



A PROTEÇÃO DE DADOS SENSÍVEIS NA ÁREA DE SAÚDE EM LABORATÓRIOS

THE PROTECTION OF SENSITIVE DATA IN THE FIELD OF HEALTH IN LABORATORIES

Roberta de Oliveira Sutel¹
Pedro Henrique Hermes²
Rosane Leal da Silva³

RESUMO

As Tecnologias da Informação e Comunicação (TIC) têm sido aliadas em várias áreas do conhecimento, dentre elas na área da saúde. Este segmento realiza o tratamento de informações sobre as condições clínicas, concentrando inúmeros dados sensíveis dos pacientes, fator que o torna de alto risco em face dos danos que a divulgação indevida pode gerar na vida do paciente e de toda a sua família. Ciente desses novos riscos, este artigo visa investigar esse tema em maior profundidade, analisando-o à luz da Lei n. 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais, com a finalidade de responder ao seguinte questionamento: é possível afirmar que a nova Lei Geral de Proteção de Dados Pessoais trará proteção suficiente e adequada para os dados sensíveis na área da saúde, especialmente nos casos de tratamento de dados pelas operadoras assistenciais de saúde? Para seu enfrentamento utilizou-se o método dedutivo de abordagem, ao qual se seguirá procedimento monográfico, vez que a investigação aborda uma área específica para estudá-la em maior profundidade. Conclui-se que, se bem aplicada e fiscalizada, a Lei n. 13.709/2018 poderá trazer maior proteção aos dados sensíveis dos pacientes, especialmente pelo combate de práticas indevidas das operadoras assistenciais de saúde, que divulgam dados íntimos de seus pacientes às redes credenciadas de prestadores.

Palavras-chave: Dados Pessoais Sensíveis; Dignidade da pessoa humana; Direito à intimidade; Lei de Proteção de Dados Pessoais; Operadoras Assistenciais de Saúde.

ABSTRACT

The use of information and communication technologies (ICT) has been allied in several areas of knowledge, among them in the area of health. This segment carries out the treatment of information about the clinical conditions, concentrating countless patient sensitive data, a factor that makes it high risk in the face of the damage that undue disclosure can generate in the life of the patient and the whole family. Aware of these new risks, this article aims to investigate this subject in greater depth, analyzing it in the light of the Law n. 13.709/2018, called the General Law of protection of personal data, in order to answer the following question: it is possible to affirm

¹ Acadêmica do 7º semestre de Direito da Antonio Meneghetti Faculdade. Estagiária Escritório de Advocacia. E-mail: robertasutel@hotmail.com

² Acadêmico do 7º semestre de Direito da Antonio Meneghetti Faculdade. Estagiário do Ministério Público do Estado do Rio Grande do Sul. E-mail: pedrohermes.1@hotmail.com

³ Doutora em Direito pela UFSC. Professora da Graduação e Mestrado em Direito da UFSM, Coordenadora do NUDI. Professora do Curso de Direito da Antonio Meneghetti Faculdade - AMF. Coordenadora do Grupo de Pesquisa "Direito & Internet", da AMF. E-mail: rolealdasilva@gmail.com

that the New general law of personal data protection will bring sufficient and adequate protection for sensitive data in the health area, especially in cases of data processing by healthcare providers? The deductive approach method was used to cope with the monographic procedure, once the investigation approaches a specific area to study it in greater depth. It is concluded that, if well applied and supervised, the Law n. 13.709/2018 can bring greater protection to sensitive data of patients, especially by combating improper practices of health care providers, which disclose intimate data of their patients Accredited network of providers.

Keywords: Sensitive personal data; Dignity of the human person; Right to intimacy; Personal Data Protection Act; Health care providers.

INTRODUÇÃO

A configuração atual da sociedade é marcada pelo desenvolvimento tecnológico, cujas facilidades permitem tanto a criação, quanto a reinvenção e facilitação de inúmeras atividades profissionais. Os múltiplos impactos dessa inserção das tecnologias no cotidiano geram novos problemas sociais e jurídicos, pois se de um lado há um incremento e facilitação das atividades, por outro há inúmeros casos de violação a direitos fundamentais, o que pode ser mais ou menos intenso, a depender da área de atuação.

Uma das áreas de grande vulnerabilidade refere-se à saúde, pois as instituições hospitalares, clínicas, laboratórios, consultórios médicos e demais operadores assistenciais de saúde recolhem, tratam e utilizam dados pessoais sensíveis referentes às condições de saúde dos pacientes.

A divulgação indevida dessas informações ou seu acesso a outras empresas pode produzir impacto severo na vida e na dignidade do titular desses dados, especialmente porque essas informações podem gerar a discriminação do titular, fato cujos efeitos podem atingir inclusive outros membros da família.

É sobre esse tema que versa o presente artigo, cujo objetivo é discutir a proteção de dados pessoais sensíveis em face da atuação das operadoras assistenciais de saúde, abordagem que será realizada no intento de responder ao seguinte problema de pesquisa: É possível afirmar que a nova lei geral de proteção de dados pessoais trará proteção suficiente e adequada para os dados sensíveis na área da saúde, especialmente nos casos de tratamento de dados pelas operadoras assistenciais de saúde?

O método de abordagem eleito foi o dedutivo, partindo o estudo de visão geral e mais abrangente do tema para, posteriormente, focar-se especificamente no controle de



dados pelas operadoras assistenciais de saúde, momento em que será aplicado o método de procedimento monográfico.

1 DADOS SENSÍVEIS NA SAÚDE E A NOVA LEI DE PROTEÇÃO DE DADOS

Os dados pessoais não foram expressamente regulados na Constituição Federal de 1988, cujo artigo 5. dedicou-se a referir a proteção da vida privada e da intimidade. A ausência de previsão legal específica, no entanto, não impediu a violação a essas informações, situação que tem sido impulsionada pelo uso crescente das tecnologias.

A informatização e a interoperabilidade dos sistemas facilitam a atividade empresarial, pois minimizam as atividades internas, o que confere maior rapidez nos atendimentos. Tais sistemas também permitem que as informações, além de arquivadas, possam ser facilmente repassadas a outras pessoas físicas e jurídicas e é exatamente essa funcionalidade que revela novos, invisíveis e irreversíveis danos ao titular dos dados pessoais.

A gravidade se acentua quando os dados pessoais em questão se referem à saúde das pessoas, pois ali constam tanto predisposições genéticas que apontam para um provável desenvolvimento futuro de doenças, quanto registros de enfermidades já manifestadas. Seu tratamento e as respostas do organismo do titular dos dados também são mantidos nesses arquivos, o que leva a dizer que esse conjunto de informações conduz a um verdadeiro scanear da pessoa. Essas informações, altamente sensíveis e que se relacionam com a dignidade humana, precisam ser tratadas em ambiente seguro e controlado, pois sua disponibilização para terceiros pode gerar graves prejuízos ao titular.

Ainda que o armazenamento de dados dos pacientes não seja algo novo, pois qualquer médico ou profissional da área mantinha seus fichários em papel, é inegável que o uso dos sistemas informáticos trouxe maior complexidade ao tema, colocando em destaque uma nova categoria: os dados pessoais. Essa complexidade não foi suficientemente acompanhada pela legislação brasileira, cuja Constituição Federal de 1988 não contemplou expressamente esses direitos.

Ainda que sem previsão legal expressa, sua proteção decorria do direito fundamental à vida privada e intimidade, cuja tutela, segundo José Afonso da Silva



[...] visa proteger as pessoas de dois atentados particulares: (a) ao segredo da vida privada; e (b) à liberdade da vida privada. O segredo da vida privada é condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada, sem perturbação de terceiros⁴.

A formação de variados tipos de bancos de dados passou a ser uma constante a partir da década de 90, o que ensejou inclusive a previsão da matéria na Lei n. 8.078/1990, cujo artigo 43 contemplou este importante ponto. Nesse contexto, Eduardo Gabriel Saad sustentava que “é a Lei Básica que oferece, ao cidadão, meio idôneo para saber o que existe, sobre sua pessoa, em qualquer cadastro oficial ou não”⁵.

Essas previsões legais, no entanto, não tiveram o condão de enfrentar, sequer minimamente, a proteção dos dados pessoais sensíveis, restringindo-se ao tratamento da situação econômica e de (in)adimplência do consumidor. O avanço tecnológico, somado a novas formas de atuação empresarial, em que empresas repassam os dados de clientes e pacientes a outras, revelaram que a proteção legal até então existente era insuficiente para prevenir e impedir a violação dos direitos fundamentais, afetados tanto por ações do Estado quanto por atividade econômica dos particulares.

Nesse sentido é imperioso lembrar, a partir da lição de Ingo Sarlet⁶, que os direitos fundamentais vinculam ambos os atores e reclamam atuação positiva do Estado, pois constitui condição de existência das liberdades fundamentais e no princípio da dignidade humana.

Portanto, a lacuna existente não se justificava, sobretudo ante os novos mecanismos tecnológicos, cujo potencial de violação dos direitos não só se amplifica como também se renova a cada novo aplicativo ou sistema informático criado.

A novel legislação trouxe ao ordenamento jurídico brasileiro uma série de regras para as pessoas jurídicas e físicas que utilizarem, tratarem e armazenarem dados pessoais,

⁴ SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 23. ed. São Paulo: Malheiros, 2004. p. 90.

⁵ SAAD, Eduardo Gabriel. **Comentários ao Código de Defesa do Consumidor: Lei n. 8.078, de 11.9.90. LTr**, 1999.

⁶ SARLET, Ingo W. **Direitos Fundamentais e Direito Privado: uma Perspectiva de Direito Comparado**. Coimbra: Almedina, 2008.



arrolando direitos e obrigações para quem realiza a manipulação de dados sensíveis, objetivando trazer ao usuário a segurança de que não tenha seus dados violados.

Segundo a lei, dado pessoal pode ser considerado como a “informação relacionada a pessoa natural identificada ou identificável”⁷, ao passo que o dado sensível é

[...] 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 natural⁸

Em se tratando de proteção, o marco legislativo se torna paradigmático não somente às situações que rodeiam o tema de direito e internet, mas também qualquer relação jurídica existente entre alguém que realize o tratamento, utilização, armazenamento ou manipulação de dados pessoais de pessoas.

É justamente nesse âmbito de proteção de dados que Stefano Rodotà apresenta importância da necessidade de se proteger as informações dos indivíduos frente a sociedade da vigilância quando enuncia que a

Proteção de dados é uma expressão de liberdade e dignidade pessoais e, como tal, não se deve tolerar que um dado seja usado de modo a transformar um indivíduo em objeto sob vigilância constante. Confrontamo-nos com uma progressão de etapas: sendo esquadrihados por meio da vigilância por vídeo e tecnologias biométricas, os indivíduos podem ser ‘modificados’ pela inserção de chips ou etiquetas ‘inteligentes’ legíveis por identificação de radiofrequência dentro de um contexto que nos transforma cada vez mais em ‘pessoas na rede’ - pessoas que estão permanentemente na rede, aos poucos configuradas para transmitir e receber sinais que permitam escanear e perfilar movimentos, hábitos e contatos [...].⁹

⁷ BRASIL. **Lei 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). Diário Oficial da República Federativa do Brasil, 15 ago. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 14 abril 2019.

⁸ BRASIL. **Lei 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). Diário Oficial da República Federativa do Brasil, 15 ago. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 14 abril 2019.

⁹ RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p.18.



Como se percebe, a proteção de dados é consectária do direito à privacidade e intimidade, previstos em documentos internacionais e contemplados expressamente na Constituição Federal de 1988. Ao mesmo tempo a questão os dados pessoais se ligam a outros direitos, como a liberdade e dignidade, a merecer ampla guarida legislativa, especialmente ante à possibilidade de armazenamento e pareamento de informações identificáveis dos indivíduos, procedimentos que permitem a constante vigilância e classificação das pessoas por meio dos seus dados.

Nesse sentido, inserem-se na temática a ser protegida os dados sensíveis no âmbito das informações relativas à saúde do indivíduo. Com a era informática os usuários de serviços de saúde rotineiramente são catalogados pelos prestadores de serviço, quer da saúde pública ou da privada, englobados, inclusive, os procedimentos de baixa complexidade (como exames de sangue, por exemplo), o que promove ampla identificação das doenças e demais patogenias enfrentadas. Tal recolhimento e tratamento de dados possibilita, sem a observância de proteção, severa violação de direitos fundamentais, já que a partir da sua divulgação desautorizada o titular pode sofrer preconceitos, discriminação e fragilização da honra objetiva. Basta imaginar os resultados de alguém diagnosticado com o vírus HIV ter essa informação divulgada acidentalmente pelo banco de dados de determinado laboratório.

Nesse aspecto, a Lei Geral de Proteção de Dados Pessoais busca criar um arcabouço jurídico de proteção de tais informações, a ser cumprida por qualquer pessoa física ou jurídica que realize a coleta, tratamento e armazenamento de dados pessoais sensíveis, impondo aos provedores uma série de obrigações que devem ser respeitadas por ele, arquitetadas a partir dos princípios da finalidade do tratamento, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização.

2 REDES CREDENCIADAS DE PRESTADORES - LABORATÓRIOS E O DEVER DE SEGURANÇA DE DADOS

Realizados os aportes teóricos necessários para compreensão dos panoramas antes

**Anais do 5º Congresso Internacional de Direito e Contemporaneidade:
mídias e direitos da sociedade em rede (2019)**

<https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congresso-direito-anais>



e depois da Lei Geral de Proteção de Dados Pessoais, bem como dos conceitos, insta nesse momento aprofundar a temática sob o viés da proteção de dados de saúde pelos laboratórios à luz da nova lei e de que forma o paradigma proposto é gerador de obrigações por parte das redes credenciadas.

Atualmente, o uso de informações pessoais sensíveis tem se tornado estratégia econômica para as redes de prestadores, neste caso, os laboratórios. Nesse sentido, a questão, no entanto, tem-se centrado na utilização dessas informações para fins comerciais e econômicos, o que visivelmente afronta o direito de proteção dos dados pessoais amparado pela legislação. Em consequência disso, os prestadores de serviço ligados a área da saúde, como os mencionados laboratórios, usam do armazenamento, tratamento e manipulação das informações sensíveis de seus clientes como estratégia comercial, caracterizando nítida violação dos direitos de qualquer usuário e titular de dados pessoais.

Com o advento da Lei Geral de Proteção de Dados Pessoais o ordenamento jurídico procura conferir proteção e segurança ao usuário das prestadoras de serviços laboratoriais, de modo que as suas informações sensíveis não sejam violadas pela pessoa jurídica e pela própria rede. Alias, ressalta-se que a dita proteção de dados pessoais pretendida com a referida lei é consectária dos direitos fundamentais contidos na Constituição da República, notadamente os direitos à vida privada e intimidade. Nesse sentido, leciona Sarlet, Marinoni e Mitidiero:

A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática. [...] A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social.¹⁰

Destaque-se também que a nova Lei de proteção de dados pessoais tem ancoragem em importantes princípios, tais como dignidade da pessoa humana, respeito à privacidade, liberdade de informação, pois reconhece que a violação aos dados sensíveis

¹⁰ MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 472.



pode ocorrer de maneira indireta, pela manipulação de um conjunto de outros dados, que combinados podem gerar um dado sensível:

[...] Diversas modalidades de tratamento discriminatório possam ser realizadas sem o recurso a dados sensíveis, porém com o tratamento automatizado e estatístico de dados pessoais não sensíveis que acabem, por fim, revelando ou possibilitando a inferência de informações sensíveis quanto ao seu titular¹¹.

O tratamento discriminatório é a principal consequência quando estes dados são divulgados e utilizados indevidamente, principalmente quando envolvem doenças estigmatizadas pela população. Exemplo disso ocorre quando o indivíduo que faz exames em um laboratório é diagnosticado com doença grave e tem essa informação comercializada pelo banco de dados do laboratório para empresas, resultando na perda de oportunidades de emprego. Rodotà traz exemplo elucidatório acerca da discriminação por parte daquele que tem acesso a esse tipo de informação sensível:

Não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado¹².

Para compreender a matéria e os riscos a ela inerentes deve-se ter presente que banco de dados é um conjunto de dados organizados, que podem ser confidenciais ou públicas, cujo objetivo é permitir a extração de informações. Via de regra, essas informações deveriam auxiliar os laboratórios na melhor prestação de serviço a seus clientes, no entanto, a fim de obter lucros, muitas dessas informações são negociadas e transferidas sem o consentimento dos pacientes.

Essa finalidade mercantilista é extremamente arriscada e violadora do direito de proteção individual. Manuel Castells adverte para utilização dos dados pessoais com finalidades econômicas e ditadas pelo incentivo ao consumo, explicitando por meio de um

¹¹ SOUZA, Allan; DONEDA, Danilo; NASCIMENTO, Francisco; GUANAES, Paulo. **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde**. Rio de Janeiro: Fundação Oswaldo Cruz, 2018.p.7.

¹² RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p.70.



exemplo que

As oportunidades de negócios nessa nova indústria do marketing do comportamento são ilimitadas. Nas eleições de 2000 nos EUA, uma companhia criou um banco de dados, chamado Aristotle, que, usando dados de diferentes fontes, fornecia perfis políticos de nada menos que 150 milhões de cidadãos, vendendo esses perfis pela maior oferta, em geral dos escritórios de campanha de candidatos políticos.¹³

Nesse aspecto, de acordo com Danilo Doneda¹⁴, o tratamento de dados pessoais, principalmente no que se refere procedimentos automatizados, é uma operação de risco. Esse risco se materializa quando os dados são expostos e utilizados inadequadamente, em especial quando as informações estão incorretas ou representam erroneamente seu titular.

O uso dos dados dos pacientes tem cada vez mais ocorrido sob o argumento ou a justificativa de auxiliar os laboratórios no melhor atendimento de seus clientes. Com maior acesso a informações sobre os pacientes, como por exemplo histórico de doenças e alergias a medicamentos, os prestadores de serviço possuíam mais subsídios para tomarem decisões de como tratar as pessoas. No entanto, a destinação desse tipo de conteúdo para fins comerciais têm fragilizado os dados pessoais do indivíduo, tornando-o uma forma de proveito econômico por parte do provedor, mesmo quando houver consentimento do titular, que, por vezes, sequer percebe a manipulação existe.

Este processo de mercantilização fortalece o conflito de concorrência entre os laboratórios, pois se criam perfis dos consumidores com estes dados a fim de serem comercializados e explorados por terceiros, relativizando a inviolabilidade da intimidade da vida privada, visto que o detentor acaba tendo seus dados disponibilizados a outras empresas que utilizam essas informações em estratégias de marketing. Observa-se que essa violação de direitos fundamentais pela atividade econômica ocorre principalmente com a finalidade de dimensionar e individualizar os gostos e apreços do usuário da rede, conforme bem acentua Laymert Garcia dos Santos:

Controlar os consumidores e, principalmente, monitorar as potencialidades

¹³ CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003. p. 145

¹⁴ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Espaço Jurídico, 2011.



de cada uma das dimensões de suas vidas tornam-se uma exigência do próprio processo, impondo a coleta e o tratamento das informações. Ora, se lembrarmos que uma parcela cada vez maior da vida e das atividades do homem contemporâneo tendem a passar pelas redes quem mais bem colocado para acessar os seus dados senão os provedores de acesso ao ciberespaço? Como observa Emilio Pucci, é preciso ter em mente que se por um lado as redes oferecem um enorme fluxo de informações no sentido provedor-usuário, por outro, preciosíssimos fluxos partem desse último para o gestor do serviço, compostos sobretudo de dados relativos aos hábitos e à identidade dos utilizadores.¹⁵

A solução para esse problema é encontrar formas de a pessoa proteger seus dados com o seu consentimento, pois na era da informação não se tem o controle desses dados divulgados. Nesse contexto é que se insere a Lei Geral de Proteção de Dados Pessoais quando enuncia como principal fundamento para qualquer manipulação de dados a necessidade do consentimento de seu titular para tratamento, armazenamento e outras formas de utilização dessas informações.

Essa inovação permitiria, em tese, que o usuário tivesse maior controle e disponibilidade na utilização dos seus dados pessoais, notadamente aqueles que dizem respeito à saúde. Essa medida, se de fato for implementada, valorizará a autonomia de vontade do titular dos dados, permitindo que escolha a quem disponibilizará os dados, com ciência de eventuais repasses, a terceiros, dessas informações. Haveria maior segurança, evitando-se que as suas informações pessoais no tocante à saúde sofram qualquer tipo de violação por parte dos provedores assistenciais de saúde.

Em síntese, a Lei Geral de Proteção de Dados Pessoais impõe ao prestador, aqui, quando se fala em tratamento de dados, considerado como provedor, o dever de segurança dos dados de seu cliente, gerando a obrigação de que não tenha suas informações sensíveis comercializadas ou manipuladas indevidamente, principalmente pelo fato de se tratar de informação capaz não só de individualizar o titular, mas de torná-lo alvo de estigmatização e discriminação frente à sociedade.

¹⁵ SANTOS, Laymert Garcia dos. **Politizar as novas tecnologias: o impacto sócio-técnico da informação digital e genética**. São Paulo: Editora 34. 2003. p. 144.

CONCLUSÃO

O presente trabalho teve por objetivo investigar se a Lei Geral de Proteção de Dados Pessoais poderá trazer suficiente e adequada proteção aos dados sensíveis no tratamento de operadoras assistenciais de saúde.

Nesse sentido, foi possível verificar que o Brasil, até a promulgação da referida lei, carecia de uma legislação específica destinada a proteger qualquer operação, guarda, armazenamento ou tratamento que envolvesse as informações pessoais sensíveis do indivíduo, especialmente em face dos bancos de dados automatizados e utilizados por distintos operadores, tanto públicos quanto privados. Este quadro tornava-se ainda mais complexo em face da ausência de específico amparo constitucional dos dados pessoais, já que tais direitos de proteção de informações pessoais eram considerados albergados pela previsão dos direitos à intimidade e vida privada.

A crescente utilização das redes como principal forma de armazenamento de dados, principalmente os dados relativos à saúde, trouxe à pauta o debate acerca da necessidade de maior proteção de dados pessoais sensíveis do internauta, buscando evitar as violações de direitos. Nesse panorama, o surgimento da nova lei ao ordenamento pátrio pretende possibilitar ao cidadão que suas informações não sejam rotineiramente violadas por qualquer servidor, provedor ou mesmo prestador de serviços, utilizando-se para tanto de rigorosos procedimentos, englobando, principalmente, a necessidade de consentimento para o tratamento de dados. Aliás, diga-se que a lei geral elevou os dados pessoais formal e explicitamente à condição de bem jurídico, buscando proteger e resguardar qualquer informação pessoal na sociedade em rede, movida pela informação e cujos fluxos tornaram-se a base da economia e modo de operação da vida social.

Especificamente quanto à proteção dos dados pessoais na saúde, verificou-se que com a nova legislação as operadoras assistenciais necessitarão se ajustar aos termos de uso e observar as autorizações concedidas pelos titulares para proteger seus clientes e usuários ao longo da execução dos contratos de prestação de serviços na área da saúde. Busca-se com isso evitar a crescente comercialização de dados para outras empresas ou interessados em obter tal informação pessoal.

Assim, na tentativa de frear um mercado promissor, como publicamente o faz o



Facebook com seus usuários, a nova legislação impõe uma série de deveres e obrigações por parte das operadoras assistenciais para que possam dar prosseguimento aos serviços para o usuário, de forma a resguardar seus direitos mediante um sistema de tratamento de dados pessoais.

Veja-se que as exigências impostas pela novel legislação abarcam situações como necessidade de consentimento, novas responsabilidades para o controlador de dados, necessidade de comunicação do titular dos dados sobre eventuais intercorrências e, especialmente, casos de transmissão de dados a terceiros, observância do princípio da finalidade do tratamento de dados e, especialmente, necessidade de informação do titular sobre o uso compartilhado de dados pelo controlador, expondo ao titular a sua finalidade.

No entanto, ressalta-se que no plano fático não se verificou, até o presente momento, grande debate acerca dessas modificações e imposições às pessoas jurídicas, o que poderá ensejar uma dificuldade de implementação nos ditames da lei geral. Por outro lado, necessário contemplar com expectativa os novos rumos traçados, eis que possibilitarão ao usuário ter maior segurança e controle de suas informações.

REFERÊNCIAS

BRASIL. **Lei 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). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 17 jun. 2019.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 17 jun. 2019.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Espaço Jurídico, 2011.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional**. 6. ed. São Paulo: Saraiva, 2017.



MULHOLLAND, Caitlin. **Dados pessoais e sensíveis e a tutela de direitos fundamentais**: uma análise a luz da lei geral de proteção de dados. Rio de Janeiro: R. Dir. Gar. Fund., 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SAAD, Eduardo Gabriel. **Comentários ao Código de Defesa do Consumidor**: Lei n. 8.078, de 11.9.90. LTr, 1999.

SANTOS, Laymert Garcia dos. **Politizar as novas tecnologias**: o impacto sócio-técnico da informação digital e genética. São Paulo: Editora 34, 2003.

SARLET, Ingo W. **Direitos Fundamentais e Direito Privado**: uma Perspectiva de Direito Comparado. Coimbra: Almedina, 2008.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 23. ed. São Paulo: Malheiros, 2004.

SOUZA, Allan; DONEDA, Danilo; NASCIMENTO, Francisco; GUANAES, Paulo. **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde**. Rio de Janeiro: Fundação Oswaldo Cruz, 2018.