Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Jurisprudência e legislação sanitária comentadas
Lei Geral de Proteção de Dados e segurança da informação na área da saúde

Jurisprudence and health law
General Data Protection Law and information security in healthcare

Jurisprudencia y legislación sanitária
Ley General de Protección de Datos y seguridad de la información en el ámbito de la salud

Renata Salgado Leme[1]

Marcelo Blank[2]

Resumo
Objetivo: análise descritiva e explicativa da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, em especial no aspecto do direito à saúde e suas implicações na segurança do tratamento dos dados decorrentes da revolução tecnológica. **Metodologia**: pesquisa exploratória de caráter bibliográfico e documental, com base em livros, artigos, legislações e documentos. **Resultados:** a investigação demonstrou que a difusão do uso dos meios digitais na área da saúde e da medicina expõe o paciente, titular das informações, seja pela negligência no tratamento, seja pela comercialização indevida ou pelo vazamento dos dados. **Conclusão:** o estudo aponta ser imprescindível o consentimento qualificado do titular dos dados sensíveis para o seu tratamento, bem como o uso de sistemas digitais seguros como meios de salvaguardar os direitos fundamentais da pessoa, alertando o profissional e as instituições de saúde para a necessidade urgente de se adequar à Lei Geral de Proteção de Dados.
Palavras-chave: Saúde. Medicina. Paciente. Proteção de dados.

Abstract
Objectives: descriptive and explanatory analysis of the General Data Protection Law, Law n. 13.709/2018, especially in the aspect of the right to health and its implications for the security of data processing resulting from the technological revolution. **Methods:** exploratory research of bibliographic and documentary character based on books, articles and documents. **Results:** the investigation showed that the widespread use of digital media in the area of health and medicine exposes the information holder (patient), either due to negligence in treatment, or due to improper commercialization or data leakage. **Conclusion:** the study points out that the qualified consent of the holder of sensitive data is essential for its treatment, as well as the use of secure digital systems as a means of safeguarding the fundamental rights of the person, alerting professionals and health institutions to the urgent need to comply with the General Data Protection Law.
Keywords: Health. Medicine. Patient. Data protection.

[1] Doutora em Filosofia e Teoria Geral do Direito, Universidade de São Paulo, São Paulo, SP, Brasil; professora titular, Universidade Santa Cecília, Santos, SP, Brasil. http://orcid.org/000-0003-2298-9975. E-mail: renataleme@aasp.org.br
[2] Especialista em Direito para Startups FGV, São Paulo, SP, Brasil; diretor de TI e *compliance*, Blank Sistemas, Consultoria e Desenvolvimento de Sistemas, São Paulo, SP, Brasil. http://orcid.org/0000-0002-7938-8751. E-mail: mablankg@gmail.com

Resumen
Objetivos: análisis descriptivo y explicativo de la Ley General de Protección de Datos, Ley n° 13.709/2018, especialmente en el aspecto del derecho a la salud y sus implicaciones para la seguridad del tratamiento de datos producto de la revolución tecnológica. **Metodología:** investigación exploratoria de carácter bibliográfico y documental a partir de libros, artículos y documentos. **Resultados:** la investigación mostró que el uso generalizado de los medios digitales en el área de la salud y la medicina expone al titular de la información (paciente), ya sea por negligencia en el tratamiento, bien por mala comercialización o fuga de datos. **Conclusión:** el estudio señala que el consentimiento calificado del titular de los datos sensibles es fundamental para su tratamiento, así como el uso de sistemas digitales seguros como medio de salvaguardar los derechos fundamentales de la persona, alertando a los profesionales e instituciones de salud de la urgente necesidad para cumplir con la Ley General de Protección de Datos.
Palabras clave: Salud. Medicina. Paciente. Protección de datos.

Introdução

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), publicada em 14 de agosto de 2018 (1), é inspirada na legislação europeia[3] e busca instituir um maior rigor na regulamentação da proteção de dados, ao resguardar de maneira mais efetiva os direitos fundamentais[4] de liberdade, privacidade e autonomia informativa, cuja tutela individual e social é vital para a consolidação do regime democrático nas sociedades contemporâneas. É notório que o ordenamento jurídico brasileiro não era destituído de instrumentos regulatórios de proteção de dados, no entanto, existiam leis setoriais e especiais[5], desprovidas de uma sistematização capaz de fornecer um paradigma tanto ao setor privado quanto público, orientado por princípios, categorias e institutos gerais e específicos aplicáveis à matéria.

A LGPD estava programada para entrar em vigor em agosto de 2020, todavia, com o advento da pandemia da Covid-19, houve a edição da Medida Provisória nº 959/2020 (2), publicada no D.O.U. em 29 de abril 2020, prorrogando o início da sua vigência para 03 de maio de 2021. No entanto, o Ministério Público Federal, em nota técnica enviada ao Congresso Nacional, em 14/04/2020, manifestou-se contrário a qualquer iniciativa com o objetivo de postergar a entrada em vigor da LGPD, destacando a importância do estatuto legal no contexto da pandemia da Covid-19:

[3] O Regulamento Europeu de Proteção de Dados (GDPR) entrou em vigor em maio de 2018.
[4] O reconhecimento do direito à proteção de dados pessoais decorre da tutela constitucional da pessoa humana e de sua dignidade, conforme dispõe o art. 1º, inciso III, da Constituição Federal de 1988.
[5] A título ilustrativo, citamos a Lei nº 12.257/2011, ou Lei de Acesso à Informação; a Lei nº 12.737/2012 (Lei Carolina Dieckmann); e a Lei nº 12.965/2014 (Marco Civil da Internet).

> A LGPD é uma importante aliada no desenvolvimento seguro e parametrizado de ações fundamentais para a proteção à saúde, isolamento social e colaboração com atores estrangeiros, na troca de dados essenciais para o enfrentamento da crise. (3)

O Projeto de Lei nº 1.179/2020 (4) estava em tramitação no Congresso Nacional, originário do Senado Federal, e previa a vigência da Lei a partir de agosto de 2020, mas ressalvava que as multas e as sanções somente poderiam ser aplicadas a partir de agosto de 2021.Ffinalmente, em 17 de setembro de 2020, o Presidente da República sancionou a Lei referente à Medida Provisória nº 959 (2) e a LGPD entrou em vigor em 18 de setembro de 2020, com sanções aplicáveis a partir de agosto de 2021.

O objeto da LGPD é a proteção de dados de qualquer pessoa natural, identificada ou passível de identificação, cujas informações sejam tratadas por controladores e/ou operadores na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração da informação. Os principais objetivos do estatuto legal são garantir a transparência no uso dos dados das pessoas; proteger os usuários e coibir o uso indevido, abusivo ou discriminatório dos seus dados, resguardando os direitos fundamentais da pessoa humana. Cabe destacar que a LGPD, cuja principal característica é sua natureza conceitual, trouxe inúmeras inovações nesse campo, dentre elas a definição de *dado pessoal sensível*.

Sendo assim, o presente estudo tem por finalidade aprofundar a análise do conceito *dado pessoal sensível* relativo ao tratamento e à segurança das informações concernentes à saúde das pessoas. Ademais, busca evidenciar as particularidades da proteção de dados pessoais sensíveis no âmbito da saúde – dados genéticos, sanitários, sexuais etc –, bem como a necessidade de se adotar mecanismos e ferramentas de segurança da informação (*health tech*) capazes de garantir a proteção ou, ao menos, reduzir substancialmente os riscos de eventual vazamento destes dados.

A proposta do estudo, mais do que oferecer respostas definitivas para assegurar o não vazamento dos dados pessoais sensíveis dos pacientes na esfera da saúde individual e coletiva, seja no setor público quanto privado, é destacar a importância da questão relativa à segurança da informação e alertar os profissionais da área da saúde para a necessidade de se adequar à nova Lei tanto no plano jurídico-normativo quanto tecnológico.

Dados Pessoais Sensíveis: conceito e fundamento

A LGPD estatuiu no seu art. 5º, inciso II, que *dado pessoal sensível* é

> [...] dado pessoal sobre origem racial e 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 [...]". (1)

Destaca-se que o rol apresentado nessa definição não é taxativo, enumerando, de maneira apenas exemplificativa, algumas hipóteses em que os dados pessoais são considerados sensíveis, dando margem às interpretações extensivas. Trata-se de rol meramente ilustrativo, constituindo uma amostra oferecida pelo legislador com a finalidade de esclarecer o conceito.

Segundo Doneda (5) dados sensíveis "seriam determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva" ou, ainda, de acordo com Bioni (6) seriam "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação." Os dados pessoais sensíveis, entretanto, não são assim classificados tão-somente pela sua natureza intrinsecamente personalíssima, mas também devido ao uso e à finalidade que são outorgados a eles por meio do seu tratamento. Infere-se, portanto, que um dado comum, trivial ou até ordinário pode se transformar em um dado sensível quando há ferramentas tecnológicas capazes de estabelecer relações e correlações entre os mesmos, permitindo a previsibilidade de condutas, comportamentos, ações, ocorrências e acontecimentos.

Como é sabido, as ações dos usuários nas plataformas e ambientes digitais produzem informações que podem ser organizadas e compiladas com base em algoritmos matemáticos, originando o que se denomina *big data*.

O uso de *big data* tem crescido significativamente em todas as áreas científicas, inclusive na saúde. Destacam-se alguns setores da saúde no Brasil nos quais a utilização de *big data* é promissora: medicina de precisão, prontuários eletrônicos e internet das coisas (7). Todavia, não se pode esquecer de mencionar uma outra área em crescente expansão, a telemedicina, prática regulada pelo Conselho Federal de Medicina, por meio da Resolução nº 1.643/2002 (8) e que ganhou evidência com a propagação da pandemia da Covid-19, com a edição da Lei nº 13.989/20 (9).

A difusão do uso da internet, de forma ilimitada no tempo e no espaço, conduziu ao crescimento da quantidade e da diversidade de informações que podem ser combinadas e relacionadas, ampliando consideravelmente o risco de re-identificação dos dados, mesmo após a sua anonimização ou desidentificação de bases isoladas. Dessa forma, a LGPD terá um grande impacto no *big data*, visto que a obtenção de informações pessoais por meio do tratamento de dados, sem que sejam observados os paradigmas ali instituídos, poderão gerar danos aos indivíduos, ferindo gravemente a privacidade, a liberdade e a autonomia dos mesmos, ou seja, os pilares da nova lei. Nesse sentido, pode-se evidenciar o instituído no artigo 20 do referido estatuto, que declara que o titular dos dados tem o direito de solicitar revisão de decisões tomadas, unicamente em tratamento automatizado de dados pessoais e que afetem seus interesses (podendo ser técnicas de *big data*) como, por exemplo, perfil profissional, consumo, crédito, personalidade, o que pode gerar conseqüências jurídicas negativas para as empresas e para os profissionais considerados controladores ou operadores desses dados.

A LGPD adota como fundamento para o tratamento de dados pessoais o consentimento do titular, estabelecendo no seu artigo 5º, inciso XII, que o tratamento de informações pessoais está condicionado à manifestação livre, informada e inequívoca do titular, que deverá concordar com o tratamento de seus dados pessoais para uma finalidade específica (1). E, em se tratando de consentimento para o tratamento de dados pessoais sensíveis, a lei prescreve a necessidade de que ele seja feito de forma determinada e destacada, indicando a(s) finalidade(s) de maneira expressa (artigo 11, inciso I) (1). Isso significa que a manifestação de vontade genérica é vedada pela lei, sendo ilegítima e inválida a declaração de vontade que não esteja relacionada ao(s) objetivo(s) específico(s) para seu tratamento.[6]

A justificativa para o consentimento qualificado, no que tange ao tratamento dos dados sensíveis, deve-se à natureza dos seus conteúdos, que demandam um cuidado especial, em particular os dados de natureza médica, genética, sexual, devendo ser salvaguardados como meio de garantir o pleno exercício dos direitos fundamentais da pessoa. Ademais, conforme o caput do artigo 8º, o consentimento previsto no inciso I do

[6] Artigo 8º, parágrafo 4º, da LGPD – “O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas”.

artigo 7º da LGDP deverá ser fornecido por escrito, de maneira expressa, ou por outro meio que demonstre a manifestação da vontade do titular.

O consentimento só será válido se as informações fornecidas ao titular dos dados sejam apresentadas com transparência, de forma clara e inequívoca. Se houver mudança da finalidade para o tratamento dos dados pessoais, o controlador deverá informar previamente o detentor das informações acerca das alterações da finalidade, podendo o titular revogar o consentimento, caso discorde da modificação de finalidade de tratamento, consoante previsto no artigo 9ª, parágrafos 1º e 2º da LGPD (1). Há também previsão legal para a revogação do consentimento a qualquer momento, mediante manifestação expressa do titular das informações, consoante estabelecido no artigo 9º, parágrafo 5º.

O artigo 11 da LGPD, entretanto, prevê situações excepcionais que permitem o tratamento de dados sensíveis sem a necessidade do consentimento do titular, por exemplo, com o fim de cumprir obrigação legal ou regulatória pelo controlador; para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis e regulamentos; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados; a fim de proteger a vida ou a incolumidade física do titular ou de terceiro; com a finalidade de tutelar a saúde, em procedimentos realizados por profissionais da área ou por entidades e autoridades sanitárias. Ressalte-se, ainda, que a lei também prevê a garantia da prevenção à fraude e proteção da segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º do referido estatuto legal.

Saúde e tecnologia

Uma revolução está em curso na saúde e na medicina com a introdução crescente e acelerada da tecnologia. Como exemplo, podemos citar a telerradiologia que, por meio da internet, captura as imagens de um exame de raio-x ou de ressonância magnética, as quais são enviadas em segundos para uma central de telerradiologia. A partir dessas imagens, os profissionais habilitados elaboram os laudos, que são imediatamente disponibilizados para os consultórios, as clínicas e os hospitais.

A telemedicina foi regulamentada pelo Conselho Federal de Medicina, por meio da Resolução nº 1.643/2002 (8), possibilitando a realização da videoconferência entre os

médicos para a discussão de casos e a troca de opiniões. Entretanto, com a edição da Lei nº 13.989/20 (9), o CFM reconheceu a possibilidade e a eticidade de uso da telemedicina, enquanto perdurar o combate à Covid-19, além do que está estabelecido na Resolução nº 1.643/2002 (8), que continua em vigor. Esse novo entendimento do CFM[7] (10) prevê que a telemedicina poderá ser usada nos seguintes moldes: teleorientação, permitindo que os médicos realizem à distância a orientação e o encaminhamento de pacientes em isolamento; telemonitoramento, permitindo que, sob supervisão e orientação médicas, sejam monitorados à distância a saúde e/ou doença de pacientes; teleinterconsulta, possibilitando a troca de informações e opiniões exclusivamente entre médicos, para auxílio diagnóstico ou terapêutico.

Segundo Chiavegatto, Kawaschi e Gotlieb (11), uma vultosa parte do conhecimento científico é fundada em grandes médias. Por exemplo, quando uma pesquisa conclui que o uso de determinado medicamento oral diminui o risco de acidente vascular cerebral e de eventos embólicos sistêmicos em 19%, isso significa que algumas pessoas tiveram o risco diminuído em 100% (não tiveram nenhum desses eventos) e as outras em 0% (tiveram pelo menos um desses eventos). Podemos inferir, portanto, que não se sabe para quais pessoas o medicamento não funciona.

Mas a revolução digital na medicina caminha adiante. O objetivo do desenvolvimento da medicina de precisão é possibilitar a prescrição do medicamento somente para aqueles indivíduos para os quais o fármaco funcione efetivamente. Assim, para se alcançar essa precisão, será imprescindível aumentar o tamanho das amostras das pesquisas, a fim de que elas representem o universo estudado de maneira fidedigna.

A digitalização do maior número de informações dos pacientes pelos serviços de saúde é fundamental para se avolumar o tamanho e o detalhamento das amostras, e é outra tendência importante para a organização, atualização e transferência de dados.

A universalização da digitalização dos prontuários no Brasil é essencial, porém insuficiente, para se promover o avanço na atenção à saúde dos cidadãos e no desenvolvimento da pesquisa científica na área da saúde. Além da implantação do prontuário eletrônico do paciente (PEP) será necessário possibilitar o uso remoto do

[7] Ofício CFM nº 1756/2020 – COJUR, encaminhado ao Ministro de Estado da Saúde Luiz Henrique Mandetta, em 19/03/2020, pelo presidente do CFM Mauro Luiz de Brito Ribeiro.

prontuário por todos os estabelecimentos de saúde, ou seja, facilitar o uso integrado dessa base de dados.

Outro campo para o uso de *big data* é a internet das coisas (*internet of things),* ou seja, todos os objetos estarão conectados entre si por meio da internet, ou, ainda, a possibilidade de uso de objetos eletrônicos conectados ao corpo das pessoas. O volume e o detalhamento dos dados gerados pela internet das coisas serão imensamente úteis para a área da saúde, que poderá identificar as causas e as concausas das doenças, dos acidentes, com a finalidade de agir preventivamente, mitigar riscos e definir com maior precisão as condutas e os tratamentos.

A ampliação e a difusão das bases de dados, contudo, torna o titular das informações cada vez mais vulnerável, seja pela negligência na coleta, uso, compartilhamento, armazenamento ou descarte dos dados, seja pela comercialização indevida ou vazamento das informações. Logo, o desenvolvimento do planejamento e gerenciamento de riscos é indispensável para salvaguardar a confidencialidade, a integridade e a segurança das informações.

Segurança da informação

Dentro das organizações, as informações ou dados são coletados, manipulados e processados por três figuras distintas: o controlador, responsável pelo tratamento da informação; o operador, que executa as ordens do controlador em relação ao processamento das informações e o oficial de dados (*data protection officer*[8]*, ou DPO, na sigla em inglês*), responsável pela execução das diretrizes definidas pelo controlador e operador. (1)

O controlador é obrigado a implantar medidas técnicas e organizacionais apropriadas para assegurar que o processamento das informações seja executado de acordo com o artigo 46 da LGPD, ou seja, impedir “acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” (1). Já os operadores e os oficiais de dados (DPO), como agentes de execuções das políticas definidas pelos controladores, devem, de acordo com o artigo 47, “obrigar-se a garantir a segurança da informação prevista na lei em relação aos dados pessoais, mesmo após o seu término” (1).

[8] *Data protection officer* (DPO) é o profissional que, dentro de uma empresa, entidade ou instituição é encarregado de cuidar das questões relativas à proteção dos dados da organização e de seus clientes.

Com relação ao tratamento de dados, o estatuto legal, no seu artigo 50, concede liberdade para a formulação e definição de

> [...] regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (1).

O mesmo artigo ainda define como as regras devem ser implementadas e integradas no processo de tratamento de dados e governança da empresa, bem como as informações devem ser apresentadas à Autoridade Nacional de Proteção de Dados. Para tanto, um programa de governança em privacidade deve ser estruturado sob os seguintes pilares: transparência; gestão de riscos; adaptação à realidade; dimensão do tamanho e volume das operações da organização; governança com controles e monitoramento; monitoramento contínuo; efetividade do programa; aplicação de boas práticas, elaboração de código de conduta, com políticas e procedimentos e atualização periódica.

Mesmo com as definições de funções e elaboração de regras de controle das informações, ainda existe um risco no processo de tratamento de dados efetuado pelas organizações, que são os sistemas que processam estes dados. Neste aspecto, a LGPD, em seu artigo 49, define que os

> [...] sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (1)

Esse é um dos pontos mais críticos para todas as empresas e organizações que tratam dados pessoais, sobretudo nas de pequeno porte, que não realizam políticas de *compliance*. O *compliance* faz parte da estrutura de governança corporativa e tem como proposta aperfeiçoar o modelo de gestão da organização por meio da prevenção, monitoramento e mitigação de riscos. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD. Sendo assim, os novos sistemas deverão ser desenvolvidos já baseados nos conceitos de *privacy by design* e *privacy by default*.

Privacy by design (privacidade por design) significa que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma empresa devem zelar pela privacidade, em primeiro lugar. Ou seja, o conceito de privacidade deve estar totalmente inserido no projeto original, desde o início do seu desenvolvimento (12). O conceito de *privacy by default* (privacidade por padrão) significa que um produto ou serviço, ao ser lançado no mercado, deve vir com as configurações de privacidade no modo mais restrito possível por padrão e o usuário deve liberar acesso à coleta de mais informações, caso julgue necessário (12).

Os agentes de tratamento devem, portanto, desde a concepção do produto ou do serviço, até a sua execução, adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (artigo 46, II). (1)

Dado este cenário inicial de segurança de dados, baseado na LGPD, avançamos para o aspecto mais relevante, a proteção de dados em sistemas de *businnes inteligence*. Por meio deste sistema os dados do *big data* – que constituem um alto volume de informações virtuais, complexas, diversas, heterogêneas, provenientes de fontes variadas, autônomas, independentes e que apresentam controles distribuídos e descentralizados – são aplicados a um resultado com a extração de informações úteis sobre a massa de dados coletados (13).

Como exemplo, temos a *DeepMind* (14), *startup* adquirida pela gigante *Google*, que é formada por equipes de cientistas, engenheiros, especialistas em aprendizado de máquinas e outros profissionais, os quais trabalham para avançar o estado da arte em inteligência artificial, definida como a utilização dos padrões extraídos do *big data* que, por meio de algoritmos, consegue prever determinado comportamento ou resultado, utilizando as tecnologias para benefício do público em geral e também para alavancar as descobertas científicas (15).

Assim como a engenharia de *software* possui um conjunto de práticas recomendadas para segurança e confiabilidade, as equipes de segurança de inteligência artificial desenvolvem abordagens de especificação, robustez e garantia para sistemas de inteligência artificial, agora e no futuro. Outra empresa em destaque é a Babylon, que tem como missão disponibilizar um serviço de saúde acessível a todas as pessoas do planeta. A inteligência artificial foi projetada com base no cérebro de um médico, a fim de fornecer

assistência médica acessível a milhões de pessoas, por meio de um aplicativo que captura os dados fornecidos pelos usuários, como sintomas e dores que estão sentindo e, com um *bot*[9], são feitas questões de anamnese até que o sistema identifique o provável diagnóstico e indique um médico online para a realização de vídeoconsulta. A empresa possui operações nos EUA, Reino Unido, Canadá, Ruanda e vários países da APAC (Ásia-Pacífico ou Ásia Pacífico)[10] e do Oriente Médio, bem como planos de expansão em andamento com os principais provedores de saúde dos EUA, América do Sul e EMEA (*European Medicine Agency*).

A preocupação com segurança de dados é fundamental para o sucesso e a credibilidade do empreendimento o que fez a organização detalhar na sua página de política de privacidade (*privacy policy*) a maneira pela qual faz o armazenamento dos dados, destacando que adotam os seguintes protocolos:

a. não armazenam os dados pessoais de saúde em seu dispositivo móvel, optando por armazenar todos os dados pessoais de saúde, incluindo as informações de cuidados primários, informações sobre medicamentos e informações sobre diagnóstico, em servidores seguros;

b. não armazenam informações de cartão de crédito ou débito, alertando que os pagamentos são processados por meio de um provedor de pagamento terceirizado, que é totalmente compatível com os padrões de segurança de dados do nível 1 do setor de cartões de pagamento (PCI), e todas as transações de pagamento são criptografadas usando a tecnologia SSL;

c. criptografam os dados transmitidos de e para o aplicativo e, depois de receber as informações, usam procedimentos estritos e recursos de segurança para tentar impedir o acesso não autorizado, asseverando que tomarão todas as medidas, razoavelmente necessárias, para garantir que os dados sejam tratados com segurança e de acordo com a política de privacidade;

d. esclarecem que os dados podem ser processados ou armazenados em destinos fora do Reino Unido e do Espaço Econômico Europeu (EEA), mas sempre de acordo com a

[9] *Bot* são robôs (algoritmos) que, por meio de perguntas respondidas pelos usuários conseguem enviar respostas, utilizam inteligência artificial e são as interfaces entre os sistemas e os usuários.
[10] É a parte do mundo dentro ou próxima do Oceano Pacífico Ocidental, incluindo grande parte da Ásia Oriental, Sul da Ásia, Sudeste da Ásia e Oceania.

lei de proteção de dados, incluindo mecanismos para transferência legal de dados, através das fronteiras e sujeitos a rigorosas salvaguardas. (16)

Os principais aplicativos de análise de *big data*, como o *Microsoft Power BI*, o *Tableut da Sales Force* e o *Qlick View*, entre outros, possuem políticas de privacidade de dados bem definidas, mas, em se tratando de ferramentas de desenvolvimento pelo usuário final, consumindo dados próprios ou de terceiros, o responsável pelo processamento das informações será sempre o controlador ou o operador pelo tratamento dos dados, cabendo ao desenvolvedor da solução os cuidados em relação a segurança dos acessos do software final e de proteção de acessos.

Conclusão

A proteção dos dados pessoais sensíveis é um dos temas mais desafiadores da atualidade.

A acelerada revolução tecnológica em curso, o crescente aumento do volume dos dados e das informações tratados por diversos atores sociais (organizações, entidades, instituições etc.), públicos e privados, podem ocasionar problemas de ordem ética que afetam a liberdade, privacidade e autonomia dos indivíduos.

Sendo assim, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) –, foi editada com o objetivo de garantir a transparência no uso dos dados das pessoas físicas; assegurar a privacidade dos titulares das informações; bem como coibir o uso abusivo e discriminatório destes dados. O alcance de tais propósitos, no entanto, está condicionado ao desenvolvimento de regras e mecanismos de segurança da informação. A adequação à LGPD com a observância do princípio da finalidade, a coleta de dados específicos para o tratamento das informações, o consentimento livre, expresso e informado manifestado pelo dono dos dados são alguns dos paradigmas que devem ser seguidos. Além disso, no que tange à segurança da informação, pode-se ressaltar que os sistemas devem ser projetados com base em conceitos de *privacy by design* e *privacy by default*. Há, ainda, o desafio de desenvolver a segurança e proteção de dados em sistemas de *businnes inteligence* e de *inteligência artificial*.

Ante a complexidade do tema, destaca-se a necessidade daqueles que controlam e/ou operam dados pessoais sensíveis de serem zelosos na escolha de ferramentas e

plataformas, observando a segurança e confiabilidade destas, que podem ser aferidas por meio da transparência da política de privacidade adotada para o tratamento dos dados.

O aperfeiçoamento da governança corporativa é, portanto, imprescindível para a adequação à lei e para a implantação de ferramentas que garantam a segurança dos dados, tendo como proposta aperfeiçoar o modelo de gestão das organizações por meio da prevenção, monitoramento e mitigação de riscos

Por todo o exposto, recomenda-se aos profissionais da área da saúde, bem como às entidades e instituições do setor, adotar as melhores práticas no que diz respeito à proteção de dados dos pacientes, com o escopo de assegurar a confiabilidade e integridade das ações destes atores perante os cidadãos, evitando condutas ilegais que possam resultar na aplicação das sanções previstas no artigo 52 da LGPD.

Referências

1. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018 [Acesso em 12.jun.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

2. Brasil. Medida Provisória nº 959, de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a *vacatio legis* da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. (institui regras para o auxílio emergencial e adiamento da LGPD). Brasília, DF: Presidência da República; 2020 [Acesso em 12.jun.2020]. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753

3. Brasil. Ministério Público Federal. Nota técnica conjunta PFDC & Câmara Criminal, Epidemia covid-19 e PLS (Substitutivo) 1179/20: manutenção do prazo de entrada em vigor da LGPD (ressalvadas as sanções administrativas), de 14 de abril de 2020. Brasília, DF; 2020 [Acesso em 12.jun.2020]. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas/notas-tecnicas-1/2020/pr-sp-00039100-2020_nota_tecnica.pdf

4. Brasil. Senado Federal. Projeto de Lei nº 1.179 de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). Brasília, DF: Senado Federal; 2020 [Acesso em 12.jun.2020]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141306.

5. Doneda D. Da privacidade à proteção de dados. Rio de Janeiro: Renovar; 2005. p.160-161.

6. Bioni BR. Proteção de Dados Pessoais – A Função e os Limites do Consentimento. Rio de Janeiro: Forense; 2018. p.14.

7. Chiavegatto Filho ADP. The use of big data in healthcare in Brazil: perspectives for the near future. Epidemiol. Serv. Saúde. Brasília, abr-jun 2015; 24 (2):325-332.

8. Conselho Federal de Medicina. Resolução nº 1.643/2002. Define e disciplina a prestação de serviços através da Telemedicina. Brasília, DF; 2002 [Acesso em 12.jun.2020]. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643

9. Brasil. Lei nº 13.989/2020, de 16 de abril de 2020. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). Brasília, DF: Presidência da República; 2020 [Acesso em 12.jun.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13989.htm

10. Conselho Federal de Medicina. Ofício CFM nº 1.756/2020 – COJUR. Brasília, DF; 9/03/2020 [Acesso em 14.jun.2020]. Disponível em: https://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf

11. Chiavegatto Filho ADP, Kawachi I, Gotlieb SL. Propensity score matching approach to test the association of income inequality and mortality in São Paulo, Brazil. J. Epidemiol Community Health. 2012 jan; 66 (1):14-7.

12. 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). Bruxelas: Parlamento Europeu; 2016 [Acesso em 21.jun.2020]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

13. Mcafee A, Brynjolfsson E. Big data: The management revolution. Harvard Business Review. 2012; 90(10). p. 60.

14. Deepmind Blog. Scientific advances, real world benefits. 2020; [Acesso em 21.jun.2020]. Disponível em: http://deepmind.com

15. Gabriel I. Artificial Intelligence, Values and Alignment. Cornell University. 2012, jan. [Acesso em 21.jun.2020].10:32:16 UTC. Disponível em: http://arxiv.org/pdf/2001.09768.pdf.

16. Babylon Health Service. Babylon Privacy Policy. [s.d.] [Acesso em 21.jun.2020]. Disponível em: http://www.babylonhealth.com

Colaboradores

Todos os autores contribuíram com a concepção, elaboração, redação, revisão e aprovação do artigo.

Submetido em: 27/06/20
Aprovado em: 26/08/20

Como citar este artigo:

Leme RS, Blank M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos Ibero-Americanos de Direito Sanitário. 2020 jul./set.; 9(3): 210-224.

http://dx.doi.org/10.17566/ciads.v9i3.690