VICTOR NABHAN SILVEIRA

LEI GERAL DE PROTEÇÃO DE DADOS APLICADA À SAÚDE

Trabalho de Conclusão de Curso apresentado como requisito para a conclusão da graduação em Direito do Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa-IDP

ORIENTADOR: GUILHERME PEREIRA PINHEIRO

BRASÍLIA
Novembro 2020

RESUMO
A Lei nº 13.709 (Lei Geral de Proteção de Dados – LGPD) é uma lei de aplicação transversal e multissetorial, que exigirá adaptação das organizações dos mais variados setores econômicos. O setor de saúde é constantemente anunciado como um dos mais impactados pela lei, ao se considerar que os dados relacionados à saúde estão categorizados como dados pessoais sensíveis, para os quais a LGPD prevê hipóteses mais restritivas de tratamento. Trata- se, todavia, de um setor altamente regulado, que tem considerado valores como o sigilo e a proteção da privacidade na adoção das Tecnologias da Informação e Comunicação (TICs), seja na esfera ético-profissional pelos Conselhos profissionais, ou em âmbito administrativo pela Agência Nacional de Saúde (ANS) e Ministério da Saúde (MS). O objetivo deste artigo é analisar a legislação setorial da saúde no tocante à proteção de dados, no intuito de compará-la à LGPD e extrair quais as implicações para a atividade a partir da vigência da nova lei.
Palavras-chave: Proteção da Dados. Lei Geral de Proteção de Dados. Dados de Saúde.

ABSTRACT
Law No. 13,709 (General Data Protection Law - LGPD) is a cross-cutting and multi-sectoral law, which will require adaptation by organizations from the most varied economic sectors. The health sector is constantly advertised as one of the most impacted by the law, considering that health-related data is categorized as sensitive personal data, for which the LGPD provides for more restrictive treatment hypotheses. It is, however, a highly regulated sector, which has considered values such as secrecy and protection of privacy in the adoption of Information and Communication Technologies (ICTs), whether in the ethical-professional sphere by the professional Councils, or in the administrative sphere by the National Health Agency (ANS) and the Ministry of Health (MS). The purpose of this article is to analyze the sectoral health legislation with regard to data protection, in order to compare it to the LGPD and extract what are the implications for business activity in the sector since the new law came into force.
Palavras-chave: Data Protection. General Data Protection Law. Health Data.

Introdução

É cada vez mais comum a afirmação de que atualmente vivemos na “sociedade da informação”, em que a propriedade das coisas tem sido substituída pelo controle das informações (LIMA, 2017). Dia após dia, as chamadas Tecnologias da Informação e Comunicação - TICs, impulsionadas por técnicas de tratamento de dados e pela altíssima relevância das decisões baseadas em dados, têm propiciado o surgimento de inovações capazes de alterar profundamente as relações sociais.

Em igual passo, ganha força a concepção de que o desenvolvimento tecnológico deve ser harmonizado com a preservação da privacidade, e deve ser atribuído às pessoas maior liberdade e controle sobre informações pessoais coletadas, armazenadas, processadas e disseminadas (MENDES, 2014).

Este contexto, somado à necessidade de alçar o Brasil a um padrão internacional de proteção de dados, resultou na sanção da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), que passou a ter eficácia a em 18 de setembro de 2020. A nova lei visa à conciliação entre o desenvolvimento econômico e tecnológico e a proteção aos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, objetivo declarado em seu artigo 1º. (BRASIL, 2018).

De um lado, a LGPD traz fundamentos protetivos ao usuário-cidadão, tais como o “respeito à privacidade” e a “autodeterminação informativa”, a partir dos quais permite criar mecanismos de correção da assimetria da informação e de poder para conferir maior transparência e responsabilidade nos processos envolvidos no tratamento de dados. De outro, busca compatibilizá-los com “o desenvolvimento econômico tecnológico e a inovação” e “a livre iniciativa”, a fim de que o viés protetivo não represente um freio ao avanço econômico e tecnológico.

Trata-se de uma lei geral de aplicação transversal e multisetorial (MONTEIRO, 2018) que tende a exigir adaptações nas mais diversas atividades econômicas, de maneira que, nas predições iniciais sobre os impactos em diferentes setores, o setor de saúde é constantemente anunciado como um dos mais afetados, por se considerar que

os dados relacionados à saúde estão categorizados como dados pessoais sensíveis, para os quais estão previstas as hipóteses mais restritivas de tratamento.

O setor de saúde é rico em geração de dados e com a adoção das TICs tem passado por uma revolução no acesso aos serviços, na prevenção de doenças, no controle de epidemias e na otimização de recursos humanos e financeiros. Os exemplos nesse sentido são fartos: projetos relacionados à contenção da propagação do mosquito *aedes aegypti* por meio de drones; a realização de exames oftalmológicos remotos por robôs; algoritmos que auxiliam no diagnóstico de depressão; até projetos relacionados à integração de base de dados nas redes prestadoras de serviços da saúde visando ao aprimoramento da pesquisa científica (PAÍS DIGITAL, 2019).

Assim, as TICs abrem possibilidades concretas de melhoria na qualidade da atenção à saúde com resultados “contendo alta resolução e confiabilidade, e criando, com isso, novas oportunidades para que pesquisadores entendam a saúde e as doenças não apenas no âmbito populacional, mas também no individual” (SERPA NETO, 2015).

Por exemplo, o tratamento dos dados epidemiológicos e clínicos colhidos da prestação direta de serviços de saúde pública podem solucionar problemas típicos do sistema de saúde brasileira relacionados “às suas dimensões continentais, à deficiência na infraestrutura dos serviços de saúde, à desigualdade no acesso e até mesmo quanto às questões mais específicas, como é o caso da falta de suporte para a obtenção de uma segunda opinião” (SARLET, KEINERT, 2015).

Contudo, dada importância de se garantir a segurança desses dados, que transitam de forma às vezes desordenada em redes informatizadas de várias instituições, há um enorme esforço do ponto de vista regulatório para proteger essas informações, em respeito à privacidade dos pacientes, mediante regulamentos editados pelos conselhos profissionais, pelo Ministério da Saúde (MS), pela Agência Nacional de saúde (ANS) e pela Agência Nacional de Vigilância Sanitária (ANVISA), referentes a sigilo profissional, segurança na adoção de TICs, bem como guarda e manuseio das informações por parte de seus profissionais.

Diante do cenário exposto, em que já há uma extensa, porém esparsa, regulação setorial, é de se questionar se o advento de uma lei específica sobre proteção de dados

trará impactos significativos a um setor tradicionalmente zeloso no sigilo das informações de seus usuários/pacientes.

Ante o exposto, o objetivo deste artigo é investigar as eventuais alterações na legislação setorial da saúde em razão da entrada em vigor LGPD e investigar suas implicações para a atividade empresarial no setor. Para tanto, primeiramente se analisará a proteção de dados relacionados à saúde sob a ótica da LGPD; em seguida, serão apresentados os principais dispositivos da legislação setorial de saúde no tocante a proteção de dados; por fim, as considerações finais terão por escopo extrair quais as implicações para a atividade do profissional a partir da vigência da nova lei.

2. Dados Relacionados à Saúde na LGDP

O artigo 5º, II, da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018) inclui os dados referentes à saúde na categoria de dados pessoais sensíveis:

> 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; (BRASIL, 2018).

A categoria dos dados pessoais sensíveis envolve dados que exigem maior proteção, pois constituem um risco maior à personalidade do indivíduo, caso conhecidos ou processados (MENDES, 2014), e estão sujeitos a revelar informações com potencial uso discriminatório ou particularmente lesivo com maiores riscos de trazer restrições ao acesso de bens, serviços e ao exercício de direitos (FRAZÃO, 2018). Segundo Mendes (2014), o rigor das normas no âmbito dos dados sensíveis reflete em alguns aspectos, tais como:

i) ampliação das exigências legais para o consentimento do indivíduo sobre a disposição de seus dados pessoais; ii) ampliação das exigências legais para o tratamento desses dados pelo responsável, como, por exemplo, a intensificação de medidas de segurança, em alguns casos; e iii) pelo aumento do controle pela autoridade administrativa para a autorização de armazenamento, processamento e circulação dos dados sensíveis. Quanto ao conceito de “dado referente à saúde”, não há uma definição

específica na LGPD. Entretanto, importa assinalar que o conteúdo da lei brasileira foi produzido à semelhança do regulamento europeu de proteção de dados, o General Data *Protection Regulation* – GDPR (Regulamento UE 2016/679), que, por sua vez, em seu Considerando nº 35, traz um conceito extensivo de dados relativos à saúde, descrevendo diversas ocorrências práticas, conteúdo que serve inclusive de ferramenta interpretativa para se chegar ao conceito aplicável à lei brasileira:

> (35) Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação e serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro (UNIÃO EUROPEIA, 2016)

Dito isso, o artigo 11 da LGPD enumera as hipóteses autorizadoras de tratamento de dados pessoais sensíveis, de forma mais restritiva se comparada aos dados pessoais (não sensíveis). A tabela seguinte expõe de forma comparativa as hipóteses possíveis de tratamento de dados pessoais sensíveis e não sensíveis:

Tabela 1: hipóteses possíveis de tratamento de dados pessoais sensíveis e não sensíveis

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS	HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Consentimento pelo titular (art. 7º, I)	Consentimento pelo titular, de forma específica e destacada, para finalidades específicas (art. 11, I)
Cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II)	Cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, "a")
Tratamento e uso compartilhado de dados, pela administração pública, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei (art. 7º, III)	Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, II, "b")
Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, IV)	Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (art. 11, II, "c")
Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7º, V)	Não há previsão correspondente
Exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da **Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) (art. 7º, VI)**	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)**; (art. 11, II, "d")
Proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII)	Proteção da vida ou da incolumidade física do titular ou de terceiro (art. 11, II, "e")
Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (art. 7º, VIII)	Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (art. 11, II, "f")
Necessidade de atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, IX)	Não há correspondente
Proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, X)	Não há correspondente
Não há correspondente específico, embora se possa compreender que a previsão do art. 7º, IX, abarcaria, com maior razão, a hipótese do art. 11, II, "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

Fonte: JOTA. FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 01nov. 2020.

Como se observa, há uma correlação entre boa parte das hipóteses previstas no artigo 9 (dados pessoais) e no artigo 11 (dados pessoais sensíveis), de modo que "os cuidados já previstos para o tratamento dos dados pessoais devem ser aplicados, com maior razão, ao tratamento de dados pessoais sensíveis" (FRAZÃO, 2018). O comparativo também revela que, nas hipóteses de tratamento de dados pessoais sensíveis, ficam de fora algumas possibilidades previstas para dados pessoais no artigo 7º da lei, a saber, da execução dos contratos, do legítimo interesse do controlador e, no

lugar deste último, o artigo 11, II, “g” previu hipótese mais restritiva e vinculada essencialmente aos interesses dos titulares de dados (FRAZÃO, 2018).

A hipótese autorizadora para tratamento de dados pessoais sensíveis que se destaca como regra geral é a hipótese de consentimento “I – quando o titular ou seu representante legal consentir, de forma específica e destacada, para finalidades específicas” (BRASIL, 2018).

Não obstante, dentre as hipóteses de tratamento de dados de saúde que dispensam o consentimento do titular, merece destaque aquela relativa à “tutela da saúde” em procedimentos realizados por profissionais da área de saúde ou entidades sanitárias (art. 11, inciso II, “f”, da LGPD). A dispensa do consentimento ganha sentido na medida em que o atendimento a pacientes, revestido pelo sigilo profissional, não se viabiliza sem o acesso a dados sensíveis, e caso exigido o consentimento específico para todo e qualquer ato, haveria um provável impasse burocrático na atividade. Outra hipótese semelhante em que consentimento é dispensado faz referência à proteção da vida ou incolumidade física do titular ou de terceiros (art. 11, II, “e”, da LGPD) e deve ser aplicada especialmente em casos de urgência e/ou emergência.

Já a disposição do artigo 11, §4º, veda a possibilidade de utilização de dados relacionados à saúde para comunicação ou uso compartilhado com objetivo de obter vantagem econômica, exceto nas hipóteses de “I - portabilidade de dados quando consentido pelo titular; ou II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar” (BRASIL, 2018).

Outra disposição que se relaciona com o setor de saúde diretamente concerne à hipótese que autoriza o acesso a bases de dados pessoais por órgãos de pesquisa para fins de estudos de saúde pública, independentemente do consentimento específico do titular, conforme previsão do artigo 13 da 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 (BRASIL, 2018).

A hipótese autoriza o acesso, desde que seguro e em ambiente controlado, a bases de dados de pacientes por órgãos de pesquisa, mas veda sob qualquer hipótese que os resultados das pesquisas revelem dados pessoais (art.13, §1º) ou sejam transferidos a terceiros (art.13, §2º), e ainda prevê que o acesso para fins de pesquisa deverá ser regulado pela Autoridade Nacional de Proteção de Dados - ANPD e as autoridades de saúde, que deverão editar regulamento específico sobre anonimização ou pseudonimização desses dados (art. 13, §3º).

Ademais, além daqueles dispositivos que se refletem diretamente em dados referentes à saúde, incide sobre as atividades de tratamento de dados pessoais sensíveis os princípios enumerados no artigo 6º da LGPD: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Esses princípios, cujos conceitos são definidos pela lei, têm grande relevância para sua compreensão sistemática, e servem como importante ferramenta interpretativa de todos os demais dispositivos.

Decorrem diretamente dos princípios mencionados os direitos conferidos aos titulares de dados pessoais (art.18, da LGPD), que, a partir da vigência da lei, terão amplas possibilidades de controle sobre seus dados. Em suma, com a LGPD, o titular dos dados passa a ter direito de obter do controlador, a qualquer momento, informações detalhadas sobre seus dados (confirmação de existência, acesso e informação sobre com quem foram compartilhados), a possibilidade de corrigi-los, eliminá-los ou exigir anonimização de dados desnecessários, bem como revogar o consentimento e até solicitar a portabilidade dos dados a outro fornecedor.

Desses direitos emergem uma série de obrigações práticas às organizações que exercem atividade de tratamento de dados. No caso da rede prestadora de serviços de saúde, para se adequarem à LGPD, serão necessárias medidas que assegurem o livre e fácil acesso aos dados pelos usuários/pacientes, transparência nos processos utilizados no tratamento dos dados, bem como a manutenção de registros íntegros que garantam a qualidade desses dados. Além disso, são necessárias adoção de técnicas de segurança para proteção a acessos não autorizados e situações acidentais, bem como a

implementação de sistemas interoperáveis que permitam ao titular o exercício do direito à portabilidade.

É de se questionar até que ponto o exercício do controle dos dados pelo titular deve ser aplicado em matéria de dados referentes à saúde, uma vez que, por exemplo, a interferência nos registros clínicos de um paciente poderia suprimir informações importantes para o embasamento de decisões futuras, o que inclusive o colocaria em risco. Observa-se que o artigo 18, VI, trata da eliminação dos dados pessoais tratados com o consentimento do titular, de modo que em princípio a hipótese de tutela da saúde, que é processada sem o consentimento, estaria fora do conjunto dos dados passíveis de serem eliminados pelo titular. Trata-se de um ponto importante a ser esclarecido mediante uma regulamentação mais específica pela autoridade de dados, discutida conjuntamente com autoridades do setor da saúde.

Além das incumbências já mencionadas, cada organização deverá designar em seus quadros um encarregado pelo tratamento de dados pessoais, que deverá estabelecer um canal de comunicação entre a organização, que possui a guarda dos dados, e os titulares dos dados, a quem os dados pertencem, bem como junto à autoridade de dados, a fim de receber comunicações e adotar providências. O encarregado também deve orientar funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e seu contato deverá ser divulgado publicamente, preferencialmente no sítio eletrônico do controlador.

A lei, em seu artigo 5º, define como agentes no tratamento de dados o controlador, “VI - a quem compete as decisões referentes ao tratamento de dados pessoais” e o operador, “VII - que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018), os quais são incumbidos de uma série de atribuições e responsabilidades, tais como o registro das operações de tratamento de dados, a elaboração de relatório de impactos à proteção de dados, caso solicitado, a obrigação de comunicar a autoridade de dados em caso de incidente, ou ainda a obrigação de reparar danos a terceiros em decorrência de violação à legislação de proteção de dados.

Outro fator importante trazido pela LGDP está na previsão de sanções administrativas aos agentes de dados em caso de infração à lei, cujas penas contemplam,

entre outras, advertência com indicação de medidas corretivas, obrigações de fazer como a publicização da infração, bloqueio de dados e multa diária e multa simples de até 2% faturamento da organização até o limite de R$50.000.000,00.

3. Proteção de Dados na Legislação Setorial de Saúde

A confidencialidade e o respeito à privacidade constituem preceitos morais tradicionais das profissões de saúde (VILLAS-BÔAS, 2015), nas quais há consenso em torno de um direito-dever de sigilo profissional e da necessidade de se proteger dados do paciente obtidos em decorrência da atividade laboral.

Nesse sentido, o Código de Ética Médica (Resolução CFM nº 2.227/2018) elege como infração ética o ato de "Art. 73: revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente". Ainda, ao corroborar preceito da Declaração de Genebra de 1924, prevê que o sigilo deve ser respeitado mesmo após a morte do paciente e sobre fatos que sejam de conhecimento público (Art. 73, § único, "a").

Disposições semelhantes estão presentes nos códigos de ética de enfermagem (Art. 52 da Resolução COFEN nº 564/2017), fisioterapia (Art. 32 da Resolução COFFITO nº424/2013), psicologia (Art. 9º da Resolução CFP nº10/2005), odontologia (Art. 14 da Resolução CRO nº 112/2018), educação física (Art. 6, XII, da Resolução CONFEF nº 307/2015) e nutrição (Art. 20 da Resolução CFN nº 599/2018).

O regramento ético médico também impõe vedação ao médico de fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens, mesmo com a autorização deste, bem como de permitir o manuseio e o conhecimento de prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade (art. 75 e 85 da Resolução CFM nº 2.227/2018).

Os dados clínicos dos pacientes claramente pertencem a eles próprios, que escolhem a quem deve ser confiado o seu acesso. A vedação ao manuseio dos registros de saúde por profissionais não sujeitos ao sigilo da relação médico-paciente, salvo se consentido pelo próprio paciente, é uma clara conotação nesse sentido. Exceção feita à

possibilidade de acesso aos prontuários por médicos para fins de pesquisa em estudos retrospectivos com questões metodológicas justificáveis e autorizado pelo Comitê de Ética em Pesquisa (CEP) ou pela Comissão Nacional de Ética em Pesquisa (Conep) (Art. 101, §2º, da Resolução CFM nº 2.227/2018).

Também no sentido de reconhecer a propriedade dos dados de saúde por seu titular, a regra expressa no artigo 88 da Resolução CFM nº 2.227/2018 veda ao médico a possibilidade de negar acesso do paciente ao seu prontuário médio:

> Capítulo X DOCUMENTOS MÉDICOS
>
> É vedado ao médico:
>
> [...]
>
> Art. 88 Negar ao paciente ou, na sua impossibilidade, a se 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.

Outro fator central na relação médico-paciente diz respeito à autonomia do paciente e, em certa medida, à sua autodeterminação informativa, que estão contemplados na obrigatoriedade de obtenção do consentimento deste para a realização de qualquer procedimento médico, mediante termo de consentimento livre e esclarecido (TCLE). O paciente, autonomamente, deve decidir sobre optar ou não por um procedimento consciente dos riscos aos quais se submeterá e de todas as possíveis consequências daquele ato, ao passo que ao médico cabe esclarecê-las em linguagem acessível, visando minimizar o quanto possível a assimetria da informação.

Nesse sentido, o artigo 22 da Resolução CFM nº 2.217/2018 dispõe que é vedado ao médico: “Deixar de obter consentimento do paciente ou de seu representante legal após esclarecê-lo sobre o procedimento a ser realizado, salvo em caso de risco iminente de morte”. Ainda, a Recomendação CFM nº1/2016 recomenda que o consentimento seja obtido mediante documento escrito, com linguagem clara, acessível e com conteúdo suficiente.

3.1. Consentimento na Saúde

O consentimento é um dos requisitos para que ocorra o tratamento de dados pessoais. Conforme o art. 5º, XII, da LGPD, o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

O fornecimento do consentimento, de acordo com a Lei Geral de Proteção de Dados Pessoais, em seu art. 8º, deverá ser realizado por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Se fornecido por escrito, deverá constar, dentre as cláusulas contratuais, cláusula destacada sobre o assunto, conforme o parágrafo primeiro do artigo supracitado.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
>
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

O consentimento deve ser, também, informado. Isto porque, o titular só poderá controlar seus dados e decidir sobre a utilização se for informado adequadamente, possuindo à sua disposição, as informações necessárias para tal decisão. Apesar do cidadão dificilmente alcançar o mesmo nível informativo do fornecedor, a informação permite a autoproteção, cabendo ao titular compreender os riscos e possíveis implicações que a utilização de seus dados pode causar (LIMA; BIONI, 2015).

Nesse sentido, o art. 9º da Lei Geral de Proteção de Dados dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva.

> 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:
>
> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;
>
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.
>
> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
>
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Um princípio diretamente ligado ao da informação é o da transparência, vez que a LGPD prevê, em seu art. 6º, VI que a transparência é a garantia de informações claras, precisas e facilmente acessíveis ao titular. Já em seu art. 9º, §1º, a LGPD dispõe que o consentimento será nulo caso as informações fornecidas ao titular, dentre outras hipóteses, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

O consentimento deve ser realizado, ainda, de forma inequívoca, vale dizer, não pode ser feito de forma passiva, mas sim como uma ação do titular, que, conforme visto

anteriormente, deverá ser realizado sob a forma escrita ou por outro meio que demonstre sua vontade (BIONI, 2019, p. 194).

Tal preceito deve ser observado em conjunto com outro adjetivo, o da especificidade. Para que o consentimento seja específico, a expressão da vontade inequívoca deve se referir ao processamento de um dado específico, não podendo ser uma simples autorização de forma geral.

Tanto a característica de especificidade, como da inequivocabilidade, estão intimamente ligadas com o princípio da finalidade, previsto no art. 9º, inciso I, da Lei Geral de Proteção de Dados. Tal qual estabelece que o tratamento de dados deve ter um propósito específico. No caso do consentimento, seja qual for a declaração de vontade, deve ter um direcionamento, uma vez que não se consente no vazio e de forma genérica. Seria semelhante a emitir uma espécie de cheque em branco que esvaziaria qualquer esfera de controle do cidadão sobre seus dados. Tendo assim, com o princípio da finalidade, a possibilidade de analisar se o titular foi adequadamente informado (BIONI, 2019).

Consegue-se perceber, então, que ao decorrer dos anos, a importância da necessidade do consentimento foi crescendo, onde as informações disponíveis são sensíveis e vulneráveis. Toda essa adjetivação do consentimento serviu, principalmente, para que o titular pudesse participar efetivamente no comando de seus dados pessoais.

> O consentimento recebeu, dessa forma, uma adjetivação que auxilia a entender o que é considerado como um consentimento válido pelos vetores da Lei Geral de Proteção de Dados Pessoais. Entre as características, mencionadas acima, consta que o consentimento deverá ser livre, ou seja, deve ser feito de forma espontânea, devendo ser caracterizado pela tomada de uma escolha em meio a tantas outras que poderiam ser feitas por alguém (BIONI, 2019, p. 197).

É relevante destacar que, é possível que haja a revogação do consentimento pelo titular dos dados pessoais. Conforme as diretrizes da Lei Geral de Proteção de Dados, a revogação é um direito do titular, conforme o art. 18, inciso IX, que se dará através da manifestação expressa do titular, por procedimento gratuito e facilitado, em qualquer momento.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Ainda, se as informações disponibilizadas ao titular constarem conteúdo enganoso, abusivo ou não estiverem sido fornecidas com transparência, de forma clara e inequívoca, o consentimento obtido será considerado nulo, conforme o parágrafo 1º do art. 9º, da LGPD.

No parágrafo 2º do artigo citado, encontra-se outra hipótese de revogação do consentimento, de quando houver a mudança da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento anteriormente obtido, o titular precisará ser informado sobre as alterações e, em circunstância de discordância, poderá revogar o consentimento.

A Resolução nº 466/2012 do Conselho Nacional de Saúde, que é o diploma normativo que rege a pesquisa clínica no Brasil, também preconiza o uso do termo de consentimento livre e esclarecido (TCLE) no âmbito das pesquisas, de modo a garantir que dados que permitam a identificação do participante voluntário da pesquisa, sejam mantidos confidenciais, a fim de preservar a privacidade e não provocar danos relativos a estigmatização e discriminação.

A transferência de dados pelo centro de pesquisa, seja ao patrocinador ou para relatar um evento adverso ao Conep ou à Agência Nacional de Vigilância Sanitária (Anvisa), deve ser mantido nível de anonimização, a fim de garantir a privacidade do titular. Além disso, o item IV.3.d. da Resolução CNS 466/2012 orienta que o TCLE deve assegurar plena liberdade ao participante para revogar o consentimento em qualquer momento da execução da pesquisa, inclusive verbalmente, com o respectivo registro no prontuário médico do participante (DALLARI, 2018).

4. Tratamento dos Dados de Saúde

No tocante à guarda dos prontuários, os profissionais ou a instituição que assistem o paciente são responsáveis por armazená-los de modo seguro (Art. 87 §2º, da Resolução CFM 2.227/2018), seja em meio físico ou digital, de modo a preservar-lhes o conteúdo e, consequentemente, o segredo e a não violação à esfera de privacidade e intimidade do assistido. Na área da saúde, portanto, a noção de que os dados de saúde são espécies de dados sensíveis encontra respaldo na regulamentação ética e administrativa. O profissional da saúde, para atuar conforme a ética, deve partir da premissa de que o histórico médico de um paciente contém informações sensíveis cujo vazamento acidental ou voluntário pode ser catastrófico para a vida dele e de e seus familiares e com efeitos irreversíveis (LUCIANO, BRAGANÇA e TESTA, 2011).

Dados os riscos envolvidos no tratamento de dados de saúde, tem se formado uma legislação setorial robusta para impor obrigações e padrões mínimos de segurança no dever de guarda e manuseio dos registros dos pacientes. Processo este que vem se intensificando com o surgimento de tecnologias da informação e comunicação para mediar a atenção à saúde, as denominadas “e-Saúde” (KAMEDA, PAZELLO, 2015, p.50), que englobam serviços como teleconsultorias, telediagnóstico, segunda opinião formativa, telecirurgia, telemonitoramento, teleducação e prontuário eletrônico.

A iniciar pelo prontuário médico, trata-se de documento único que reúne todos os dados da assistência prestada ao paciente, a permitir uma prestação continuada. A Resolução CFM nº 1.638/2002, além de trazer o conceito de prontuário médico, traz informações sobre seu conteúdo essencial e as atribuições de responsabilidade sobre preenchimento, guarda e manuseio, bem como torna obrigatória a criação de Comissão de Revisão de Prontuários, (MALDONADO, 2015), a quem compete observar a qualidade dos dados inseridos no prontuário e verificar a presença dos seguintes requisitos mínimos:

> a. Identificação do paciente – nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (indicando o município e o estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP);
>
> b. Anamnese, exame físico, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado;

> c. Evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que os realizaram, assinados eletronicamente quando elaborados e/ou armazenados em meio eletrônico;
>
> d. Nos prontuários em suporte de papel é obrigatória a legibilidade da letra do profissional que atendeu o paciente, bem como a identificação dos profissionais prestadores do atendimento. São também obrigatórias a assinatura e o respectivo número do CRM;
>
> e. Nos casos emergenciais, nos quais seja impossível a colheita de história clínica do paciente, deverá constar relato médico completo de todos os procedimentos realizados e que tenham possibilitado o diagnóstico e/ou a remoção para outra unidade.

Por sua vez, a Resolução CFM nº 1.821/2007, que revogou a Resolução CFM nº 1.639/2002, trouxe respaldo legal ao uso cada vez mais frequente de sistemas informatizados de guarda e manuseio dos prontuários, o chamado prontuário eletrônico do paciente (PEP) ou ainda prontuário médico eletrônico (PME). A legislação veio a tornar possível a eliminação total de prontuários em suporte de papel, desde que garantidos padrões mínimos de segurança aos sistemas informatizados aptos a garantir a preservação integral dos dados, o que compreende o uso de certificação digital e método de indexação que permita criar arquivo organizado, possibilitando a pesquisa de maneira simples e eficiente.

Cientes da complexidade de aprofundamento dos aspectos técnicos sobre o tema, o Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) firmaram um convênio de cooperação técnica-científica para a elaboração de requisitos e avaliação da conformidade de sistemas de informação, mediante a edição contínua de manuais de certificação e expedição de selos de qualidade. O SBIS-CFM mantém em seu site cartilhas explicativas sobre a utilização de PEPs, bem como lista atualizada dos sistemas ativos certificados e auditados pelo convênio, com informações detalhas sobre o grau de segurança e as funcionalidades de cada sistema, o que denota a preocupação do setor em garantir o tráfego seguro de informações sensíveis de pacientes.

No que tange aos prontuários, a migração para sistemas de informação eletrônicos apresenta inúmeras vantagens que contribuem para a eficiência na prestação dos serviços de saúde e qualidade dos dados: maior legibilidade, acurácia, compartilhamento remoto, capacidade de processar grande volume de dados, entre outros. Porém, apesar

do ganho de eficiência da redução de custos no longo prazo, a migração demanda um complexo e custoso processo de implementação, já que os dados sensíveis não podem estar sujeitos ao armazenamento em bases de dados vulneráveis. Pesquisas indicam que a migração para prontuários eletrônicos ainda enfrenta uma série de desafios, os quais são descritos por Serpa Neto (2017) como: a falta de interoperabilidade entre os PME e outros sistemas de informação, não apenas entre diferentes sistemas, mas até dentro de um mesmo hospital ou clínica; o alto custo de sua implementação e de sua manutenção; e o impacto negativo real e/ou observado no fluxo de trabalho dos profissionais.

Apesar das barreiras técnicas e financeiras à plena migração dos estabelecimentos para sistemas eletrônicos, entende-se que a utilização das Tecnologias da Informação e Comunicação permitirão significativo salto qualitativo na prestação da saúde, de modo que há um esforço legislativo contínuo no sentido da implantação de padrões de informação e interoperabilidade entre sistemas, a permitir a melhoria e modernização dos atendimentos em saúde, bem como uma maior segurança no tratamento de dados de saúde.

O início foi dado pelo Ministério da Saúde, por meio da Portaria 2.073/2011, que definiu parâmetros de estruturação dos dados de saúde para a implementação de um Registro Eletrônico de Saúde (RES) e a interoperabilidade entre sistemas de informação do Sistema Único de Saúde (SUS) operantes em municípios, estados e União, e de saúde suplementar, com vistas ao compartilhamento de dados "em meio seguro e com respeito ao direito de privacidade" (art. 2º, II).

O RES é um registro único centrado em todo o histórico do paciente, numa forma processável eletronicamente, que possibilita o compartilhamento de informações sobre a saúde de um ou mais indivíduos, inter ou multi-instituição, dentro de uma região (município, estado ou país), ou ainda entre um grupo de hospitais, capaz de auxiliar em tomada de decisões e na formulação de políticas públicas de saúde, ao gerar dados demográficos. Segundo Araújo, Pires, Bandeira e Paiva (2014):

> Um Registro Eletrônico em Saúde (RES) define-se, inicialmente, como um conjunto de informações de saúde e assistência de um paciente durante toda a sua vida. Os registros possuem aplicações não só na assistência, como também

> em pesquisas e educação em saúde. Englobam todo tipo de informação referente ao paciente, como procedimentos, consultas, administração de medicamentos, resultados de exames e informações demográficas. Além de ser um registro centrado no paciente, um RES está baseado nas necessidades dos serviços de saúde, bem como também nos conceitos de saúde e doença de indivíduos e comunidade

O RES e o Prontuário Eletrônico diferenciam-se na medida em que o primeiro engloba apenas as informações individuais do paciente, que seriam de uso exclusivo e interno da instituição de saúde, enquanto o segundo as processa de forma longitudinal a permitir a interoperabilidade. Conforme esclarecem Araújo, Pires, Bandeira e Paiva:

> Daí a sua diferença em relação ao Prontuário Eletrônico do Paciente (PEP), que corresponde apenas às informações de saúde individuais do paciente e seu atendimento, como um registro pessoal do seu histórico de atendimentos, não possuindo base em necessidades extrínsecas ao atendimento hospitalar.

Os RES são cada vez mais utilizados, uma vez que substituem o trabalho manual de manipulação de prontuários em papel, susceptíveis a erros no seu processo de manutenção. Os RES possuem outras vantagens em relação ao prontuário em papel: o registro eletrônico pode tornar o prontuário um registro único, o que antes não era possível, tendo em vista que cada especialidade e contexto clínico desenvolvia suas próprias fichas de atendimento; um prontuário em papel não pode ser acessado em mais de um lugar ao mesmo tempo, e sua disponibilidade é limitada; por conter registros escritos manualmente, um prontuário em papel pode conter partes ilegíveis; o RES pode oferecer apoio a decisões e maior suporte à pesquisa e ao ensino em saúde. Todos estes fatores colaboram significativamente para a efetividade e eficiência dos registros, o que torna o RES uma ferramenta extremamente valiosa nos ambientes hospitalares.

Do ponto de vista da privacidade no uso dos RES, enquanto a Portaria 2.073/2011 promove a utilização de uma arquitetura de dados e tem como escopo principal a promoção da segurança no compartilhamento de informações, a Portaria nº 940/2011, que regulamenta a criação do Sistema Cartão no âmbito do SUS, traz medidas expressas sobre garantia de sigilo no tratamento de dados. Além de abordar expressamente a privacidade ao colocar como um dos objetivos do cartão SUS: “Art. 4º, III - garantir a segurança tecnológica da base de dados, respeitando-se o direito constitucional à intimidade, à vida privada, à integralidade das informações e à confidencialidade”, o Ministério da Saúde destinou um capítulo próprio para abordar a matéria do sigilo:

> CAPÍTULO V
>
> DO SIGILO DAS INFORMAÇÕES
>
> Art. 29. Os dados e as informações individuais dos usuários do SUS, captados pelo Sistema Cartão e disponibilizados de forma segura e exclusiva ao usuário devidamente identificado por meio do Portal de Saúde do Cidadão, deverão permanecer armazenados sob sigilo, pelo prazo previsto no parágrafo único do art. 11 do Decreto nº4.553, de 2002,
>
> ficando assegurado que:
>
> I - pertencem à pessoa identificada no cartão todos os dados e informações individuais registrados no sistema informatizado, que configura a operacionalização do Cartão Nacional de Saúde;
>
> II - os dados e as informações referidas são sigilosas, obrigando todos os profissionais vinculados sob qualquer forma aos sistemas de saúde a respeitar e assegurar que essas informações sejam indevassáveis;
>
> e III - são garantidas a confidencialidade, a integralidade e a segurança tecnológica, no registro, na transmissão, no armazenamento e na utilização dos dados e informações individuais. (MINISTÉRIO DA SAÚDE, 2011)

Contudo, a norma dispõe que o sigilo abarca somente os registros individualizados dos usuários, de modo que a hipótese de divulgação de dados anonimizados com informações de consolidadas ou agrupadas não é atingida pelas restrições de sigilo, consoante o artigo 30, §1º e 2º da Portaria nº 940/2011:

> § 1º As restrições à divulgação dos dados e informações do Sistema Cartão aplicam- se somente aos registros individualizados, ou seja, aqueles que permitem a identificação do beneficiário do atendimento.
>
> § 2º A divulgação de dados e informações de forma consolidada ou agrupada, desde que não permita a identificação de nenhum dos beneficiários, não é atingida pelas restrições de que trata este artigo, obedecendo-se, em todo caso, a Resolução do Conselho Nacional de Saúde (CNS) nº 196, de 10 de outubro de 1996.

Em consonância com a mencionada Portaria 2.073/2011, a Agência Nacional de Saúde (ANS), mediante as Resoluções Normativas nº 305 e 341/2012, criou o padrão TISS (Troca de Informação de Saúde Suplementar) como padrão obrigatório para troca de dados de beneficiários de planos privados de assistência à saúde no âmbito da saúde suplementar, com vistas a permitir a interoperabilidade entre os sistemas de informação das operadoras de saúde e à adoção de “normas nacionais de informação, terminologia única e identificadores unívocos”.

Dentre as finalidades do padrão TISS declaradas no artigo 3º da Resolução nº 305, estão: a padronização das ações administrativas de verificação, solicitação, autorização, cobrança, demonstrativos de pagamento e recursos de glosas; o subsídio à

ANS para acompanhamento e controle das operadoras de planos de saúde; bem como a composição do registro eletrônico dos dados de atenção à saúde dos beneficiários de planos privados de assistência à saúde.

No tocante à garantia dos direitos do titular dos dados no tratamento dos dados do padrão TISS, o artigo 14 da norma assim estabelece como requisitos de proteção de dados a garantia do direito individual ao sigilo e à confidencialidade dos dados de saúde:

> Art. 14. O componente de segurança e privacidade estabelece os requisitos de proteção dos dados de atenção à saúde.
>
> § 1º O componente de segurança e privacidade visa assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde.
>
> § 2º O componente de segurança e privacidade baseia-se no sigilo profissional e segue a legislação vigente no País.

A padronização de troca de informação vem demonstrando efetividade em operações de autorização, elegibilidade, faturamento e demonstrativos de pagamentos, porém ainda enfrenta barreiras no compartilhamento de dados assistenciais dos pacientes, devido à fragmentação do cuidado através de diversos atores. Segundo Mendes (2009):

> A maioria das informações em saúde está armazenada em prontuários de papel, espalhados pelos diversos estabelecimentos de saúde. Isso dificulta o compartilhamento e a reutilização das informações por outros profissionais de saúde. Mesmo para o próprio paciente, organizar suas informações torna-se uma tarefa quase impossível, sem a ajuda de sistemas destinados a esta finalidade.

Em relação ao tratamento de dados e requisitos de segurança para equipamentos médicos, a Agência Nacional de Vigilância Sanitária (ANVISA) editou medidas regulatórias exigindo certificação compulsória de equipamentos que visam garantir a presença de mecanismos de segurança da informação, tendo em vista a importância dos dados sensíveis que trafegam em softwares médicos, bem como a interoperabilidade entre sistemas (RDC nº 40/2015).

O fato é que o debate acerca da proteção de dados de saúde tem se intensificado com o surgimento de redes de telessaúde e desenvolvimento da telemedicina, que surgem como ferramentas importantes para o enfrentamento dos desafios contemporâneos dos sistemas de saúde universais.

Segundo Maldonado, Marques e Cruz, (2015, p.1),

> “a telemedicina conceitua- se como uso das tecnologias de informação e comunicação na saúde, viabilizando a oferta de serviços ligados aos cuidados com a saúde (ampliação da atenção e da cobertura), especialmente nos casos em que a distância é um fator crítico”.

Para a Organização Mundial da Saúde (OMS), a telemedicina deve ser entendida como a prestação de serviços de saúde, onde a distância é um fator crítico, por todos os profissionais de saúde que utilizam tecnologias de informação e comunicação para a troca de informações válidas para diagnóstico, tratamento e prevenção de doenças e lesões, pesquisa e avaliação, e para a educação continuada dos prestadores de cuidados de saúde, tudo no interesse do avanço da saúde indivíduos e suas comunidades.

No Brasil, deu-se início à utilização de ferramentas de telessaúde a partir da Rede Universitária de Telemedicina (RUTE), em 2006, com o objetivo de aproximar hospitais universitários de todo o país para fins de aprimoramento de atividades de ensino, pesquisa e reuniões clínicas entre hospitais. No mesmo ano, a Portaria MS nº 3.275/2006 criou o Conselho Brasileiro de Telemedicina e Telessaúde (CBTms).

Ato contínuo, o Ministério da Saúde instituiu o Programa Telessaúde Brasil mediante a Portaria nº 35/2007 e o ampliou com a Portaria MS nº 2.546/2011, e por meio desta última regulamentou a disponibilização aos profissionais integrantes da rede do SUS quatro tipos de serviços de telessaúde: teleconsultorias, telediagnósticos, tele-educação e segunda opinião formativa (SOF)[1].

O programa, integrado por diversos atores da saúde - gestores de saúde, instituições formadoras da saúde, núcleo técnico-científico composto por teleconsultores de corpo clínico referência e prestadores de serviços do SUS -, visa à qualificação da atenção básica espalhada pelo país ao fornecer apoio assistencial com a utilização de tecnologias da informação e comunicação, seja em tempo real online (sícrona) ou off-line respondidos em até 72 horas (assíncrona).

[1] Nas Teleconsultorias, há um canal entre profissionais de saúde/estabelecimentos com especialistas para esclarecimento de dúvidas sobre procedimentos clínicos e ações de saúde; na Tele-educação, atividades de ensino à distância visando à qualificação de profissionais da saúde; na Segunda Opinião Informativa, respostas sistematizadas obtidas com base em revisão bibliográfica, evidências científicas e perguntas originadas de teleconsultorias; no Telediagnóstico, a possibilidade emissão de laudos à distância por especialistas a partir de exames realizados por profissionais em áreas remotas (BRASIL, 2011)

No tocante à proteção dos dados produzidos em atividades de telessaúde no SUS, compete à Coordenação Nacional de Telessaúde Brasil Redes garantir a interoperabilidade e segurança das informações:

> Art. 7º Compete à Coordenação Nacional do Telessaúde Brasil Redes: [...]
> V - definir os padrões tecnológicos de interoperabilidade, conteúdo e segurança que permitirão a troca de informações entre os sistemas que viabilizam a operação do Telessaúde Brasil Redes e os diferentes sistemas de informação do SUS, incluídos o Cartão Nacional de Saúde e o Sistema de Cadastro Nacional de Estabelecimentos de Saúde (SCNES);
>
> VI - definir o conjunto de dados que fará parte do Registro Eletrônico de Saúde (RES) a partir das Teleconsultorias realizadas, visando à implementação de um registro nacional e longitudinal, conforme Portaria nº 2.073/GM MS, 2073/GM/MS de 31 de agosto de 2011; e (Retificado no DOU nº 209 de 31.10.2011, Seção 1, página 74)

Para além das inovações na comunicação entre profissionais da saúde, as tecnologias da informação e comunicação trouxeram possibilidades inovadoras para uso da telemedicina diretamente na relação profissional-paciente, tais como a teletriagem médica, a teleconsulta, telediagnóstico, telecirurgia, teleconferência de ato cirúrgico.

A atividade, que está em pleno desenvolvimento na prática, chegou a ser regulamentada pelo CFM na Resolução CFM nº 2.227, no dia 13 de dezembro 2018, cujo objetivo era permitir e regulamentar a prática da modalidade no país, entretanto, devido a um elevado número de críticas e propostas de alteração por diversas entidades médicas, além do impacto social envolvido na medida, o órgão voltou atrás e revogou seu próprio ato, a fim de amadurecer a discussão e chegar a um novo texto, que segue em debate.

Cumpre mencionar, por fim, que a prática da telemedicina deve trazer ainda mais complexidade e especificidade na regulamentação sobre dados de saúde, uma vez que o os sistemas de informação e comunicação passarão a coletar uma massiva quantidade de dados (imagem, texto e áudio) de pacientes, que necessitarão de registro e tráfego extremamente seguros, cuja realização segura depende de garantia de funcionamento, como estabilidade no fornecimento de energia elétrica e segurança eficiente contra vírus ou invasão de *hackers*.

5. Considerações Finais

Observa-se que o setor de saúde dispõe de uma vasta regulamentação sobre proteção de dados, que tem sido incrementada à medida que novas TICs são adotadas pelo setor. Ainda que não se identifique na legislação a menção expressa à categoria “dados pessoais sensíveis”, ou ainda a um regulamento específico que concentre uma sistemática de proteção a dados de maneira clara e abrangente, percebe-se que boa parte das normas trazidas pela LGPD estão contempladas pelo setor de forma esparsa.

A importância dada ao sigilo e à confidencialidade nos códigos de ética, que impõem uma série de cuidados na guarda dos registros, demonstra que a proteção à privacidade sempre balizou as atividades relacionadas à saúde, inclusive sob a dimensão da autodeterminação informativa, na medida em que há diversas obrigações e padrões mínimos relacionados à guarda dos registros clínicos e assistenciais de pacientes.

Ao traçar um paralelo com os princípios gerais listados na LGPD, é possível identificar diversos deles contemplados na legislação setorial, especialmente no tocante aos prontuários e Registro Eletrônico de Saúde: finalidade e adequação (discriminação de todos os procedimentos e informação correta ao paciente); livre acesso (vedada a negativa de acesso a prontuários); a qualidade dos dados (identificação correta e atualização constante dos dados no prontuário); a transparência (legibilidade e completude das informações), a segurança (exigências de padrões de segurança na guarda, especialmente no uso de PEPs).

O consentimento se manifesta nas atividades de saúde especialmente para garantir autonomia aos pacientes para determinar o rumo de seus tratamentos, por meio do Termo de Consentimento Livre e Esclarecido (TCLE), obrigando os profissionais a empreender esforços no sentido de fornecer informações claras, completas e precisas, de modo a corrigir a assimetria de informação. No caso da realização de pesquisas envolvendo seres humanos, o consentimento ganha ainda mais relevo, pois é possível revogá-lo a qualquer momento, pedindo a exclusão dos dados coletados na pesquisa, sem qualquer tipo de penalização.

Também é importante ressaltar que o processo de migração para sistemas eletrônicos no setor de saúde resultou em um acúmulo de regulamentos, a exemplo do Cartão SUS e da certificação ISBIS-CFM para prontuários eletrônicos, ambos com

produção extensa de manuais sobre os padrões técnicos necessários à informatização. Nesse sentido, ao passo que em alguns setores a LGPD demandará profundas transformações, no setor da saúde, devido ao estágio avançado da legislação, que contempla uma cultura de proteção a dados, bastará seguir os padrões já estabelecidos ou adaptá-los a padrões eventualmente revisados pela autoridade de dados.

Quanto ao direito à portabilidade dos dados e necessidade de se viabilizar a interoperabilidade nos sistemas eletrônicos, embora seja uma novidade em diversos setores, também se verifica que há uma extensa regulação a respeito no setor da saúde, tanto na saúde pública (RES) quanto na saúde complementar (padrão TISS), e há uma concentração de esforços no sentido de permitir maior integração entre diferentes bases de dados, visando maior eficiência na prestação de serviços. Trata-se de um desafio ainda a ser colocado plenamente em prática, dada a alta complexidade na implementação, mas que do ponto de vista regulatório também se encontra em estágio avançado de discussão.

Nesse sentido, diversas disposições da LGPD vêm apenas reafirmar e legitimar boa parte da legislação setorial existente e, ainda que demande modificações pela Autoridade Nacional de Proteção de Dados, não representaria uma total novidade ao setor.

Um impacto da lei, que certamente suprirá uma lacuna na legislação setorial, diz respeito à definição das responsabilidades entre os agentes de dados e à possibilidade de sanção administrativa e ressarcimento de danos em caso de incidentes com dados. Apesar de parte da legislação setorial prever a proteção no tratamento de dados em diversas esferas, a responsabilização em caso de dano não se dava de maneira expressa, à exceção das violações na esfera do exercício profissional, cuja responsabilidade não atingiria atos praticados por terceiro ou pela pessoa jurídica do controlador.

Conclusão

A Lei Geral de Proteção de Dados Pessoais, que inclui previsões para garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos visa permitir maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando a garantia de seus direitos e liberdades fundamentais.

A promulgação da recente lei tem como vantagens unificar e harmoziar o uso de dados pessoais em todos os setores. Nesse passo, torna o Brasil apto a processar dados oriundos de países que exigem um nível elevado proteção de dados, o que pode fomentar, principalmente, os setores da tecnologia da informação, bem como gera confiança em outras nações em relação ao tratamento de dados realizados em nosso país.

Nessa perspectiva, a lei deve ser aplicada de forma ostensiva e integrada, propiciando aos titulares dos dados pessoais o controle sobre suas informações, sobre a coleta, o tratamento, retificação, autodeterminando as informações que lhes acomete, possibilitando o acompanhamento do fluxo de seus dados.

Contudo, cabe aos titulares dos dados terem maior consciência do que pode ocorrer com seus dados pessoais e manter a cautela no uso das tecnologias disponíveis, atentando-se para os termos de uso que se utiliza, bem como verificar as configurações de privacidade, de serviços onlines e redes sociais que se utiliza, atentando-se para a possibilidade de se desativar determinadas funcionalidades dessas contas, a fim de minimizar os riscos à privacidade.

Talvez os maiores impactos trazidos pela LGPD ao setor de saúde estão em exigir maior robustez administrativa às organizações para que criem um canal de comunicação através do encarregado, bem como adotem programas de governança e *compliance* com processos e políticas internas sobre proteção de dados pessoais.

Além disso, exige que disponham de equipe qualificada apta a atender solicitações da autoridade de dados, tais como a elaboração de relatório de impacto à proteção de dados pessoais ou, eventualmente, a detecção, comunicação e mitigação de riscos em caso de incidente.

Por fim, quanto ao debate polêmico travado a respeito da telemedicina, cuja adoção deverá multiplicar a quantidade de dados coletados e demandará padrões ainda maiores de segurança, com tráfego seguro e proteção contra vírus ou *hackers*, possivelmente iniciará um novo movimento regulatório no setor, a ser norteado pela Autoridade Nacional de Proteção de Dados em conjunto com *players* e autoridades do setor.

Por fim, conclui-se, que a Lei Geral de Proteção de Dados Pessoais se apresenta, nesse sentido, como passo indispensável no caminho da proteção efetiva e do pleno exercício da autodeterminação informacional do cidadão. Implementando um controle específico da circulação de informações, trazendo segurança jurídica necessária ao desenvolvimento da cultura de tutela de dados pessoais relacionados à saúde dos cidadãos brasileiros.

Referências

AGÊNCIA NACIONAL DE SAÚDE (ANS). **Resolução Normativa nº 305**, de 09 de outubro de 2013. Esta Resolução estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde; revoga a Resolução Normativa - RN nº 153, de 28 de maio de 2007 e os artigos 6º e 9º da RN nº 190, de 30 de abril de 2009. .Disponível em: <http://www.ans.gov.br/component/legislacao/?view=legislacao&task=PDFAtualizado&format=raw&id=MjYyMQ=> Acesso em: 10 nov. 2020.

AGÊNCIA NACIONAL DE SAÚDE (ANS). **Resolução Normativa nº 341**, de 27 de Novembro de 2013. Altera a Resolução Normativa RN n. 305 de 09 de outubro de 2012 que estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde e revoga a Resolução Normativa - RN nº 153, de 28 de maio de 2007 e os artigos 6º e 9º da RN nº 190, de 30 de abril de 2009. Disponível em: <http://www.ans.gov.br/component/legislacao/?view=legislacao&task=PDFAtualizado&format=raw&id=MjYyMQ=> Acesso em: 10 nov. 2020.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Resolução RDC nº40**, de agosto de 2015. Define os requisitos do cadastro de produtos médicos. Disponível em: http://www.sbpc.org.br/upload/conteudo/anvisa_rdc40_27ago2015.pdf. Acesso em: 01 nov. 2020.

ARAUJO TV, PIRES SR, BANDEIRA PAIVA. P. Adoção de padrões para Registro Eletrônico em Saúde no Brasil. **Revista Eletrônica de Comunicação Informação &**

Inovação em Saúde [Internet]. 2014 dez. Disponível em: <http://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/440> Acesso em: 01 nov. 2020.

BRAGANÇA, C.E.B.A.; LUCIANO, E.M.; TESTA, M.G. **Segurança da Informação e privacidade de informações de pacientes de instituições de saúde:** uma análise exploratória da privacidade percebida pelos profissionais. In: ENCONTRO DA ANPAD, 34., Rio de Janeiro, 25-29 set. 2010. Disponível em: <http://www.anpad.org.br/admin/pdf/adi2653.pdf>. Acesso em: 01 nov. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD) Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 01 nov. 2020.

BRASIL. **Medida Provisória nº 869**, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm#art1>. Acesso: 03 nov. 2020.

BRASIL. MINISTÉRIO DA SAÚDE. **Portaria nº 940, de 28 de abril de 2011**. Regulamenta o Sistema Cartão Nacional de Saúde (Sistema Cartão). Disponível em < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html>. Acesso: 22 nov. 2020.

BRASIL. MINISTÉRIO DA SAÚDE. **Portaria nº 2.546, de 27 de outubro de 2011**. Redefine e amplia o Programa Telessaúde Brasil, que passa a ser denominado Programa Nacional Telessaúde Brasil Redes (Telessaúde Brasil Redes). Disponível em < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2546_27_10_2011_comp.html>. Acesso: 22 nov. 2020.

BRASIL. MINISTÉRIO DA SAÚDE. Portaria nº 2.073, de 31 de agosto de 2011. **Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar**. Disponível em <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html>. Acesso: 01 nov. 2020.

BRASIL, **País Digital.** Disponível em: <https://brasilpaisdigital.com.br/casos/#saude> Acesso em: 03 nov. 2020.

CONJUR. DALLARI, Analluza Bolivar. **Impactos da nova Lei Geral de Proteção de Dados na pesquisa com seres humanos**. Disponível em <https://www.conjur.com.br/2018-nov-02/analluza-dallari- impactos-lgpd-pesquisa-seres-humanos>; Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE EDUCAÇÃO FÍSICA. **Resolução CONFEF nº 207/2015**. Dispõe sobre o Código de Ética dos Profissionais de Educação Física registrados no Sistema CONFEF/CREFsDisponível em: https://www.confef.org.br/confef/resolucoes/381>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE ENFERMAGEM. **Resolução COFEN nº564/2017**. Aprova o novo Código de Ética dos Profissionais de Enfermagem. Disponível em: < http://www.cofen.gov.br/resolucao-cofen-no-5642017_59145.html>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE FISIONTERAPIA E DE TERAPIA OCUPACIONAL. **Resolução Nº424**, DE 08 DE JULHO DE 2013 – Estabelece o Código de Ética e Deontologia da Fisioterapia. Disponível em: < https://www.coffito.gov.br/nsite/?p=3187> . Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.638/2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde.. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.821/2007.** Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em: < http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.pdf>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 2.227/2018**. Aprova o Código de Ética Médica. Disponível em: <https://portal.cfm.org.br/images/PDF/resolucao222718.pdf>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE MEDICINA. **Cartilha sobre prontuário eletrônico:** a certificação de sistemas de registro eletrônico de saúde¸ fev. 2012. Disponível em: <http://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012 .pdf>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE MEDICINA. **Recomendação CFM nº 01/2016**. Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. Disponível em: <https://www.ghc.com.br/files/Sobre%20Consentimento%20Informado.pdf>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE NUTRICIONISTAS. **Resolução CFN nº 599/2018**. Aprova o Código de Ética e de Conduta do Nutricionista e dá outras providências. Disponível em: < http://www.cfn.org.br/wp-content/uploads/2018/04/codigo-de-etica.pdf>. Acesso em: 01 nov. 2020.

CONSELHO FEDERAL DE ODONTOLOGIA. **Resolução CFO nº118/2012**. Disponível em: < http://cfo.org.br/website/wp-content/uploads/2018/03/codigo_etica.pdf> . Acesso em: 01 nov. 2020.

CONSELHO FEDERAL PSICOLOGIA. **Resolução CFP nº018/2005.** Disponível em: < https://site.cfp.org.br/wp-content/uploads/2012/07/Co%CC%81digo-de-%C3%89tica.pdf> . Acesso em: 01 nov. 2020.

JOTA. FRAZÃO Ana. **Nova LGPD**: o tratamento dos dados pessoais sensíveis. Disponível em < https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018> Acesso em: 01 nov. 2020.

JOTA. MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada- 14072018>. Acesso em: 03 nov. 2020.

KAMEDA, Koichi; PAZELLO, Magaly. **E-Saúde e desafios à proteção da privacidade no Brasil** In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB, organizadores. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde; 2015. p. 50-61. Disponível em: <https://www.researchgate.net/publication/314090227_E-Saude_e_desafios_a_protecao_da_privacidade_no_Brasil>. Acesso em: 03 nov. 2020.

LIMA, Cíntia Rosa Pereira de. BIONI, Bruno Ricardo. **A proteção dos dados pessoais na fase de coleta**: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do Marco Civil da Internet a partir da human computer interaction e da privacy by default. In Direito & Internet III: Marco Civil de Internet. Quartier Latin, 2015.

LIMA, Cíntia Rosa Pereira. **Parecer Técnico** encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima; 2017. Disponível em <https://www2.camara.leg.br/atividade-legislativa/comissoes/com;issoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp >. Acesso em: 01 nov.2020.

MALDONADO, José Manuel Santos; MARQUES, Alexandre; CRUZ, Antonio. **Telemedicina**: desafios à sua difusão no Brasil. Caderno de. Saúde Pública, vol.32, supl.2. Rio de Janeiro, 2016. Disponível em < http://dx.doi.org/10.1590/0102-311X00155615> . Acesso: 21 nov. 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Edição do Kindle.

MENDES, Simone Fabiano. et al. Uma análise da implantação do padrão de troca de informação em saúde suplementar no Brasil. **Journal of Health Informatics**, v. 1, n. 2, 2009. Disponível em: http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/view/86/97 . Acesso em 02 nov. 2020.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). TELEMEDICINE: **Opportunities and developments in Member States**. 2011. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/44497/9789241564144_eng.pdf;jsessionid=A 23134BA23154B4A2F129E694906E6F3?sequence=1 Acesso em: 22 nov. 2020.

SARLET, Ingo. KEINER Tania Margarete. O direito fundamental à privacidade e as informações em saúde: alguns desafios. In: Keinert TMM, Sarti FM, Cortizo CT, Paula

SHB, organizadores. **Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética.** São Paulo: Instituto de Saúde; 2015. Disponível em: <https://scielosp.org/article/csp/2018.v34n7/e00039417/pt/> Acesso em: 03 de nov. 2020.

SERPA NETO. Et al. **Prontuários Médicos eletrônicos: análise secundária para melhorar o atendimento ao paciente. TIC Saúde.** Pesquisa Sobre o Uso de Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros. Núcleo de Informação e Comunicação do Ponto BR; 2017. Disponível em: https://www.nic.br/media/docs/publicacoes/2/tic_saude_2017_livro_eletronico.pdf . Acesso em 01 nov. 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679** do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679> . Acesso em: 01 nov. 2020.

UNIÃO EUROPEIA**. Diretiva 2011/24/UE** do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).

VILLAS-BOAS, Maria Elisa. **O direito-dever de sigilo na proteção ao paciente.Revista Bioética**, 2015; 23 (3): 513-23. Disponível em < http://dx.doi.org/10.1590/1983-80422015233088>. Acesso em: 01 nov. 2020