UM DIÁLOGO SOBRE A RELEVÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS NOS ESTABELECIMENTOS DE SAÚDE.

Thauane Prieto Rocha[1]
Lucas Colombera Vaiano Piveto[2]
Trabalho de conclusão de curso[3]

RESUMO: O objetivo da presente pesquisa é apresentar os reflexos da Lei Geral de Proteção de Dados nos estabelecimentos de saúde, principalmente diante do acúmulo de dados enfrentado por esses estabelecimentos após o quadro de pandemia com a aparição do vírus Sars-Cov-2. A metodologia aplicada se classifica como qualitativa. Quanto aos procedimentos técnicos, a pesquisa é classificada como: bibliográfica, com base em dados já analisados e publicados, e documental, material ainda não analisado, nem publicado. Igualmente, a pesquisa abordará as problemáticas a serem enfrentadas na adequação dos estabelecimentos de saúde à LGPD. Isto pois, o armazenamento de dados se encontra saturado nesses locais, principalmente, de dados sensíveis o que torna a adequação ainda mais cirúrgica. Nesse prisma, serão apresentados, não só os benefícios da adequação à Lei Geral de Proteção de Dados, como também o impacto de tal conduta perante a sociedade e o mercado. Em síntese, buscará dialogar sobre a importância em observar as normas da LGPD no cotidiano dos estabelecimentos de saúde frente ao plano global vivido hoje.

PALAVRAS-CHAVE: Privacidade. Estabelecimentos de saúde. Dados pessoais. Proteção de dados pessoais. Privacy by design.

[1] Aluno do Curso de Direito da Fundação de Ensino Eurípides Soares da Rocha, Marília, São Paulo.
[2] Sócio do Gomes Altimari Advogados. Coordenador Adjunto do Curso de Direito do Centro Universitário Eurípides de Marília. Mestre em Direito pelo Centro Universitário Eurípides de Marília (UNIVEM). Pós-Graduado em Direito Digital e Compliance pelo Complexo Educacional Damásio de Jesus. Bacharel em Direito pelo Centro Universitário Eurípides de Marília, UNIVEM (2016). Advogado atuante na área do direito privado, com ênfase em direito empresarial e direito digital. Membro do Núcleo de Estudos em Direito e Internet (NEPI).
[3] Trabalho de Conclusão de Curso em Direito apresentado à Fundação de Ensino Eurípides Soares da Rocha, Mantenedora do Centro universitário Eurípides de Marília, para obtenção do grau de bacharel em Direito.

INTRODUÇÃO

Com o surgimento do Coronavírus SARS-CoV-2 em 2019, não só os hospitais como também as clínicas que realizam exames laboratoriais se encontraram armazenando o dobro de dados pessoais e sensíveis oriundos das vítimas da pandemia. Buscar-se-á, nesse contexto, demonstrar a importância da adequação desses estabelecimentos de saúde à Lei Geral de Proteção de Dados, que trouxe um impacto econômico regulatório transversal em todos os modelos de negócio, como forma de mitigação de riscos e violação a preceitos regulatórios.

A pesquisa se dará por meio da metodologia qualitativa e procedimento técnico bibliográfico além de documental, material ainda não analisado, nem publicado. Ainda, será desenvolvida com a utilização de um plano de trabalho que irá orientar a identificação e seleção das fontes bibliográficas e documentais que serão utilizadas.

O estudo passará pelo plano geral do tratamento de dados nos estabelecimentos de saúde, em seguida se atentará ao *privacy by design e privacy by default* para fins de proteção dos dados e por fim demonstrará os benefícios de um Programa de Conformidade à LGPD a estes estabelecimentos.

Toda essa narrativa se faz relevante, pois, com a promulgação da Lei 13.709/2018, houve inovação no ordenamento jurídico brasileiro incluindo regras, direitos e princípios para o tratamento de dados pessoais. Sem falar do impacto econômico e regulatório do regime geral de proteção de dados que irá refletir diretamente na imagem dos hospitais.

Desse modo, o presente artigo irá dialogar e refletir sobre as vertentes da Lei Geral de Proteção de Dados, bem como elucidar de forma objetiva a relação entre a privacidade e o âmbito da saúde. Não obstante, apresentará, por fim, os benefícios da adoção de um Programa de Conformidade.

1. O TRATAMENTO DE DADOS NOS ESTABELECIMENTOS DE SAÚDE.

Primordialmente, a própria Constituição Federal, em seu art. 5º, inciso X[4], aborda o direito de proteção à privacidade como um direito inviolável do cidadão, salvaguardando,

[4] (LGPD, Art. 5º) Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

assim, a intimidade, a vida privada, a honra e a imagem das pessoas, garantindo o direito à indenização pelo dano material ou moral decorrente de sua violação.

Isto quer dizer que toda pessoa tem o direito a ter paz, tranquilidade da sua vida privada, sua intimidade resguardada, além de permitir que toda pessoa impeça que determinados aspectos de sua vida sejam submetidos contra sua vontade, à publicidade e a outras finalidades feitas por terceiros.

Além disso, o inciso XII[5], do mesmo artigo, da Constituição declara ser inviolável o sigilo de dados. A esse respeito, mostra-se relevante destacar que o Supremo Tribunal Federal proferiu decisão reconhecendo a proteção de dados pessoais como um direito fundamental autônomo.

Isso aconteceu porque, com a ascensão da tecnologia nos métodos de tratamento de dados pessoais há, de forma proporcional, a ascensão dos riscos para a personalidade do cidadão, logo, fazendo jus ao amparo constitucional de forma distinta a proteção já cedida à intimidade e privacidade.

Já no que diz respeito ao Código de Defesa do Consumidor (Lei 8.078/1990), interessante mencionar como este regulamento se inclina no sentido de proporcionar livre acesso ao consumidor às informações existentes em cadastros, fichas, registros e dados pessoais constantes nos bancos de dados de consumidores, nos termos do art. 43 do Código de Defesa do Consumidor[6].

Inegável a semelhança nos objetivos do Código de Defesa do Consumidor e da LGPD, na qual, em seu art. 9°[7] prevê o acesso facilitado às informações sobre tratamento de dados, os quais devem ser disponibilizados de forma clara, adequada e ostensiva.[8]

O Código Civil (Lei 10.406/200) também tem papel fundamental na formação dessas diretrizes, ao proteger os direitos inerentes à personalidade, entre os quais o direito à

[5] (LGPD, Art. 5º) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

[6] (LGPD, Art. 43) O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[7] (LGPD, Art. 9º) O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

[8] MENDES, Laura Schertel e DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados Revista do Direito do Consumidor**, n. 120, São Paulo: Ed. RT, p. 369-483. p. 481

privacidade e à intimidade. Tal zelo pode ser observado em seu artigo 11[9], que declara os direitos de personalidade como intransmissíveis e irrenunciáveis.

Não obstante, o Marco Civil da Internet[10] (Lei 12.965/2014) e seu Regulamentador[11] (Decreto nº 8.771/ 2016) dispõe de forma significativa o tratamento de dados pessoais. Contudo, não estreita seu olhar aos dados coletados no modo off-line ou por meio de redes privativas, limitando-se aos dados que de alguma forma trafegam na internet. Isto se faz possível observar logo no artigo 1º da Lei 12.965/2014[12], o qual direciona tal regulamentação para o uso da internet no Brasil e nada além disso.

Como se pode observar, o tratamento de dados pessoais era abordado pela nossa legislação, de forma direta ou indireta, mas com certa delimitação pelos dispositivos. Diferentemente, por exemplo, da União Europeia que desde 2016 aprovou o General Data Protection Regulation ("GDPR")[13] servindo como fonte de inspiração à LGPD.

Para o perfeito entendimento dessa pesquisa, é fundamental apresentar o conceito de dado pessoal. Em seu artigo 5º, inciso I[14], a legislação traz o dado pessoal como sendo o dado relacionado à pessoa natural identificada ou identificável. Basicamente, o dado identificado é aquele que identifica, imediatamente, uma pessoa, como por exemplo o nome, número do CPF, imagem, entre outros.

Em contrapartida, o dado identificável é aquele que detecta o indivíduo por meio de características esparsas armazenadas num banco de dados que, conjugados, chegam à identidade da pessoa, ainda que separadamente não alcancem tal identificação. Em outras palavras, é um compilado de dados que tornam identificável o indivíduo após o cruzamento de migalhas de informações pessoais.

---

[9] (LGPD, Art. 11) Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

[10] Lei 12.965, de 23 de Abril de 2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[11] Decreto nº 8.771, de 11 de Maio de 2016 - Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

[12] (Lei 12.965/2014, Art. 1º) Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

[13] The European Data Protection Regulation is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe. If you find the page useful, feel free to support us by sharing the project.

[14] (LGPD, Art. 5º) Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Com efeito, a Lei Geral de Proteção de Dados visa regulamentar as formas de tratamento de dados pessoais, sendo importante abordar que, inclusive, os dados públicos ou tornados públicos pelos próprios titulares são foco da proteção pela Lei[15]. Estes, ainda que tratados de forma diferenciada, são abrangidos pela Lei em seu artigo 7º, §3º.[16]

Em um banco de dados de um mesmo controlador[17] podem existir diversas informações relacionadas à uma pessoa que direcionam sua identificação. Nestas informações podem estar presentes 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 vida sexual, genético ou biométrico, são os chamados dados sensíveis[18].

Ao contrário do que muitos pensam, a LGPD não detém sua atenção apenas aos dados cadastrais, na realidade, vai muito além disso. Ela se encarrega de proteger, preventivamente, os dados pessoais como um todo visando evitar o abuso em seu tratamento, que, caso ocorra, tem como consequência o punho repressivo da Lei de Dados.

Os dados sensíveis têm uma proteção extraordinária pela LGPD haja vista serem capazes de conectar ao mais profundo da privacidade do ser humano, atingindo sua intimidade, além de poderem gerar consequências de cunho discriminatório.

Especialmente no âmbito da saúde, o tratamento de dados é carregado de tensão, uma vez que os dados referentes à saúde são dados sensíveis e, por consequência, demandam dupla atenção por parte dos agentes de tratamento no momento do tratamento. Outrossim, não há como falar em atendimento médico sem o compartilhamento do histórico de saúde, do uso de medicamentos, de diagnósticos e de resultados de exames gerando o prontuário médico.

Em qualquer procedimento médico de praxe, o profissional precisa de um histórico completo do indivíduo a fim de proporcionar a devida tutela à saúde do paciente, para, por exemplo, evitar a repetição de exames. Diante disso, pode-se concluir que os dados de saúde trafegam, e necessitam trafegar, dentro de uma cadeia hospitalar.

---

[15] TEREPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato.Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2019, p. 103.

[16] (LGPD, Art. 7º) O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.)

[17] (LGPD, Art. 5º) Para os fins desta Lei, considera-se: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

[18] (LGPD, Art. 5º) Para os fins desta Lei, considera-se: 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.

Nesse sentido, importante ressaltar que, apesar da necessidade, esse fluxo de dados carece de consentimento[19] por parte do paciente titular, via de regra, e excepcionalmente, sem consentimento nos casos em que o objetivo for a tutela da saúde, proteção da vida, isenção de perigo físico do titular ou terceiros.

Vale salientar que, um dos princípios fundamentais do exercício da função médica[20] é exatamente quanto ao dever de sigilo do médico perante informações sobre seus pacientes. Logo, conclui-se que o médico não tem liberdade para compartilhar os dados aos quais tem acesso em razão de sua função.

Como se não bastasse, o mesmo, artigo 85[21], proíbe o médico de revelar o conteúdo do prontuário ou da ficha médica sem o consentimento do paciente, e a penalidade desta disposição acarreta ato ilícito tipificado pelo nosso Código Penal, artigo 154[22].

Nesse mesmo sentido, a Resolução CFM 2.217/2018[23], reforça o ponto sobre sigilo profissional, proibindo o médico de permitir o manuseio, ou o mero conhecimento, de prontuário por pessoas não obrigadas ao sigilo profissional, quando sob sua responsabilidade.

Imprescindível, diante de todo o exposto, notar os impactos positivos do Compliance à LGPD, que vai desde o descobrimento de vulnerabilidades no tratamento de dados até o treinamento de funcionários com o intuito de adequá-los às novas normas. Até porque, a inobservância de tais normas pode acarretar sérios prejuízos à imagem do controlador.

Ainda que existam regulamentações gerais no que diz respeito aos dados pessoais na cadeia hospitalar, nada se compara à atenção oferecida pela nova lei. Todavia, o caminho a ser trilhado pelos hospitais na busca por estes benefícios não é nada simples, e é sobre toda essa trajetória que a presente pesquisa irá dialogar.

Por conseguinte, esse caminhar passará pela evolução da privacidade alinhada com o avanço da tecnologia bem como nas possibilidades de diminuição das brechas nos

---

[19] (LGPD, Art. 5º) Para os fins desta Lei, considera-se: XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

[20] Capítulo I. Princípios fundamentais: XI - O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei.

[21] Art. 1º O médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica (Código de Ética Médica).

[22] (CP, Art. 154) Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.

[23] (CFM 2.217/2018) Capítulo X. É vedado ao médico: Art. 85 Permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade.

tratamentos de dados pessoais nas organizações hospitalares, observando sempre os princípios trazidos pela Lei 13.709/2018.

2. *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT* PARA FINS DE PROTEÇÃO DE DADOS.

É cediço que, os juristas devem sempre acompanhar a realidade da sociedade de modo que o direito atenda as novas e futuras necessidades. Com a privacidade, não foi diferente. A proteção à privacidade e aos dados pessoais sugiram com o propósito de ocupar as lacunas existentes com a migração das relações físicas para o mundo hiperconectado.

Incontestável é que, ante a democratização do acesso à internet majoritariamente no território nacional, com a crescente descomunal de acesso às plataformas digitais, os indivíduos estão conectados ao ambiente de internet e utilizam de forma expressiva as ferramentas, seja para execução do seu respectivo trabalho, seja como uma forma de lazer. E, é fato que a privacidade foi um dos direitos colocados em xeque com tal evolução, estando cada vez mais vulnerável.

No setor da saúde não foi diferente, haja vista que seu laço com a privacidade se dá desde o juramento hipocrático feito pelo médico até a regulação ética e prática da formação do profissional. Contudo, com a aparição do SARS-Cov-2 em meados de 2019, e a consequente situação pandêmica gerada, os hospitais se encontram saturados de informações.

Diante dessa situação apressaram-se na busca por novas tecnologias de informação e comunicação a fim de gerir de forma mais eficaz a demanda triplicada em suas mãos. Eis a relevância da aplicação das diretrizes trazidas pela LGPD nos procedimentos hospitalares os quais têm como combustível dados pessoais de seus respectivos pacientes.

Na prática, para atender tal prerrogativa, é necessário estabelecer termos de adesão nos prontuários que apontem, por exemplo, a integração dos respectivos dados para estudos científicos e análises estatísticas. Uma vez ferido esse princípio, fere-se também o Princípio da Adequação (LGPD, Art. 6º, II[24]) e o da Limitação ao Tratamento Mínimo (LGPD, Art. 6º, III[25]).

[24] (LGPD, Art. 6º) [...] II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

[25] (LGPD, Art. 6º) [...] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Salienta-se que os dados compartilhados dentro de uma cadeia hospitalar são, em sua grande maioria, dados sensíveis, que navegam por meio de exames laboratoriais ou prontuários médicos e, vale reforçar, carecem de mais cautela uma vez que podem trazer consequências de cunho discriminatório ferindo a honra e dignidade de seu titular.

Conforme já mencionado, a LGPD se inspirou de forma significativa na GDPR. Tanto é verdade que usa como fonte legislativa alguns termos, destacando a privacidade na concepção ("data protection by design") ou privacidade por padrão ("privacy by default") denominação estas abordadas pelo artigo 25 da Lei Europeia[26].

Na LGPD essa influência é tratada pelo artigo 46[27] que aborda a necessidade de medidas de segurança, administrativas e técnicas capazes de proteger os dados pessoais e evitar acidentes de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

No contexto do privacy by design ("PbD"), parte-se da premissa de que não é possível promover uma organização capaz de garantir a privacidade dos dados de modo efetivo dentro de um estabelecimento se inclinando apenas para as regulamentações e setores específicos acerca do assunto.

A aplicação do PbD garante a privacidade e permite que os indivíduos tenham controle sobre seus dados pessoais, dando uma clara vantagem competitiva às organizações que adotam tal metodologia. Nesse diapasão, o PbD tem como baluarte 7 princípios.

O primeiro é o caráter proativo e não reativo desse método, ou seja, prever e prevenir incidentes de privacidade antes que estes aconteçam. Em seguida, ter a privacidade como

[26] (GDPR. Art. 25) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

[27] (LGPD, Art. 46.) Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

padrão (privacy by default) em qualquer sistema ou prática de negócio, com a configuração de privacidade já embutida nos produtos, tecnologias ou serviços oferecidos.

Além do mais, o princípio da privacidade incorporada ao design, sendo a privacidade um componente do sistemas de Tecnologia de Informação e práticas de negócio. Outro princípio é da funcionalidade total, cuja ideia é acomodar todos os interesses e objetivos da organização do estabelecimento com a proteção à privacidade.

Ainda neste plano, tem-se o princípio da segurança de ponta a ponta, que nada mais é que proteger os dados desde sua coleta, acesso, uso e armazenamento até o seu descarte. O próximo, mas não menos importante, é do da visibilidade e transparência estabelecendo responsabilidade e confiança.

Por último, o PbD é regido pelo respeito pela privacidade do usuária que foca na necessidade de sempre manter os interesses do usuário acima de tudo, oferecendo, assim, configurações efetivas para proteção da privacidade, informações claras e objetivas sobre o tema e opções "user-friendly".

Nesse prisma, impossível falar sobre o tema sem discursar sobre o Princípio da Finalidade (LGPD, art. 6º, I[28]) no qual os propósitos do tratamento de dados devem ser "[...] legítimos, específicos, explícitos e informados ao titular [...]" e o Princípio de Proteção (LGPD, Art. 6º VII a X[29]) que visa proteger os titulares contra acessos não autorizados, destruição, perda e outros danos, bem como do uso destes dados para fins discriminatórios, ilícitos ou abusivos.

Logo, o tratamento de dados dos pacientes titulares tem como fonte basilar as concepções supracitadas, isto quer dizer que, é levado em conta os efeitos para a privacidade e proteção de dados de todos os mecanismos utilizados dentro do estabelecimento de saúde com o intuito de evitar eventuais riscos à privacidade do paciente.

[28] (LGPD, Art. 6º) As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[29] (LGPD, Art. 6º) [...] VII - segurança: 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; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Ao citar riscos à privacidade no âmbito hospitalar impossível não trazer à tona o ocorrido no final do ano de 2020, quando houve o vazamento de dados de ao menos 16 milhões de brasileiros expondo informações dos pacientes diagnosticados com Covid-19 por quase 1 mês.[30]

Em breve síntese, um funcionário do Hospital Albert Einstein publicou senhas do Ministério da Saúde em uma plataforma aberta o que permitia acesso a dados como CPF, endereço, telefone e doenças pré-existentes de milhares de pessoas, de forma mais específica, houve o vazamento de dados de 16 milhões de pessoas.

Como já abordado na presente pesquisa, a cadeia hospitalar conta com diversos procedimentos e todos dirigidos, de certa forma, por humanos. Ora, já é possível concluir o mérito do compliance de hospitais à Lei Geral de Proteção de Dados.

Pois bem, a implementação de um Programa de conformidade à LGPD nos hospitais traz em seu bojo a conscientização de todos os contribuintes desta cadeia a fim de evitar a catástrofe ocorrida no Hospital Albert Einstein, sendo uma das mais importantes vertentes instaladas durante a adequação do estabelecimento.

É possível afirmar que o ser humano é chave central da maioria dos procedimentos hospitalares e, igualmente, podendo ser centro de inúmeros episódios como do Hospital Albert Einstein. Ao buscar alternativas para se esquivar de tais eventualidades se faz considerável mencionar o artigo 12 da LGPD.

Esse dispositivo oferece a opção da anonimização de dados pessoais sensíveis. A anonimização nada mais é que converter um dado pessoal a um dado anônimo, ou anonimizado. Essa conversão impede que o dado seja associado, direta ou indiretamente, ao seu titular, utilizando-se de meios técnicos disponíveis no momento do tratamento.

Bioni trata do assunto e disciplina que, a supressão ou generalização para anonimização dos dados pessoais é um método cujo intuito é gerenciar a identificabilidade de uma base de dados. Nesse diapasão, as características de cada dado devem estar inseridas em um conjunto de informações as quais irão orientar a análise.

Existem duas formas de anonimizar dados pessoais. A primeira é convertendo de fato o dado pessoal em dado anônimo de modo que este não possa ser revertido em dado pessoal identificado ou identificável. A segunda maneira é conhecida como pseudoanonimização.

[30] Vazamento de dados na Saúde pode gerar ações de reparação, dizem especialistas. Revista Consultor Jurídico, 26 de novembro de 2020.

A LGPD se inclina sobre a necessidade de que, sempre que possível, ocorra a anonimização dos dados (arts. 7º, IV[31], 11, II, "c"[32], 13[33] e 16, II[34]), assim como determina que, embora uma das exceções à eliminação dos dados após o término do tratamento seja o uso exclusivo do controlador, tal possibilidade está condicionada à vedação do acesso aos dados por terceiro e também à anonimização dos dados (art. 16, IV[35]).

Contudo, há ressalvas, para Paul Ohm, professor da Georgetown Law School, a anonimização não passa de um "ouro de tolos" como afirmou em 2010. Isto pois, primeiramente, seria impossível alcançá-la de fato e, ainda que fosse, deixaria a análise dos dados sem conteúdo para estudo[36].

Já o procedimento da pseudoanonimização se dá com a adição de uma determinada informação, esta informação é capaz de associar o dado pessoal propriamente dito ao seu titular. Todavia, essa informação fica sob conhecimento exclusivo do controlador em ambiente diferenciado e mais seguro, não sendo acessível a todos.

É importante enfatizar a distinção entre a anonimização de fato e a pseudoanonimização pois, de um lado a anonimização tem como pressuposto a irreversibilidade (ainda que não absoluta). Em contrapartida, a pseudoanonimização torna inapta a associação do dado com seu titular podendo ser reversível com a informação detida pelo controlador, muitas vezes denominada "chave de acesso''.

---

[31] (LGPD, Art. 7º) O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] V - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

[32] (LGPD, Art. 11) O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [,,,] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: [...] c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

[33] (LGPD, Art. 13) Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

[34] (LGPD, Art. 16) Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: [...] II - fim do período de tratamento.

[35] (LGPD, Art. 16) Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: [...] IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

[36] Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L.

A relevância desses pressupostos se dá, principalmente, no que diz respeito ao tratamento de dados pessoais sensíveis. Isto pois, como já demonstrado, neste procedimento pode haver falhas que resultem no vazamento de dados, mas estes estando anonimizados, ou ainda, pseudoanonimizados, ainda que haja algum tipo de vazamento não expõe seu titular.

No âmbito hospitalar entender esses métodos pode ser essencial na medida em que buscar técnicas para anonimização dos dados garante maior proteção no seu tratamento, encadeando no crescimento da confiança do paciente ao saber que seus dados não são de fácil acesso e são bem protegidos pelo estabelecimento.

Já a pseudoanonimização é uma técnica que pode ser adotada com relação a dados de pacientes inativos. De forma análoga, pensa-se em uma peça antiga do guarda roupa, a qual não é mais usada, não há motivo para mantê-la junta com as demais peças. Essa é a lógica para pseudoaninimização de dados de pacientes inativos.

Os dados desses pacientes podem ser pseudoanonimizados uma vez que são pacientes inativos dentro da cadeia hospitalar e não há motivo para mantê-los completos no sistema. Essa lógica é observada pela autoridade responsável pela fiscalização e aplicação de punições no que diz respeito ao tratamento de dados.

Assim sendo, conclui-se que existem efeitos colaterais significativos na ocorrência de tratamento irregular de dados. Não obstante, existem também técnicas e métodos cabíveis a fim de evitar e diminuir os riscos trazidos por tal tratamento além de beneficiar o estabelecimento hospitalar que se adequa às normas da Lei.

3. OS BENEFÍCIOS DE UM PROGRAMA DE CONFORMIDADE À LGPD AOS ESTABELECIMENTOS DE SAÚDE.

O texto da Lei Geral de Proteção de Dados observou as movimentações internacionais sobre o tema e seguiu os princípios de dados pessoais extraídos de práticas da regulação internacional, qual seja, finalidade, necessidade, proporcionalidade, qualidade, transparência, segurança e livre acesso.

Logo, pode-se dizer que o estabelecimento de saúde que observar e se atentar às diretrizes apontadas pela Lei terá a seu favor o princípio da transparência, qualidade, segurança e livre acesso. O efeito disso, em um mundo cada vez mais globalizado e movido a dados, não poderia ser outro senão positivo aos olhos da Autoridade Nacional de Proteção de Dados (ANPD) e dos pacientes.

Em contrapartida, a não observância de tais prerrogativas acarretará, consequentemente, diversos malefícios que vão de punições, aplicadas desde Agosto de 2021 pela ANPD até eventual queda em sua reputação.

De modo breve, a Autoridade Nacional de Proteção de Dados é responsável pela normatização, implementação, formulação, pelo fomento, pela sanção, educação e pela oitiva da sociedade. Desse modo, pode-se dizer que ela tem uma competência normativo-regulatória.

Nesse sentido, caso o setor de saúde não se adeque será alvo do punho disciplinar da ANPD. Antes de mais nada, salienta-se que o objetivo do presente diálogo não é praticar nenhum tipo de terrorismo acerca das sanções aplicáveis, mas sim, trabalhar com a prática das normas de modo a prevenir futuras penalidades e vazamento de dados.

O artigo 42 da Lei traz a responsabilidade do controlador ou do operador (responsabilidade solidária) em reparar o dano causado a outrem, dano patrimonial, moral, individual ou coletivo, ocorrido por violação à legislação de proteção de dados pessoais. Ou seja, ocorrendo eventual tratamento irregular, ambos respondem pelos danos causados.

Esse tratamento de dados irregular pode acontecer na inobservância da legislação em pauta ou, ainda, na falta de segurança esperada pelo titular no processo de tratamento. Nesse momento, leva-se em conta o modo pelo qual o tratamento é realizado, os possíveis resultados que acarretaria algum tipo de risco ao titular e mais, é analisada as técnicas disponíveis no momento da ocorrência desse tratamento considerado irregular.

Assim sendo, os prestadores de serviços de saúde devem adotar, urgentemente, medidas técnicas e administrativas voltadas para a proteção dos dados pessoais, uma vez que o compartilhamento e divulgação indevido podem implicar em sérias penalidades asseguradas no artigo 52 da Lei Geral de Proteção de Dados.

A primeira sanção abordada pelo artigo é a de advertência, e no ato dela deve estar indicado o prazo para adoção de medidas que visem corrigir o tratamento irregular gerador da infração. Ou seja, é dado um aviso ao estabelecimento para corrigir a falha identificada no tratamento de dados. Penalidade que vem com “dever de casa”.

Ademais, a LGPD prevê multas elevadas aos estabelecimentos que descumprirem as normas, e o valor pode chegar a 2% do faturamento bruto da empresa responsável ou a um teto de 50 milhões, não sendo nada interessante cair nas amarras punitivas da Lei. Aliás, pode-se aplicar multa diária até o limite de 50 milhões.

Inobstante a multa aplicável, outra sanção é o bloqueio ou eliminação dos dados pessoais referentes a infração em questão até que a situação seja devidamente regularizada.

Além disso, é possível a suspensão parcial do funcionamento da atividade ou do banco de dados por até seis meses, sendo prorrogável por igual período, até a regularização do procedimento.

Ainda, há a possibilidade de proibição parcial ou total das atividades relacionadas a tratamento de dados. Entretanto, destaca-se que, antes da aplicação de qualquer dessas sanções há um procedimento administrativo, sendo assegurado o direito de ampla defesa e análise do caso concreto.

Importante elucidar que, a ANPD, para aplicação dessas punições, observará alguns critérios fundamentais como a reincidência, a boa-fé do infrator, a cooperação do mesmo e, pode-se até dizer o mais importante, a adoção de políticas de boas práticas e governança. Com isso, a Confederação Nacional de Saúde criou um Código de Boas Práticas, para servir de contribuição à classe do setor de saúde.

Como bem tratado pela Dra. Patricia Peck[37] as medidas de boas práticas envolvem um método complexo que objetiva inserir mecanismos de educação, conscientização e prevenção quando se trata da segurança dos dados e seu tratamento. Nesse cenário, se faz necessário a fiscalização de procedimentos e treinamento de colaboradores.

Veja como a intenção é exatamente a já abordada, de prevenção e não de punição. É fazer os estabelecimentos se inclinarem ao assunto, em um mundo cada vez mais globalizado e movido a dados pessoais, fazendo com que busquem profissionais para incluírem em seus serviços diários os princípios e normas da Lei Geral de Proteção de Dados.

Nesse diapasão, se faz de suma importância dialogar sobre o impacto na reputação do estabelecimento hospitalar caso não observe as normas da Lei Geral de Proteção de Dados. Indubitavelmente, a reputação junto ao paciente é afetada, minando a confiança e segurança necessária entre essas partes.

Nessa conjuntura, a reputação do hospital frente a outros estabelecimentos do mesmo âmbito e até da economia nacional é profundamente afetada haja vista o respeito à privacidade dos pacientes e à confidencialidade ser um dos princípios éticos basilares das profissões de saúde.

Diante dessa perspectiva, ponderoso se faz tecer sobre os benefícios de um Programa de Conformidade à LGPD aos estabelecimentos de saúde. Tal Programa tem como propósito nortear o comportamento dos profissionais bem como criar raízes de uma cultura contemporânea de proteção dos dados pessoais e de garantia de sigilo com base nos princípios da lei, direitos e bases legais.

[37] PINHEIRO, P. P. Proteção de Dados Pessoais. 2. ed. São Paulo: Saraiva, 2020, p. 166.

A Lei Geral de Proteção de Dados trouxe um impacto significativo no setor da saúde, em razão das operações exaustivas de tratamento de dados pessoais e sensíveis, tal como fortaleceu os princípios já existentes de privacidade, sigilo profissional e proteção de dados assegurados em normas do próprio setor.

Com a adequação do estabelecimento de saúde a um Programa de Conformidade a LGPD fica mais do que clara sua intenção em reduzir os riscos de incidente de segurança e violação de preceito regulatórios, além de demonstrar respeito aos direitos dos titulares de dados ao proporcionar o tratamento adequado de dados pessoais e sensíveis.

Em suma, apesar do caminho à adequação dos hospitais à LGPD ser árduo, ele oferece benefícios não só em face das fiscalizações e eventuais sanções a serem aplicadas pela Autoridade Nacional como também oferece outros pontos positivos, que vão desde a confiança do paciente titular do dado, até a reputação do próprio estabelecimento na área da saúde ao cultivar a cultura de proteção de dados.

5. CONCLUSÃO

Com o surgimento da pandemia, surgiu, de igual forma, a necessidade de uso da tecnologia para celeridade da alta demanda. Nesse sentido, com a vigência da LGPD e a constituição da Autoridade Nacional de Proteção de Dados Pessoais, as normas devem ser efetivamente cumpridas.

Saindo do âmbito da fiscalização, os estabelecimentos de saúde que adotarem um Programa de Conformidade à LGPD se beneficiaram em inúmeros sentidos que vão desde a reputação do hospital até a prevenção contra eventuais punições.

Para que isso ocorra, deverá ocorrer um engajamento total por parte dos profissionais de saúde e da sociedade como um todo. E com a crescente utilização da tecnologia nos procedimentos hospitalares, não há como se isentar da observação da LGPD.

Como já bem abordado pelo Mestre Renato M. S. Opice Blum, ignorar a seara digital, incluindo então a privacidade, do ser humano é equivalente a desrespeitar qualquer outro direito essencial. Sendo assim, pela relevância de sua aplicação, a proteção de dados pessoais, tem sido reconhecida como parte da categoria de direitos fundamentais do homem[38.]

Oportuno se faz, concluir com o recente entendimento do ministro Gilmar Mendes, na Ação de Inconstitucionalidade 6.387-DF-o referido “caso IBGE”, relatada pela ministra

[38] BLUM, Renato Opice. General Data Protection Regulation: Destaques da Regra Europeia e seus reflexos no Brasil. São Paulo: Revista dos Tribunais, 2018.

Rosa Weber, a proteção de dados é considerada direito fundamental, devendo o legislador proteger a autodeterminação informacional.[39]

Em suma, seu voto abrange a essência da presente pesquisa pois estabeleceu que o controle invocado em questão faz caminho para além da mera evolução do direito ao sigilo, sendo na realidade a afirmação da autonomia do direito fundamental à proteção de dados pessoais como categoria dentro do rol dos direitos fundamentais em nosso ordenamento jurídico.

Consequentemente, se faz relevante concluir citando a aprovação da PEC 17/2019 pelo Plenário do Senado Federal, no dia 20 de Outubro de 2021, a qual torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental além tornar competência privativa da União a função de legislar sobre o tema.

Por fim, valioso concluir com a concepção de Rodotá, o qual trata a proteção de dados como um direito fundamental autônomo, expressão da liberdade e da dignidade humana, impedindo que o indivíduo seja objeto de vigilância incessante.[40]

4. REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. **Resolução RDC n. 9, de 20 de fevereiro de 2015**. Dispõe sobre o regulamento para a realização de ensaios clínicos com medicados no Brasil.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 22 out. 2021.

[39] STF - MS: 38187 DF 0060058-45.2021.1.00.0000, Rel. Des. Gilmar Mendes, Data de Julgamento: 02/09/2021, Data de Publicação: 08/09/2021.

[40] RODOTÁ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Trad. Danilo Doneda e Laura Cabral Doneda. Rio: Renovar, 2008. p. 18-19.

MENDES, Laura Schertel e DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados Revista do Direito do Consumidor**, n. 120, São Paulo: Ed. RT, p. 369-483. p. 481.

CONSELHO FEDERAL DE MEDICINA. Resolução n. 2.217, de 27 de setembro de 2018. Dispõe sobre o **Código de Ética Médica**. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 12 mar 2021.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM n. 1.638, de 09 de agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 12 mar 2021.

BLUM, Renato Opice. **General Data Protection Regulation: Destaques da Regra Europeia e seus reflexos no Brasil**. São Paulo: Revista dos Tribunais, 2018.

BIONI, Bruno Ricardo. **Xeque-Mate. O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo, 2015.

PINHEIRO, P. P. **Proteção de Dados Pessoais**. 2. ed. São Paulo: Saraiva, 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância. A privacidade hoje.** Trad. Danilo Doneda e Laura Cabral Doneda. Rio: Renovar, 2008.

TEREPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 2. ed. São Paulo: Revista dos Tribunais, 2019