.

A não adequação aos dispositivos legais trará consequências nada agradáveis aos envolvidos no tema, uma vez que as responsabilidades vertem de acordo com a potencial participação dos atores. A respeito Schaefer (2010, p. 60) afirma que:

> Assim, denominar um dado nominativo como sensível é reconhecer-lhe sua condição de dado que deve ser especialmente protegido uma vez que a revelação de seu conteúdo pode potencialmente causar lesão ao seu titular ou a pessoas a ele vinculadas.

Importante, portanto, que os profissionais da área da saúde, procurem estar concentrados nas novas determinações, uma vez que afetam de maneira direta as suas atividades. Não se trata apenas de um cumprimento de normas, e sim um despertar para o significado do que é realmente um dado sensível e o quanto a sua divulgação, sem critério, pode afetar a vida de seu paciente, quer seja em seu estado clínico material como também no critério emocional psicológico.

1.2. A necessidade de buscar segurança em sistemas informatizados

Para enfrentar os riscos de acesso indevido de dados privados, notadamente as empresas do ramo da saúde deverão se precaver no sentido de obter sistemas informatizados que estejam aptos e desenvolvidos especificamente para a manutenção da segurança dos dados médicos de seus pacientes.

A preocupação maior reside na qualidade desses sistemas de segurança, uma vez que este avanço tecnológico pode apresentar duas faces: a primeira refere-se ao tratamento avançado de certas comorbidades, pois as informações compartilhadas entre equipes médicas, poderão propiciar a utilização de métodos modernos e que trarão grandes benefícios coletivos, mesmo que se utilizando de dados privados. No entanto, em segundo plano, em caso de utilização para outros fins, estar-se-ia diante de uma exposição indevida e de consequências inconcebíveis, conforme leciona Schaefer (2010, p. 54):

> A informática médica permite o acesso rápido e seletivo a dados e a informações referentes ao pa-

> ciente ou à coletividade, ao alcance e determinação do tratamento, permitindo, inclusive, a atuação em equipe (com profissionais fisicamente distantes). É, portanto, instrumento imprescindível não apenas na atuação individual, mas também, para a própria pesquisa científica e definição de políticas sanitárias.
>
> A inserção de novas tecnologias na área de saúde, embora traga muitas promessas, também provoca preocupações, e uma delas está justamente ligada à digitalização do corpo humano, sua maior exposição e, consequentemente, ao problema das informações dele obtidas e do valor a elas atribuído.

Segundo Thissen *et al* (2019), é necessário um sistema de segurança robusto, capaz de minimizar os riscos de possíveis vazamentos de informações, bem como um grau elevado de responsabilidade das pessoas que tratam esses dados, tanto no dia a dia em suas funções, como em possíveis manipulações de informações, durante pesquisas, zelando pela confidencialidade que este tipo de atributo tecnológico deve proporcionar:

> Dados confidenciais de pesquisas de saúde precisam ser protegidos contra perda, dano ou liberação indesejada, especialmente quando os dados incluem informações de identificação pessoal, informações protegidas de saúde ou outro material privado. Pesquisadores e profissionais devem garantir privacidade e confidencialidade na arquitetura dos sistemas de dados e no acesso aos dados. Os riscos internos e externos podem ser deliberados ou acidentais, envolvendo perda não intencional, modificação ou exposição. Para prevenir o risco ao permitir o acesso, é necessário equilibrar as preocupações com o fornecimento de um ambiente que não impeça o trabalho.

A LGPD opta por diferenciar os dados pessoais comuns dos considerados sensíveis, os quais são monitorados de maneira mais contundente, pois podem gerar conflitos e discriminação e, portanto, devem ser tratados com extrema cautela.

A manipulação desses dados deve ser efetuada de maneira responsável, pois qualquer deslize pode implicar o desatendimento legal. Com este propósito, vislumbra-se que, dentro de uma empresa que presta serviços médicos ou afins, a orientação aos responsáveis pelas coletas e o conhecimento da lei, propriamente dito, com o devido auxílio da informática com suas inúmeras alternâncias sistêmicas, serão fundamentais para transpor estes desafios.

Os gestores das unidades devem se preocupar com a administração dos riscos apresentados na coleta, guarda, manuseio e descarte dos dados. Na condição de principais responsáveis pela segurança dos dados, devem se precaver, principalmente buscando efetivo controle sistêmico de toda captação das referidas informações, para não ficarem em situação fragilizada diante de possíveis questionamentos futuros por parte das autoridades fiscalizatórias, em caso de vazamento ou utilização indevida.

Fica bastante claro, portanto, que além da implantação de um sistema que neutralize possíveis equívocos ou desleixos no tratamento dos dados pessoais, as pessoas envolvidas na coleta, manutenção, compartilhamento e descarte destes exerçam papel fundamental neste controle. É necessária a criação de áreas específicas para administrar o conteúdo. Desde a simples divulgação do conteúdo da lei em comunicados internos, estabelecendo normas e procedimentos, o próprio incentivo e elaboração de cursos que esclareçam os pontos cruciais do dever de cautela, até mesmo organizar um setor específico de *compliance*[2], que deve ser responsável pelo estabelecimento de diretrizes de viés único, promovendo a sinergia total entre as áreas.

2 *Compliance*. O termo tem origem no verbo "to comply" ("cumprir", "obedecer") (Paz, 2019). É utilizado para definir o estado de estar de acordo com as diretrizes ou especificações estabelecidas pela lei. Portanto, compliance descreve o cumprimento de normas e leis.

O objetivo final é o simples atendimento da nova norma, e, ao mesmo tempo, espera-se manter a tranquilidade no desenvolvimento do trabalho diário, visando não comprometê-lo.

A adaptação rápida e sólida à norma deve ser embasada em programas que aparem todo e qualquer tipo de aresta relacionada à confidencialidade desses dados sensíveis do paciente. A atitude dos envolvidos, aliada ao organograma da empresa, (é claro que se o médico atua sozinho em seu consultório, este deverá assumir praticamente todas essas atividades, adequando-se nas devidas proporções) que fatalmente deverá conter alterações, contemplando governança sobre os riscos, controle, políticas de atuação pré-estabelecidas, criação ou aprimoramento da área de *compliance*, estabelecendo e divulgando as novas regras internas, terão papel crucial para atender as demandas da nova lei.

Neste sentido, opinam Thissen *et al* (2019), alertando que existe a necessidade de um planejamento primário, que contemple todas as etapas da manipulação dos dados pessoais, o que certamente irá minorar possíveis contratempos diante da nova lei:

> O planejamento da segurança de dados de pesquisas de saúde precisa começar no início do projeto e considerar cuidadosamente uma série de fatores determinantes. Para pequenas empresas e aqueles que são novos em segurança de dados, um bom ponto de partida é identificar o nível de sensibilidade dos dados em geral.

Enfim, é de primordial importância adaptar-se de maneira eficaz e célere, quer nos trâmites internos administrativos, quer nas responsabilidades individuais das pessoas envolvidas no tratamento das informações, cuja privacidade deve sempre ser preservada, o que certamente resultará na salvaguarda dos dados sensíveis do cliente e por consequência no cumprimento das normas ora em vigor.

2 DOCUMENTOS MÉDICOS E A LGPD

O profissional da saúde, em especial o médico, deverá se resguardar, documentalmente, do início ao fim em suas intervenções e procedimentos médicos. É nesse momento que se descobre o quão importante é o correto preenchimento, enriquecido ao extremo de detalhes, do bom e eficaz prontuário médico.

A Resolução n. 1.638/2002, do Conselho Federal de Medicina, define prontuário médico:

> Art. 1º -Definir prontuário médico 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.

O prontuário médico deve trazer todas as informações possíveis que envolvam o atendimento do paciente. É nele que se deve fazer constar desde as primeiras consultas efetuadas pelo paciente, as primeiras queixas, exames efetuados, fármacos receitados, enfim deve-se registrar todos os acontecimentos e situações relativas ao estado clínico do paciente e medidas tomadas pelo profissional da saúde para minimizar qualquer efeito mais grave que pudesse ser verificado no decorrer do atendimento.

O cuidado que o profissional da saúde deve ter, relativo a esta documentação, é de primordial importância para que, ao longo do tempo, venha transformar-se num arcabouço da vida clínica do paciente,

de maneira individual e sigilosa. É o que expõe, Schaefer (2010, p. 49):

> A documentação clínica é o conjunto de tudo aquilo que dá suporte à história clínica (ex.: exames, atestados, certificados etc.) e que contém um conjunto de dados e informações referentes ao estado de saúde de uma pessoa. O principal documento clínico é o prontuário médico (que pode ser inclusive eletrônico88) e que deve ser elaborado individualmente a cada paciente assistido.

O próprio Código de Ética Médica (Resolução n. 2.217 de 27.09.2018, CFM), do Conselho Federal de Medicina, em seu artigo 87, traz a obrigatoriedade da elaboração de prontuário de atendimento por parte dos médicos:

> Art. 87. Deixar de elaborar prontuário legível para cada paciente. § 1º O prontuário deve conter os dados clínicos necessários para a boa condução do caso, sendo preenchido, em cada avaliação, em ordem cronológica com data, hora, assinatura e número de registro do médico no Conselho Regional de Medicina.
>
> § 2º O prontuário estará sob a guarda do médico ou da instituição que assiste o paciente.

Importante ainda salientar que o perfeito preenchimento, legível, desses prontuários poderá ser muito útil futuramente, uma vez que servirá como base de consulta por qualquer outro profissional que venha a ter contato com o paciente, facilitando sobremaneira a condução do caso em questão, pois nele constarão medicações atribuídas, exames, possíveis sintomas alérgicos apresentados pelo paciente, enfim um histórico completo que poderá servir de base para novos atendimentos e uma maior acuracidade nas possíveis intervenções.

Ainda em relação ao Código de Ética Médica do CFM, cumpre informar que se trata de um direito do paciente ter acesso ao prontuário, ter conhecimento de todo o seu conteúdo e inclusive obter cópia do mesmo, caso seja o seu desejo:

> Art. 88. Negar ao paciente ou, na sua impossibilidade, a seu representante legal, acesso a seu prontuário, deixar de lhe fornecer cópia quando solicitada, bem como deixar de lhe dar explicações necessárias à sua compreensão, salvo quando ocasionarem riscos ao próprio paciente ou a terceiros.

Além desse direito material do paciente, o conteúdo do prontuário também gera um direito fundamental de confidencialidade desses dados, que podem ocasionar a exposição do paciente, caso esses sejam manipulados indevidamente. É o que reverbera Schaefer (2010, p. 45):

> Os pacientes, ao serem atendidos por quaisquer profissionais da área sanitária, pertencentes à rede pública ou privada, têm o direito a exigir que sua situação seja documentada; bem como, a esses profissionais se impõe tal obrigação. Fato é que o direito à história clínica e à documentação clínica gera um direito fundamental (e geral) à confidencialidade dos dados ali colhidos, que são denominados indistintamente como: dados médicos, dados clínicos ou dados de saúde.

No ponto de vista da segurança para o profissional da saúde, o preenchimento do prontuário de maneira correta e exaustiva, por certo, trará maior tranquilidade ao mesmo, uma vez que em caso de qualquer requisição futura, quer no âmbito administrativo como também na esfera judicial, servirá como documentação de fundamental importância para ser utilizada para desfazer possíveis acusações de responsabilidades ou ainda como diplomas comprobatórios, como bem exemplifica o artigo 89 do Código de Ética Médica do CFM: “liberar cópias do prontuário sob sua guarda exceto para atender a ordem judicial ou para sua própria defesa, assim como quando autorizado por escrito pelo paciente.”

Isso ainda sem falar que esses prontuários poderão conter informações que servirão para um avanço da própria Medicina, para a realização de pesquisas e trabalhos científicos, uma vez que muitas vezes é na prática e nas tentativas que acabam apresentando descobertas que transformam e extrapolam os conhecimentos até então tido como únicos. No entanto, esse é um assunto para outro momento.

2.1 Prontuários eletrônicos

A utilização de prontuários eletrônicos por parte dos profissionais da área médica, já foi e continuará sendo objeto de muita discussão ainda pela frente. Embora com parâmetros definidos tanto pela Resolução n. 1.821/2007 do Conselho Federal de Medicina, bem como pela Lei n. 13.787/2018, para alguns ainda é carente de certificação, apontando como principal característica a sua credibilidade reduzida.

No entanto, verifica-se que quaisquer dos diplomas assinalados dá ênfase à possibilidade de utilização do meio eletrônico, como instrumento capaz de satisfazer as reais necessidades que todo o sistema de informação clínica-médica precisa para prestar um bom serviço, bem como manter a integridade e confidencialidade, que devem ser consideradas basilares.

A Lei 13.787/2018 dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente e em seu artigo 1.º demonstra a pacificação do tema: "a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela Lei n.º 13.709, de 14 de agosto de 2018."

Estas disposições certificam os procedimentos que haviam sido definidos na Resolução n. 1.821/2007, do CFM, com exceção do artigo 10.º, que foi revogado pela Resolução 2.218/2018, que dizia respeito à emissão de selo de qualidade no quesito segurança sistêmica.

Em substituição a esse selo de qualidade, a Lei 13.787/2018 em seu artigo 2.º § 2.º institui: "No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito."

A Resolução n.º 1.821/2007 do CFM também regula a digitalização dos prontuários em papel, desde que siga os protocolos pré-determinados, tais como a integralidade do documento (a manutenção da originalidade de todas as informações).

> Em seu artigo 3.º., a referida resolução, apresenta que, caso o sistema implementado seja dotado de nível de segurança dentro dos patamares exigidos no Manual de Certificação para Sistemas de Registro Eletrônico de Saúde, Art. 3° Autorizar o uso de sistemas informatizados para a guarda e manuseio de prontuários de pacientes e para a troca de informação identificada em saúde, eliminando a obrigatoriedade do registro em papel, desde que esses sistemas atendam integralmente aos requisitos do "Nível de garantia de segurança 2 (NGS2)", estabelecidos no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde.

Diante das oportunidades apresentadas, cabe a viabilização de tais procedimentos e o mercado já apresentava diversas opções de *softwares* que contemplam o prontuário eletrônico.

Não se trata, porém, de escolha fácil, uma vez que, num primeiro momento, o profissional individual ou até mesmo as clínicas da área da saúde deverão tomar extremo cuidado na escolha, aquisição e posterior implantação desses aplicativos sistêmicos, em especial no quesito de atendimento às normas

de certificação e validação, relacionadas ao aspecto segurança das informações, sempre visando atender as prerrogativas da nova LGPD (artigo 46).

2.2 Armazenamento físico e digital

Toda a regulamentação do armazenamento, tanto físico como digital, da documentação clínica dos pacientes (prontuário médico) foi positivada na Resolução n. 1.821/2007, publicada em 23.11.2007. Resolução 2.218/18, CFM, teve revogado o seu artigo 10.º, colocando fim a possível parceria, que seria viabilizada mediante celebração de convênio entre o CFM e a Sociedade Brasileira de Informática em Saúde (SBIS), para a emissão de um selo de qualidade dos sistemas informatizados para estarem ajustados ao Manual de Certificação para Sistemas de Registro Eletrônico em Saúde.

Embora definida já há um bom tempo, poucos detêm o conhecimento de suas especificidades, porém agora com o advento da LGPD, se tornam importantes ou até mesmo mandatórias, pois em tudo estão relacionadas à nova lei e qualquer descuido no trato, arquivamento, descarte pode ter consequências legais aos responsáveis por esta tarefa.

A boa notícia é que, com o auxílio da tecnologia, o prontuário em papel, ainda que seja comumente utilizado, tende a perder espaço para os arquivos eletrônicos, que certamente possuem um grau de segurança muito maior, notadamente no que tange a possíveis extravios ou arquivamentos equivocados que culminam com a não localização dos mesmos. Ao encontro dessa necessidade preceitua o artigo 2.º da citada resolução:

> Art. 2º Autorizar a digitalização dos prontuários dos pacientes, desde que o modo de armazenamento dos documentos digitalizados obedeça a norma específica de digitalização contida nos parágrafos abaixo e, após análise obrigatória da Comissão de Revisão de Prontuários, as normas da Comissão Permanente de Avaliação de Documentos da unidade médico-hospitalar geradora do arquivo.
>
> § 1º Os métodos de digitalização devem reproduzir todas as informações dos documentos originais.
>
> § 2º Os arquivos digitais oriundos da digitalização dos documentos do prontuário dos pacientes deverão ser controlados por sistema especializado (Gerenciamento eletrônico de documentos -GED), que possua, minimamente, as seguintes características: a) Capacidade de utilizar base de dados adequada para o armazenamento dos arquivos digitalizados; b) Método de indexação que permita criar um arquivamento organizado, possibilitando a pesquisa de maneira simples e eficiente; c) Obediência aos requisitos do "Nível de garantia de segurança 2 (NGS2)", estabelecidos no Manual de Certificação para Sistemas de Registro Eletrônico e em Saúde.

Importante citar que esses arquivos lógicos gerados devem ser mantidos de maneira permanente, assim como devem ser dotados de mecanismos de segurança da informação, quer seja de cunho meramente de conservação e manutenção, como também capazes de inibir possíveis invasões e acessos indevidos aos dados dos pacientes. Essa determinação está positivada no artigo 7.º da resolução: *"estabelecer a guarda permanente, considerando a evolução tecnológica, para os prontuários dos pacientes arquivados eletronicamente em meio óptico, microfilmado ou digitalizado."*

Já os prontuários que por alguma razão não puderem ser informatizados terão que ser mantidos em arquivo físico, conforme infere o artigo 8.º da Resolução n. 1.821/2007:

> Art. 8° Estabelecer o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preserva-

> ção dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmado ou digitalizado

Essa situação se apresenta, no mínimo, na contramão da nova lei, uma vez que por ser arcaica, e porque não dizer retrógrada, traz consigo uma grande fragilidade no aspecto de segurança, isso sem falar da logística que o caso requer.

E é exatamente neste aspecto que o profissional da saúde pode ter problemas com a nova lei. É prudente e necessária a adequação do segmento. O arquivamento dos prontuários é talvez o momento que mais exige cuidados e todos os atores devem estar comprometidos. Desde a recepção até o especialista em informática, passando é claro pelo médico, maior responsável pela obtenção, registros e confidencialidade dos dados. É necessário um esforço neste sentido. Uma boa administração neste momento significará paz e tranquilidade para focar no objetivo maior, que é sem dúvidas o desenvolvimento do trabalho com qualidade e técnica para salvar vidas.

2.3 Eliminação de dados

Não menos importante do que o armazenamento dos prontuários eletrônicos, a eliminação desses também deve ser objeto de preocupação e zelo por parte dos profissionais da saúde em geral, uma vez que esse descarte não poderá ser efetuado sem critérios, ao contrário, necessitam de total cuidado e procedimentos que deverão ser seguidos, visando salvaguardar possíveis inconvenientes futuros.

Novamente invoca-se a Resolução n. 1.821/2007 do Conselho Federal de Medicina, bem como a Lei n. 13.787/2018, para esclarecer os procedimentos que devem ser verificados pelos profissionais da saúde, ao longo de todo o cronograma pré-estabelecido pelos normativos, para que o descarte seja efetuado da maneira correta.

A título de exemplificação, o referido dispositivo alerta em seu artigo 4.º que caso o sistema eletrônico implantado para o tratamento do prontuário não esteja contemplado com a respectiva segurança regulamentar, a eliminação do papel não poderá ser efetuada: "não autorizar a eliminação do papel quando da utilização somente do "Nível de garantia de segurança 1 (NGS1)", por falta de amparo legal."

Já o artigo 5.º dispõe sobre as condições necessárias para a precisa eliminação dos prontuários:

> Art. 6° No caso de microfilmagem, os prontuários microfilmados poderão ser eliminados de acordo com a legislação específica que regulamenta essa área e após análise obrigatória da Comissão de Revisão de Prontuários da unidade médico-hospitalar geradora do arquivo.

Conforme adiantado, outro dispositivo que esclarece e regulamenta a possibilidade de eliminação dos prontuários, tanto em papel como os já digitalizados, é a Lei n. 13.787/2018, sancionada em 27.12.2018, que ratifica a anunciada resolução:

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

Ambos os diplomas deixam bastante claras as condições necessárias para o correto descarte dos prontuários. Os responsáveis por essa eliminação de prontuários e, por consequência, de seus dados devem seguir essas orientações à risca, pois além de cumprir os dispositivos das normas, em contrapartida também estarão se adequando às determinações da LGPD (art. 16).

É uma questão de disciplina, tanto o operador[3] como o controlador[4], títulos utilizados pela própria LGPD, devem, de maneira responsável, buscar a excelência no tratamento dos prontuários. Todas as etapas são importantes, a começar pelo registro de informações nos mesmos, a documentação inerente ao processo, o armazenamento e, por fim, o descarte equilibrado e criterioso.

3 RESPONSABILIDADE CIVIL PELO TRATAMENTO DE DADOS

A não observância dos dispositivos da nova Lei Geral de Proteção de Dados, poderá acarretar sanções que variam desde uma simples advertência até multas astronômicas que podem chegar a até 50 milhões de reais (artigo 52).

Um aspecto que deve ser objeto de atenção, uma vez que se apresenta no mínimo controverso, é a figura do médico, como responsável pela guarda e tratamento dos dados. Essa dúvida vem da própria lei, que cita os operadores ou coordenadores envolvidos na manipulação do sistema utilizado para o arquivamento eletrônico dos dados. O artigo 42 da LGPD delimita as responsabilidades desses agentes:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

3 Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

4 Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Num primeiro momento, o médico poderia se encaixar tanto como operador e até mesmo como coordenador responsável, uma vez que a responsabilidade da inserção da totalidade das informações, documentações, diagnósticos, prescrições medicamentosas, entre outras, é integral do médico, então possivelmente, em uma discussão jurídica, haveria a ideia da equiparação da função do médico com a do operador ou do coordenador.

Assevera-se, então, que o profissional médico, por analogia, responderia solidariamente, tanto com o operador como com o controlador por possíveis descumprimentos da norma. Neste sentido, cabe uma atitude bastante conservadora deste profissional, principalmente ao escolher um dispositivo eletrônico confiável, dotado de aplicativo de segurança eficaz, bem como se acercar de pessoas responsáveis o suficiente para garantir a incolumidade dos prontuários eletrônicos e por consequência os dados nele inseridos, aspectos que já foram objeto de estudo em tópicos anteriores.

A LGPD não apresenta de forma clara que os atores envolvidos estariam sujeitos a responsabilidade objetiva ou subjetiva.

A doutrina também está dividida, sendo que alguns autores se posicionam para o lado objetivo da responsabilidade e outros, de maneira contrária, optam por inferir que a legislação traz um modelo de responsabilidade subjetiva.

Neste sentido, assevera Gondim (2021 – p. 25) que o legislador foi omisso na LGPD, no ponto de vista de definição sobre a modalidade de responsabilidade a ser aplicada, se objetiva ou subjetiva:

> Outro ponto que merece atenção para a análise sobre o tema e como restou previsto na LGPD, é que o legislador se omitiu em um relevante ponto para a aplicação prática da responsabilidade, que se trata da avaliação sobre se será uma responsabilidade subjetiva (com a de comprovação de culpa) ou objetiva (independentemente de culpa).
>
> Ao se omitir, a primeira conclusão é de que estaria inserida na regra geral da responsabilização subjetiva, uma vez que, para afastar o pressuposto da culpa, a conduta deve estar prevista em lei ou importar em atividade de risco (art. 927 do Código Civil[5]). Mas, há divergência sobre o tema.

Para Faleiros *et al* (2019 - p. 220), a definição do tipo de responsabilidade civil, está relacionada ao contexto e não somente ao fato. Existe a necessidade de análise aprofundada de todas as particularidades do possível ilícito praticado no tratamento de dados:

> Significa dizer que, para além de diversas situações específicas e evidentemente danosas, é de se esperar que a averiguação de eventual violação – especialmente para fins de aferição da responsabilidade civil – transcenda a mera verificação objetiva do fato e adentre aos meandros contextuais do dano e da utilização do dado.

5 "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem." (BRASIL, Lei n.º 10.406, de 10 de janeiro de 2002. Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 27 janeiro 2022.)

Moraes *et al* (2021 – p. 130) afirmam que se trata de um novo sistema de responsabilidade civil. E esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa", encontra-se indicado no inciso X do art. 6º da LGPD, que determina às empresas que não é suficiente cumprir os artigos da lei; será necessário também demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente".

O artigo 43 da LGPD demonstra as excludentes de responsabilidade dos agentes de tratamento dos dados. Isso significa que, se foram esgotadas as possibilidades de tentativas de salvaguardar a integralidade dos dados, não haveria punição:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Ainda sobre o aspecto de responsabilidade, é importante demonstrar quais as circunstâncias mais relevantes, que devem ser objeto de inquietação por parte dos profissionais da saúde envolvidos no tratamento de dados. O artigo 44 da LGPD esclarece essas deliberações:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

No mesmo artigo, em seu parágrafo único, mais uma vez a LGPD ratifica a necessidade de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, alertando ainda que o responsável: *"responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."*

Entende-se então que a lei, de uma maneira geral, aponta para uma responsabilidade subjetiva do operador, e por analogia do médico.

Parece ser esse o melhor caminho a ser seguido, muito embora exista uma distância considerável entre dados pessoais e os considerados dados sensíveis, que, por suas características, deveriam estar envoltos por um manto de segurança de maior envergadura, devido às consequências que podem ocasionar.

Procura-se, enfim, alertar aos profissionais médicos para os aspectos de diligência que o assunto requer, essencialmente no quesito relativo às medidas de proteção que devem ser implantadas, visando preservar qualquer possibilidade de vazamento de informação, inerente aos prontuários e por consequência a dados do paciente.

Aparentemente, assim procedendo, o médico estaria protegido pelas excludentes de respon-

sabilidade, apontadas nos artigos 43 e 44 da LGPD. Ao menos até que estas dúvidas de interpretação, em especial por parte da doutrina, sejam dirimidas.

CONSIDERAÇÕES FINAIS

As diretrizes estão na mesa. Acredita-se que o assunto é objeto de apreensão por parte dos profissionais da saúde. Não que seja uma matéria desconhecida por parte da classe, pois o tratamento de dados, o sigilo profissional, a relação médico-paciente, e até mesmo as responsabilidades advindas da temática, já é de domínio dos mesmos. Essa carga somente foi majorada com o advento da nova Lei Geral de Proteção de Dados e porque não dizer das sanções que podem ser impostas.

E é voltado exatamente para reduzir esta preocupação, que se procura nesta pesquisa apresentar ingredientes favoráveis para minimizar futuras consequências indesejáveis. Para tanto, será necessária a utilização de meios eletrônicos confiáveis, a exemplo da implantação de sistemas robustos de segurança, que possam proporcionar a tranquilidade para o tratamento dos dados do paciente e ao mesmo tempo atender aos dispositivos da lei. São providências imperativas que, por certo, trarão serenidade aos profissionais para se dedicarem de maneira focada nas duas atividades.

Portanto, são tomadas de decisão que devem ser priorizadas neste momento, sobretudo porque terão reflexos imediatos no dia a dia do profissional. Providenciada a adequação à nova lei, todos os esforços, então, poderão ser canalizados para o desenvolvimento profissional.

É fato de que o controle de dados clínicos não depende tão somente da atuação individual do profissional da saúde. Este trabalho deverá ser elaborado em equipe, desde a recepcionista, do médico atendente, da área da informática, do departamento de logística. Trata-se de um esforço coletivo que, se bem estruturado, tende a apresentar resultados amplamente satisfatórios.

Vislumbra-se, portanto, a necessidade da conscientização de todos os envolvidos no tratamento de dados. As pessoas devem estar engajadas, devidamente orientadas e conhecedoras da legislação. O comprometimento dos atores, aliado à implementação da tecnologia, pode levar ao incontestável, e, portanto, não passíveis de quaisquer sanções.

Diante deste caminho sem volta e de algumas nuances tornadas visíveis neste trabalho, o aspecto de maior relevância, ou que ao menos pareça merecer um certo destaque, está relacionado à capacidade do profissional da saúde em saber enfrentar esses desafios que a LGPD impõe. Essa responsabilidade que a lei delega aos envolvidos, independentemente se de cunho objetivo ou subjetivo, por si só, faz com que cresça a necessidade do comprometimento com a causa, e por consequência seja aguçada a cumplicidade entre eles, desde a recepcionista, do próprio médico, do operador, do controlador, enfim dos agentes de tratamento de dados, esperando-se que tal missão resulte como cumprida.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **CÓDIGO DE ÉTICA MÉDICA** Resolução CFM N.º 2217 de 27/09/2018. Acesso em: 16 dez 2021. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf

BRASIL. **LEI FEDERAL 13787/2018** de 27 de setembro de 2018. Acesso em 15 nov 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm

BRASIL. **RESOLUÇÃO 1821/2007 DO CONSELHO FEDERAL DE MEDICINA**. Acesso em 17 jan 2022. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821

BRASIL. **RESOLUÇÃO 1638/2002 DO CONSELHO FEDERAL DE MEDICINA.** Acesso em 16 jan 2022. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD).** (Redação dada pela Lei nº 13.853 de 2019). Brasília, DF: Presidência da República; 2018. Acesso em 17 nov 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

FALEIROS JÚNIOR, José Luiz de Moura. LONGHI, João Victor Rozatti. **ESTUDOS ESSENCIAIS DE DIREITO DIGITAL.** Laboratório Americano de Estudos Constitucionais Comparados - LAECC. Uberlância, 2019.

GODIM, Glenda Gonçalves. **A RESPONSABILIDADE CIVIL NO USO DOS DADOS PESSOAIS.** Revista IBERC v. 4, n. 1, p. 19-34, jan./abr. 2021. DOI: https://doi.org/10.37963/iberc.v3i2.140. Acesso em: 27 jan 2022. Disponível em: www.responsabilidadecivil.org/revista-iberc.

MORAES, Maria Celina Bodin de. QUEIROZ, João Quinelato de. **PROTEÇÃO DE DADOS PESSOAIS: PRIVACIDADE VERSUS AVANÇO TECNOLÓGICO.** Rio de Janeiro: Fundação Konrad Adenauer, Cadernos Adenauer xx (2019), nº3, outubro 2019. Acesso em: 27 jan 2022. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/download/140/119/.

PAZ, Nathalia. **O QUE É COMPLIANCE?** Idblog. dez. 2019. Acesso em: 17 dez 2021. Disponível em: https://blog.idwall.co/o-que-e-compliance/.

SCHAEFER, Fernanda. **TELEMÁTICA EM SAÚDE E SIGILO PROFISSIONAL.** 2010. Tese (Doutorado). Universidade Federal do Paraná. Setor de Ciências Jurídicas, Curitiba, 2010.

TEPEDINO, Gustavo. TEFFÉ, Chiara Spadaccini de. **O CONSENTIMENTO NA CIRCULAÇÃO DE DADOS PESSOAIS.** Revista Brasileira de Direito Civil – RBD. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. DOI: 10.33242/rbdc.2020.03.005. Acesso em 27 jan 2022. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/521/389.

THISSEN, M. Rita; MASON, Katherine M. **PLANNING SECURITY ARCHITECTURE FOR HEALTH SURVEY DATA STORAGE AND ACCESS**, Health Systems, 9:1, 57-63, 2020. DOI: 10.1080/20476965.2019.1599702. Acesso em 15 nov 2021. Disponível em: https://pubmed.ncbi.nlm.nih.gov/32284851/.