VI CURSO PÓS-GRADUADO EM BIOÉTICA

PORQUE A ÁREA DA SAÚDE PRECISA SE PREOCUPAR COM A PROTEÇÃO DE DADOS PESSOAIS

Maria Zilá Leal Bezerra Passo

Resumo: O presente trabalho se propõe a analisar a necessidade do setor de saúde se preocupar com a proteção de dados pessoais, principalmente porque os dados de saúde são considerados sensíveis. A nova ordem econômica mundial se caracteriza por ser informacional, assim, é inquestionável o valor dos dados, sendo assim, a Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018) surge com o intuito de proteger direitos fundamentais. Pela Lei Geral de Proteção de Dados, o tratamento de dados pessoais poderá ser realizado mediante o fornecimento do consentimento pelo titular e para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias. No Brasil, resta claro os deveres dos médicos em relação aos dados dos pacientes, vez que o Código de ética Médica (Resolução do Conselho Federal de Medicina nº 2.217/2018) já traz como dever do médico, o dever de informação, e o dever de sigilo. Assim, pode-se concluir que é essencial ao setor de saúde a garantia da privacidade dos pacientes, e que tal obrigação, no Brasil, é garantida não só através da recente lei, mas também, através do Marco Civil da Internet (Lei nº 12.965/2014), da Lei de Acesso à Informação - LAI (Lei nº 12.527/2011) e o Código de Defesa do Consumidor (Lei nº 8.078/90).

Palavras-Chave: Lei Geral de Proteção de Dados; Dados Sensíveis; Dados de Saúde; Profissionais da Saúde; Informação na Saúde.

Abstract: The present paper aims to analyze the need of special attention by the healthcare sector to the matter of protection of personal data, the main reason being that health data are considered sensitive information. The world´s new economic order is characterized by being information driven, so the value of data is unquestionable, thus, the Data Protection General Law (Law nº 13.709/2018) has arisen in order to protect fundamental rights. According to the Data Protection General Law, the processing of personal data may be carried out through patient consent, and aiming the preservation of health, in a procedure conducted by health professionals or health entities. In Brazil, the duties of physicians concerning patient´s data are clear, since the Code of Medical Ethics (Resolution of the Federal Council of Medicine Nº 2.217/2018) already lists among the duties of a physician those of information and confidentiality. Therefore, it can be concluded that it´s essential that healthcare sector ensures patient´s privacy and that such obligation, in Brazil, is guaranteed not only through more recent laws, but also through laws such as the Civil Rights Internet Framework (Law nº 12.965/2014), Information Access Law (Law nº 12.527/2011), and Consumer Protection Law (Law nº 8.078/90).

Keywords: Data Protection General Law; Sensitive Data; Health Data; Health Professionals; Health Information.

Sumário. Considerações iniciais. Visão geral sobre a LGPD: a quem se destina. o que são dados pessoais e sensíveis. definição de tratamento de dados pessoais. 1.1. Os princípios aplicados na LGPD. 2. Bases legais da LGPD que legitimam o tratamento de

dados. 3. Porque a área da saúde precisa se preocupar com a proteção de dados pessoais. 4. Responsabilidade pelo descumprimento da lei e como estar em conformidade. 5. O papel da bioética no tratamento de dados pessoais.

CONSIDERAÇÕES INICIAIS

Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018) afeta diferentes setores e serviços, seja no âmbito público ou privado, abrange desde compras on-line, redes sociais, a hospitais, bancos, corretores de seguros, escolas.

O surgimento de uma nova economia no final do século XX, a qual possui como características ser informacional, global e em rede, demonstra e explica o porquê da matéria prima desta nova economia serem os dados[1]. Neste novo cenário, no qual não temos mais fronteiras ou barreiras, as informações circulam livremente pela rede e os limites de acesso e até mesmo a finalidade de utilização destas informações abrigam uma invariável zona cinzenta.

No Brasil, outras leis já garantiam a proteção de dados, tais como a Constituição Federal de 1988, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei de Acesso à Informação - LAI (Lei nº 12.527/2011) e o Código de Defesa do Consumidor (Lei nº 8.078/90), contudo, até 2018, a matéria não era normatizada em Lei específica. A modificação deste cenário se deu com o advento do Regulamento de Proteção de Dados Pessoais europeu – RGPD, o qual serviu de inspiração ao ordenamento jurídico brasileiro, que resultou na edição da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Com a vigência da LGPD , vê-se que a tutela jurídica da privacidade ganhou ênfase, vez que a Lei dispõe sobre o tratamento de dados pessoais tanto em meios físicos, quanto em

[1] CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999. v. 1.

meios digitais, seja este realizado por pessoa física ou jurídica, pública ou privada, com o objetivo de proteger direitos fundamentais de liberdade e privacidade.

1. VISÃO GERAL SOBRE A LGPD: A QUEM SE DESTINA. O QUE SÃO DADOS PESSOAIS E SENSÍVEIS. DEFINIÇÃO DE TRATAMENTO DE DADOS PESSOAIS.

O presente capítulo pretende demonstrar o conceito de dados pessoais, dados pessoais sensíveis, o que significa tratar dados pessoais, bem como descrever o objetivo da lei.

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) colocou o Brasil em um outro nível regulatório. A coleta, armazenamento e tratamento de dados pessoais, que é uma das atividades preponderante da economia atual, passou a receber um olhar e atenção diferenciado, focado no empoderamento do titular de dados.

O novo paradigma da proteção de dados, consolidado pela LGPD reforça e sinaliza que o titular de dados é, mais do que nunca, o dono de suas informações.

Há diversas normas e regulações setoriais que versam sobre privacidade e proteção de dados no Brasil, como o Código de Defesado Consumidor, a Lei de Acesso à Informação, a Lei Geral de Telecomunicações, o Marco Civil da Internet, a própria ConstituiçãoFederal Brasileira e, no caso da saúde, as diversas normas setoriais daAgência Nacional de Saúde Suplementar (ANS), do Conselho Federalde Medicina (CFM), da Agência Nacional de Vigilância Sanitária (Anvisa), do Conselho Nacional de Saúde (CNS), entre outras.

Um dos principais conceitos para entender a LGPD está no que são dados pessoais. Assim, pode-se definir como dados pessoais toda informação sobre uma pessoa física identificada ou identificável, devendo considerar-se pessoa física identificável toda aquela que puder ser determinada, direta ou

indiretamente[2]. O critério adotado pela legislação brasileira foi o mesmo critério adotado pela legislação europeia, o critério expansionista.

Assim, pode-se concluir que dado pessoal é qualquer informação que possa identificar ou levar à identificação do seu titular, como dados cadastrais (nome, RG, CPF) e até mesmo dados comportamentais (preferências de navegação nainternet, preferências de pesquisa em um navegador, o número identificadordo seucelulareIP).

Os dados sensíveis dizem respeito a uma parte muito íntima do cidadão e, em virtude desta característica, podem gerar discriminação. Diante disso, possuem uma proteção e garantia excepcional, e em razão disso, a LGPD exigiu um consentimento específico e destacado para este tipo de dado.

O dado pessoal sensível é uma categoria especial de dados pessoais, que, ante a possibilidade de ser utilizado para fins discriminatórios, está sujeito a regras mais rigorosas para seu tratamento.

Os dados pessoais sensíveis são os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter regilioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.[3]

O legislador brasileiro adotou, portanto, o conceito amplo de saúde na LGPD, da mesma forma que o constituinte quando da sua definição nos artigos 6º e 196 da Constituição Federal de 1988[4]. Enquanto que o GDPR, regulamento europeu de proteção de dados, em seu Considerando de nº 35, traz

[2] Artigo 5º, I, da Lei nº 13.709/2018 – LGPD.

[3] Artigo 5º, II, da Lei nº 13.709/2018 – LGPD.

[4] Artigo 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição. Artigo. 196. A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação.

definições mais específicas sobre dados sensíveis[5].

Ao proteger os dados pessoais, a LGPD objetiva tutelar os direitos fundamentais de liberdade e privacidade, bem como a autodeterminação informativa da pessoa natural.

A Lei Geral de Proteção de Dados se destina a todas as pessoas naturais e jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que: a) o tratamento de dados seja realizado no Brasil; b) os dados tenham sido coletados no território nacional; ou c) ainda que ausente uma das situações anteriormente descritas, o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no Brasil.[6]

Existem, no entanto, exceções sobre a aplicação da LGPD ao tratamento de dados: a) quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos (ex: agenda telefônica usada para fins pessoais); b) quando realizado para fins exclusivamente jornalísticos; artísticos e acadêmicos; c) quando realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; d) quando os dados sejam provenientes de países que, por sua vez, ofereçam um nível de segurança jurídica adequado sobre esse tema (ex.: países

---

[5] *Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test. Disponível em: https://gdpr-info.eu/recitals/no-35/.*

[6] Artigos 1º e 3º, da Lei nº 13.709/2018 – LGPD.

da União Europeia) e apenas processados em território nacional, sem que haja qualquer intenção do agente brasileiro em compartilhar ou comunicar esses dados pessoais com outros agentes, exceto o agente que primariamente transmitiu a informação.[7]

O tratamento de dados abrange qualquer operação feita com o dado pessoal, entre elas coleta, produção, recepção, classificação, utilização, o acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[8]

Nesse sentido, qualquer procedimento que usar dado pessoal será considerado tratamento e estará sujeito às regras previstas pela Lei Geral de Proteção de Dados Pessoais.

1.1. OS PRINCÍPIOS APLICADOS NA LGPD.

A LGPD dispõe sobre uma série de regras para o tratamento de dadospessoais, sendo uma legislação essencialmente principiológica, já que estabelece os principais valores que deverão nortear a utilização dos dados pessoais pelos agentes de tratamento, sejam eles entidades públicas ou privadas.

Os princípios previstos são: a) Finalidade: todo tratamento de dados pessoais deverá ter uma finalidade legítima, específica, explícita e informada ao titular do dado pessoal, justamente para que ele possa ter controle e ciência sobre o que está sendo feito com seu dado; b) Adequação: o tratamento deverá ser adequado em relação às finalidades que foram informadas ao titular, de acordo com o contexto do tratamento; c) Necessidade: todo tratamento de dados deverá ser o menos intrusivo possível, estando limitado ao mínimo necessário para o alcance de suas finalidades, envolvendo apenas os dados pertinentes, proporcionais e não excessivos para determinada atividade de tratamento;

[7] Artigo 4º, da Lei nº 13.709/2018 – LGPD.
[8] Artigo 5º, X, da Lei nº 13.709/2018 – LGPD.

d) Livre acesso: este princípio é uma garantia ao titular de que ele possa ter acesso, de forma fácil e gratuita, à integralidade de seus dados pessoais, bem como à forma e à duração do tratamento; e) Qualidade dos dados pessoais: garante aos titulares a exatidão, clareza, relevância e atualização de seus dados, conforme necessidade e para o cumprimento da finalidade de seu tratamento, podendo os titulares corrigirem seus dados a qualquer tempo, por meio de procedimento facilitado e sem custos. Levando em consideração que os dados pessoais identificam seu titular, qualquer dado equivocado a respeito dele poderá implicar algum tipo de prejuízo; f) Transparência: determina que o tratamento de dados pessoais seja feito com a maior transparência possível, garantindo ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes que o realizam, observados, contudo, os segredos comercial e industrial; g) Segurança e prevenção: todo e qualquer agente de tratamento deverá aplicar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; h) Prevenção: deverão sempre ser adotadas medidas para fins de prevenção da ocorrência de danos em virtude do tratamento de dados pessoais; i) Não discriminação: nenhum dado pessoal poderá ser tratado em descrédito ou de forma injusta com relação ao seu titular ou, ainda, ser utilizado para discriminá-lo ou para outros fins ilícitos ou abusivos; j) Responsabilização e prestação de contas: o agente de tratamento deverá ser capaz de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das regras de proteção de dados pessoais.[9]

2. BASES LEGAIS DA LGPD QUE LEGITIMAM O TRATAMENTO DE DADOS.

[9] Artigo 6º, da Lei nº 13.709/2018 – LGPD.

As bases legais são as hipóteses que legitimam o tratamento de dados pessoais e estão definidas no artigo 7º da LGPD. Dessa hipóteses, o consentimento assume um papel de grande importância, sendo hoje uma das bases legais mais utilizadas para embasar tratamento de dados.

Segundo Danilo Doneda, em sua obra Da Privacidade à Proteção de Dados Pessoais: "Através do consentimento, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos deste consentimento à natureza dos interesses em questão"[10].

Resta claro, portanto, que o consentimento deve ser colhido de forma absolutamente clara e transparente, demonstrando sua finalidade e tempo de duração e acima de tudo, permitindo que o titular faça a gestão do consentimento fornecido.

Da LGPD, também pode se extrair as seguintes bases legais que legitimam o tratamento de dados: a) Cumprimento de obrigação legal ou regulatória; b) Tratamento de dados necessários a políticas públicas; c) Estudos por órgão de pesquisa (desde que anonimizados os dados); d) Execução de contrato; e) Exercício regular de direitos em processo judicial, administrativo ou arbitral; e) Proteção da vida ou incolumidade física; f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou por autoridade sanitária; g) Legítimo interesse; h) Proteção do crédito.

Importante destacar, ainda, que o consentimento deve ser: a) livre (voluntário e em condições de ser retirado a qualquer momento); b) específico (em relação a uma ou mais finalidades identificadas); e c) informado (com pleno conhecimento relativo às possíveis consequências decorrentes do consentimento).

O consentimento também deve ser claramente indicado por uma declaração ou ação por parte do titular dos dados.

[10] DONEDA, Danilo, Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro:Renovar, 2006.

Devendo o titular dos dados ser informado do seguinte: a) o uso que se fará de seus dados pessoais; b) os dados específicos que serão coletados; c) o nome, endereço e a informação de contato da empresa ou organização que coletará os dados; e d) se os dados serão divulgados a terceiros.[11]

Em geral, quanto mais sensível, invasiva ou não evidente é a coleta de dados, mais elevado deve ser o padrão de consentimento a ser obtido. E em se tratando de dados de saúde, os quais são classificados como dados pessoais sensíveis, estes requerem o consentimento expresso das pessoas afetadas antes que os dados possam ser coletados.

3. PORQUE A ÁREA DA SAÚDE PRECISA SE PREOCUPAR COM A PROTEÇÃO DE DADOS PESSOAIS.

Atualmente, diante de um cenário de compartilhamento e monetização dos dados, com a presença cada vez mais forte da Internet das Coisas (IoT) e da Inteligência Artificial, surgiu a necessidade de legislações para garantir a privacidade e a ética no tratamento dos dados pessoais.

A LGPD tem impactos em várias áreas, vez que todas as organizações lidam com dados pessoais, contudo, na área da sáude, a LGPD merece destaque, vez que os dados de saúde dos titules são considerados sensíveis.

Conforme dados da Agência Nacional de Saúde (ANS)[12], no Brasil, os beneficiários da saúde suplementar ultrapassam 47,6 milhões, de acordo com o número mais recente, de dezembro de 2020, e foram realizados 1,62 bilhão de procedimentos em 2019, ficando evidente o enorme fluxo e volume de dados pessoais envolvidos. E isso sem contar o Sistema Único de Saúde[13], que também deverá se adequar às disposições da LGPD,

[11] Artigo 8º, da Lei nº 13.709/2018 – LGPD.
[12] https://www.ans.gov.br/perfil-do-setor/dados-gerais. Acessado em julho/2020.
[13] Assistência pública de saúde.

já que as regras nela previstas também se aplicam ao Poder Público.

Ao mesmo tempo em que a tecnologia apresenta, através da Inteligência Artificial, ou de Big Data, por exemplo, novas ferramentas e geram facilidades a pacientes e profissionais de saúde, ela também estabelece novas responsabilidades.

Assim, é inegável a necessidade do setor de saúde, que já dispõe de uma série de regulações e normas setoriais próprias, as quais também envolvem o sigilo e a confidencialidade das informações dos pacientes e usuários do sistema de saúde, de se atentar para a privacidade e proteção de dados pessoais dos titulares, conforme regramento trazido pela Lei Geral de Proteção de Dados Pessoais.

As tecnologias, ao mesmo tempo que facilitam a vida dos pacientes e dos profissionais de saúde, exigem maior cuidado e responsabilidade para se evitar vazamentos, ou utilizações indevidas. Em razão disso, é fundamental que profissionais e instituições de saúde conheçam a LGPD para que possam cuidar de forma efetiva e preventiva dos dados dos tutulares. Ademais, além de evitar responsabilizações e penalizações, a adequação do profissional e da instituição de saúde é vista como uma vantagem competitiva no setor.

Baseado no GDPR, a LGP também faz uso do conceito de *Privacy by Design* e *Privacy by Default*, os quais demandam que a privacidade seja considerada desde a concepção do produto e como padrão.

Destas forma, as tecnologias aplicadas ao setor de saúde devem possuir a privacidade como valor nuclear e intrínseco ao produto ou serviço.

4. RESPONSABILIDADE PELO DESCUMPRIMENTO DA LEI E COMO ESTAR EM CONFORMIDADE.

Para se falar em responsabilidade pelo tratamento dos

dados, primeiro há que se entender o que é um controlador e um operador de dados. O controlador[14] é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento de dados pessoais. Já o operador[15] é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O fator mais relevante para caracterizar o controlador é a sua capacidade de decidir sobre a finalidade e os elementos essenciais dos meios de tratamento.

A LGPD destaca em seu texto, nos artigos 42 a 45, as regras que irão estabelecer os limites das responsabilidades do controlador e do operador. Em primeiro lugar, a Lei afirma que qualquer dano, seja ele patrimonial, moral, individual ou coletivo decorrente da violação da legislação de proteção de dados pelo controlador ou operador, em razão do exercício da atividade de tratamento de dados pessoais, deve ser reparado.

Danilo Doneda e Laura Schertel entendem que a responsabilidade dos agentes de tratamento é preponderantemente objetiva, levando-se em consideração o risco da atividade, independentemente da culpa do agente de tratamento[16]. Para os doutrinadores, em razão de a LGPD ter como um dos seus principais fundamentos a minimização do riscos de dano, é possível inferir que o legislador adotou o regime de responsabilidade objetiva. Isto se justifica pela existência de um risco intrínseco à atividade de tratamento de dados que está relacionado à capacidade iminente de gerar dano aos titulares dos dados caso seus direitos sejam violados ou princípios da lei não sejam observados.

O controlador responderá solidariamente por qualquer violação à legislação causados tanto pelo operador quanto por outros controladores que estiverem diretamente envolvidos no

[14] Artigo 5º, VI, da Lei nº 13.709/2018 – LGPD.
[15] Artigo 5º, VII, da Lei nº 13.709/2018 – LGPD.
[16] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor. v.120, 2018, p. 555

tratamento do qual decorreram danos ao titular dos dados.

Assim, os profissionais e instituições de saúde envolvidos no tratamento de dados devem desenvolver a cultura da privacidade em sua organização, os gestores devem ser capazes de interpretar a lei da forma correta, e devem implementar uma política de segurança de dados para proteger informações pessoais.

O uso de medidas de segurança apropriadas para fornecer a proteção necessária inclui: a) medidas físicas (arquivos trancados a chave, acesso restrito nos recintos/escritórios, sistema de alarme, câmeras de segurança); b) ferramentas digitais (senhas, encriptação, firewalls); c) controles na empresa (verificação de antecedentes, normas relativas a tirar arquivos para fora das instalações, limitar acesso sobre a base de dados a "necessidade de conhecer", formação de pessoal, acordos com clientes e subcontratados).

Uma boa política de segurança de dados deve incluir procedimentos não só para previnir vazamentos, mas também para definir condudas e processos caso ocorra uma violação.

Outra importante atitude para a proteção dos dados é eliminar a identificação dos dados. O processo de anonimizar é uma garantia que implica no apagamento ou modificação dos dados de identificação pessoal resultando em dados que não identifiquem as pessoas.

O primeiro passo para um programa de adequação à LGPD bem-sucedido é entender o papel que a entidade ou o profissioanl de saúde assume frente à LGPD. A compreensão do papel, como controlador ou operador, em relação às atividades desempenhadas é fundamental para conduzir processos que envolvam o tratamento de dados em conformidade com a LGPD e demais legislações aplicáveis. Identificar os agentes de tratamento é primordial não só para a atribuição de obrigações e responsabilidades contratuais, como também para o cumprimento de obrigações perante os titulares e a Autoridade Nacional de

Proteção de Dados[17].

Para os profissionais e entidades de saúde adequarem-se à LGPD, é imposto a eles uma mudança de postura, de conduta e de cultura. As entidades de saúde devem desenvolver uma estrutura de governança em proteção de dados com distribuição de responsabilidades. As equipes devem ser treinadas para que tenham ciência das regras de proteção, da política de privacidade, bem como das responsabilizações em caso de desvio ou descumprimento, o que resulta em uma cultura vigilante, em que todos os envolvidos permanecem diligentes para o cumprimento das regras.

5. O PAPEL DA BIOÉTICA NO TRATAMENTO DE DADOS PESSOAIS.

A bioética, em meio à evolução tecnológica, exerce papel fundamental, vez que exige auditabilidade no tratamento dos dados pessoais, ou seja, impõe a verificação das ações de tratamento de dados com a Lei. É a bioética que estimula a compreenção dos limites éticos no uso das tecnologias e no tratamento de dados. A bioética contribui para que o tratamento de dados estejam de acordo com os valores éticos e morais.

O consentimento livre, informado e inequívoco, consagrado pela LGPD, é um dos pilares da bioética, pois exprime a dignidade da pessoa. E como para o tratamento de dados pessoais é essencial o consentimento, vê-se que a bioética é um dos pilares para um tratamento de dados pessoais seja realizado de forma adequada.

Processar dados pessoais para finalidades legítimas, específicas, explícitas e informadas ao titular, ser transparente e garantir informações claras, precisas e acessíveis ao indivíduo,

[17] Artigo 5º, XIX da Lei nº 13.709/2018 – LGPD: autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

titular dos dados, e ter o titular de dados como ponto de referência para a reflexão e a ação, além de alinhar-se aos fundamentos da LGPD, é o que resulta na adequada fundamentação legal para o tratamento de dados sensíveis.

CONSIDERAÇÕES FINAIS

A proteção de dados pessoais tem como fundamentos o respeito à privacidade, a autodeterminação informativa, ou seja, o direito de cada indivíduo controlar e protreger seus dados, bem como a inviolabilidade da intimidade, o desenvolvimento tecnológico, a livre iniciativa, e a dignidade.

Neste sentido, o Código de Defesa do Consumidor (Lei nº 8.078/1990), em seu artigo 43, garante ao titular de dados (consumidor) acesso às informações existentes em cadastros, fichas, registros, e também prevê o direito de correção dos dados caso haja inexatidão desses, bem como garante acesso às fontes de tais dados.

No tocante aos profissionais e estabelecimentos de Saúde, a preocupação com a manipulação de dados é ainda maior, vez que estes lidam com dados pessoais sensíveis.

São dados de saúde, segundo a LGPD, os que revelam informações sobre a saúde física ou mental de um titular no passado, presente ou futuro. Abrangem, também, informações obtidas a partir de análises ou exames, incluindo dados genéticos e amostras biológicas

Para garantir a segurança dos dados de saúde, algumas práticas podem ser realizadas pelos profissionais e estabelecimentos, tais como: limitação de acesso de usuários confiáveis, utilização de senhas e autenticação em dois fatores, política de renovação de senhas com período de tempo determinado, estabelecimento de níveis de privilégio de acesso distintos, criptografia de ponta a ponta, entre outros.

Além da implementação de medidas de segurança da

informação, os profissionais da saúde devem compreender que o maior risco de incidente de segurança está atrelado ao fator humano, assim, é primordial o treinamento da equipe, desenvolvimento de um processo interno para controle do fluxo de dados, incluindo, inclusive, o desenvolvimento de um roteiro para condução do tratamento.

Portanto, é possível tratar dados, até mesmo os sensíveis, desde que observados os critérios de segurança da informação e respeitadas as bases legais que autorizam o tratamento. Profissionais, estabelecimentos, sejam eles públicos ou privados, que não realizarem o tratamento de dados de forma adequada e segura estão sujeitos a adquirirem grande passivo judicial, pois, além da vigência da LGPD e da instituição da ANPD - Autoridade Nacional de Proteção de Dados, órgãos de defesa do consumidor como o PROCON[18] e Ministério Público[19] já vem atuando como fiscais do cumprimento das regras de proteção de dados.

É importante que os profissionais de saúde e as entidades compreendam que a privacidade de seus interlocutores, concretizada por meio da proteção de seus dados pessoais, é valor cuja busca é perene e jamais poderá retroceder. Sendo assim, a mera implantação de controles eprocedimentos internos é insuficiente, e sua reciclagem e atualização periódica são tarefas obrigatórias.

[18] PROCON - Programa de Proteção e Defesa do Consumidor, representada órgão estatal, vinculado à Secretaria da Justiça e da Defesa da Cidadania, responsável por ajudar a mediar os conflitos entre os consumidores e os fornecedores de produtos e serviços.

[19] Artigo 127, da Constituição Federal 1988: Art. 127. O Ministério Público é instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei Federal nº 12.527/2011 Lei de Acesso à Informação - LAI . Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

BRASIL. Lei Federal nº 13.709/2018. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm.

BRASIL. Lei Federal nº 8.078/90 - Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

BRASIL. Código de Ética Médica (Resolução do Conselhor Federal de Mecina nº 2.217/2018). Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf

CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999. v. 1.

Cartilha Proteção de Dados Pessoais no Setor da Sáude – Opice Blum Academy. Diponível em: https://opiceblum.com.br/wpontent/uploads/2021/02/Cartilha_saude_dados_pessoais_04.2021.pdf.

DONEDA, Danilo, Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro:Renovar, 2006.

DLA Piper, Data Protection Laws of the World (https://www.dlapiperdataprotection.com/).

ISO 26362:2009 – Access panels in market, opinion, and social research.

MAGRANI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019, 2ª ed.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor. v.120, 2018, p. 555