



FUNDAÇÃO PRESIDENTE ANTÔNIO CARLOS DE UBÁ
FACULDADE DE DIREITO
2020

**A COLETA DE DADOS PESSOAIS POR SERVIÇOS MÉDICOS SEM
CONSETIMENTO OFENDE À PRIVACIDADE?**

RÔMULO CÉSAR A. ALMEIDA- romulocesar@rcsystemas.com

ALEXANDRE RIBEIRO DA SILVA - profalexandreriroadv@gmail.com

RESUMO:

O Presente trabalho analisará o direito à proteção de dados pessoais na sociedade brasileira. Utilizaremos o pensamento do jurista italiano Stefano Rodotà sobre as transformações do direito à privacidade em conflito com direito a saúde, ou seja, a vida. Levantaremos pontos da lei 13.709 de 15 de agosto, Lei Geral de Proteção de Dados, LGPD, que é instrumento normativo que visa tutelar o direito à proteção de dados pessoais. A LGPD veio consolidar muitas garantias e direitos que eram anteriormente tratados de forma esparsa, o que muito positivo e certamente traz segurança jurídica ao país. Para o setor da saúde, a privacidade de dados e o direito ao sigilo não são novidades. Há muitos anos se promovem ações para garantir a segurança das informações que coletam. Afinal o sigilo na saúde é um norte orientador de todos os envolvidos. O empoeiramento do paciente e o reconhecimento de sua participação no processo da assistência à saúde também tem sido cada vez mais difundidos nos estabelecimentos de saúde do país. Nos últimos anos, verificamos um aumento significativo da utilização de Termos de Consentimento, por meio dos quais os pacientes ou seus responsáveis formalizam sua concordância com o tratamento proposto e tomam conhecimento dos riscos envolvidos.

Palavras-chave: Dados Pessoais, Dados Sensíveis, Privacidade, Consentimento, Saúde.

ABSTRACT:

The present work will analyze the right to protection of personal data in Brazilian society. We will use the thought of the Italian jurist Stefano Rodotà on the transformations of the right to privacy in conflict with the right to health, that is, life. We will raise points of Law 13,709 of August 15, General Data Protection Law, LGPD, which is a normative instrument that aims to protect the right to the protection of personal data. The LGPD came to consolidate many guarantees and rights that were previously treated sparingly, which is very positive and certainly brings legal certainty to the country.

For the health sector, data privacy and the right to secrecy are not new. Actions have been taken for many years to ensure the security of the information they collect. After all, health secrecy is a guiding principle for everyone involved. The empowerment of the patient and the recognition

of his participation in the health care process has also been increasingly widespread in health facilities in the country. In recent years, we have seen a significant increase in the use of Consent Terms, through which patients or their guardians formalize their agreement with the proposed treatment and become aware of the risks involved.

As with the LGPD, this consent can also be revoked at any time.

Keywords:

Personal Data, Sensitive Data, Privacy, Consent, Health

INTRODUÇÃO

A Lei Geral de Proteção de Dados, ou LGPD lei 13709/18, possui amplo escopo de incidência, uma vez que dispõe sobre dados pessoais de pessoa naturais. Estabelece as bases legais como hipóteses autorizadas para tratamento dos dados pessoais que devem ser cuidadosamente analisadas e escolhidas para cada tratamento de dados pessoais realizados.

Contudo, a dúvida ainda é muito grande diante do ineditismo da matéria. O que Deve-se solicitar o consentimento para todo tratamento de dados pessoais?.

Diante disto, o presente estudo analisará em um ponto muito questionado e controverso da própria lei previstos nos artigos 7º inciso VII e 11, II letra “f”: a coleta de dados pessoais e dados sensíveis por profissionais de saúde, serviços de saúde ou autoridade sanitária viola o direito da privacidade ou é um corolário defesa da saúde? Incidentalmente deve-se responder: Precisa-se de coletar o consentimento do paciente para tudo?

No primeiro capítulo abordaremos a privacidade da pessoa e o que são dados pessoais e dados sensíveis voltado para o lado da saúde de privacidade queremos saber todos os seus exames, histórico de saúde desde quando nasceu até o presente momento, exames de sangue, doenças, vai permitir ter acesso a imagem do seu rosto, estamos mexendo em um direito fundamental da pessoa, direito à privacidade, direito consagrado na constituição federal, todavia dados pessoais e conceituado como informação relacionada a pessoa natural, que identifica ou identificável, utilização do conceito expansionista, já dado pessoal sensível quando tratado pode trazer ao titular do dado alguma discriminação, são os que revelam origem racial ou étnica, opiniões políticas, filiação sindical, biometria e sobre a saúde ou a vida sexual da pessoa.

No segundo capítulo falaremos sobre o consentimento para tratamento dos dados que é uma das dez bases legais para tratamento de dados, e a base mais falada, a mais exposta, falaremos do consentimento para coleta dos dados pessoais e sensíveis.

Já no terceiro capítulo entraremos na problemática de coleta de dados relacionado a saúde, ou seja, falaremos se ofende a privacidade da pessoa ou é uma defesa da saúde.

A fim de compreender essas modificações na privacidade, bem como o impacto causado pelas tecnologias de computação em rede e internet, esse estudo ampara-se no pensamento do renomado jurista italiano Stefano Rodotà.

A metodologia utilizada foi revisão bibliográfica de obras, artigos e pesquisas referentes ao tema, além das análises constitucionais e legislativas sobre a privacidade e a proteção de dados no Brasil.

1. A PRIVACIDADE E OS DADOS PESSOAIS E SENSÍVEIS

Conforme explicitado pelo jurista italiano Stéfano Rodotà (2008, p.24) é cada vez mais patente a impossibilidade de se compreender a privacidade como um “direito de ser deixado só”, ou, “*The right to be let alone*”. Ou ainda,

Atividades cotidianas que anteriormente se realizavam no convívio social agora envolvem o uso de ferramentas e aplicações pela internet. Tornou-se comum o uso de smartphones e computadores na realização de compras e interações em sites ou aplicativos como ifood, Facebook, Mercado Livre, Whatsapp, Tinder entre tantos outros. Desta forma, uma simples compra de um lanche, uma conversa com amigos e quase todos os afazeres diários apresentam-se ligados ou com a possibilidade de estarem ligados ao uso incessante de tecnologias de rede e comunicação. A construção da personalidade humana perante o mundo não mais se limita em um campo individual, mas sim a partir de uma intersubjetividade entre indivíduos que, em tempos presentes, perpassa os meios digitais de comunicação. Não por menos, a tutela deste sujeito deve se realizar “em relação com outros (o sentido da alteridade) e com o mundo a ele externo.” (SILVA, 2017, p. 11)

Na realidade contemporânea da sociedade, com a troca instantânea e contínua de informações com altas taxas de velocidade pela internet, o direito à privacidade

estampada como garantia fundamental do art.5º, inciso X da Constituição Federal¹ deve necessariamente acompanhar a mudança dos tempos e se adequar a novos paradigmas de relacionamento das pessoas.

Ou seja, a privacidade ainda deve resguardar o direito à inviolabilidade do lar e da intimidade cada indivíduo, bem como a preservação dos direitos da personalidade a partir dos dados pessoais, como honra, imagem e o nome, do uso sem prévia autorização ou pelo mau uso depreciativo. Mas o direito à privacidade atual deve ir além, englobando a proteção dos dados pessoais compartilhados pelas pessoas, pois envolve direitos inerentes da personalidade. Ou, em outros termos,

Assim, como se vê, a privacidade não mais pode ser identificada como questão de sigilo, dentro do qual o indivíduo se isola para viver à margem de todo o tecido social. Não mais sendo possível a coexistência nesse sentido, a imbricação do ser humano na sociedade se dá, inevitavelmente, por meio da circulação de suas informações pela rede de relacionamentos pessoais e institucionais, o que clama pela alteração de perspectiva da privacidade para o controle espacial e contextual das próprias informações, convergindo, portanto, em ampla disciplina de proteção de dados pessoais. (BUCAR, 2016, p.655, apud, SILVA, 2017, p.23)

Assim, a privacidade deve abarcar a construção da personalidade individual neste novo paradigma contemporâneo, ou ainda, deve partir do controle que cada indivíduo tem sobre seus dados. Conforme Rodotá (2008, p.93) privacidade hoje é também a “possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo de informações a ele relacionadas”. Mas o que são, afinal, dados pessoais?

1.1 Os Dados Pessoais

A Lei de Proteção de Dados pessoais expressamente aduz em seu art. 5º inciso I que

“Art. 5º Para os fins desta Lei, considera-se:
I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dessa forma, pode se dizer que Dado Pessoal é qualquer informação que possa

¹ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

levar à identificação de uma pessoa física, direta ou indiretamente. Não somente nomes e CPFs, mas dados de localização, hábitos, preferências etc, e um dado identificável e um conjunto de informação que permitem a identificação de uma pessoa natural e o que a lei chama de titular, ou seja, a pessoa a que os dados se referem. Ou ainda,

O conceito de dado pessoal é bastante abrangente, sendo definido como a “informação relacionada à pessoa identificada ou identificável”. Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, Passaporte e Título de Eleitor), endereço residencial ou comercial, telefone, e-mail, cookies e endereço IP. (OLIVEIRA, 2019, n.p.)

O conceito engloba, também, dados que podem sujeitar uma pessoa natural individualizada a uma determinada atividade, comportamento ou ação (prática conhecida como “*singling out*”), tornando por vezes desnecessário saber efetivamente quem essa pessoa é (saber se tratasse de Maria ou João), desde que haja um identificador único atrelado a este indivíduo.

1.2 Os Dados Sensíveis

Já dados sensíveis estão previstos no art. 5º inciso II também da LGPD,

Art. 5º Para os fins desta Lei, considera-se:

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Tais dados trazem informações cujo tratamento sujeita o titular a um maior risco de discriminação, ou seja, dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Ou ainda,

A Lei traz também a definição de dados pessoais sensíveis, que são aqueles que se referem à “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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”. Por seu maior potencial lesivo, o tratamento desses dados deve observar regras ainda mais rígidas.

(OLIVEIRA, 2019, n.p.)

Como pode perceber os dados pessoais sensíveis trazem ainda mais detalhes sobre sua via pessoal. Esse conceito engloba, ainda, dados pessoais que, num primeiro momento, podem não parecer sensíveis, como a localização de um indivíduo (p. ex. informações de geolocalização de uma pessoa que está semanalmente em uma determinada igreja ou espaço de culto) mas que, devido ao contexto da sua coleta, podem permitir inferir dados sensíveis.

Nesse sentido dado pessoal e a informação relacionada à pessoa natural identificada ou identificável e dado pessoal sensível e o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política etc.

Deste modo, a privacidade hoje é atrelada à proteção de dados pessoais e dados sensíveis, uma vez que o controle sobre os mesmos preserva uma dimensão de proteção da própria personalidade da pessoa. Esse controle passa por garantir a cada indivíduo o conhecer e consentir o prévio uso de seus dados pessoais, muito embora a própria lei abarque exceções. É o que se passará a abordar.

2. O TRATAMENTO DE DADOS PESSOAIS E DADOS SENSÍVEIS

A LGPD estabelece orientações e princípios que devem ser observados durante todo o ciclo de vida dos dados pessoais na organização, desde a coleta até a exclusão, passando por armazenamento, reprodução, utilização e outras atividades que totalizam 20 ações de tratamento de dados. De maneira geral, qualquer tratamento envolvendo dados pessoais, salvo exceções legais, é objeto de regulamentação da lei.

Já em seu artigo 1º a LGPD expressamente reconhece que o tratamento de dados se dará em conformidade aos direitos e garantias fundamentais de liberdade e privacidade e em consonância com os direitos da personalidade (SILVA, 2017, p.72).

Expressamente,

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e

Municípios.

Ou seja, o tratamento dos dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular. Aliado ao dever de transparência o titular deve estar ciente da finalidade, a qual obviamente não pode ser justificada em atos ilegais, ainda que haja consentimento para tanto. Objeto ilícito torna nulo o ato. O quanto mais específica a descrição dos usos for, melhor.

Ainda, a regra geral para o tratamento dos dados pessoais é o consentimento prévio e informado e as excessões expressamente constam também em lei, conforme o art. 7º inciso I,

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

No mesmo sentido, tratando-se de dados pessoais sensíveis, o consentimento necessariamente será exigido, nos termos do art 1, inciso I,

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

O consentimento sempre é visto, por muitos, como a panaceia para tratamento de dados pessoais bem verdade, o consentimento é a autorização expressa dada pelo titular ao controlador para que ele possa tratar os dados da forma desejada. Ou ainda,

O consentimento do titular do dado é a permissão que ele dá para que o tratamento de seus dados pessoais ocorra. Contudo, para que o consentimento seja válido, ele tem que ser dado de forma livre, inequívoca e específica (não é válido consentimento para autorizações genéricas, sendo nulo o consentimento dado dessa forma), e se houver mudança quanto a finalidade para a qual o consentimento para tratamento de dado foi concedido, o titular deve ser informado para que novamente expresse se aceita o tratamento. (PORTO, 2020, p. 16).

Assim, o consentimento, para ser válido, deve ser livre, informado e inequívoco, fornecido por escrito ou outro meio que demonstre a manifestação da vontade do titular, em cláusula destacada, sem vício de consentimento e referir-se a finalidades determinadas. Autorizações genéricas são consideradas nulas. Caixas de seleção pré-

marcadas também são consideradas não legítimas, invalidando o consentimento conforme teor do disposto do art. 8º,

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais;

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Mas a própria lei previu a possibilidade de tratamento de dados pessoais e dados pessoais sensíveis, sem o consentimento do titular do dado, em casos muito excepcionais. Resumidamente, sem o consentimento, tal tratamento somente poderá ocorrer nas seguintes hipóteses: cumprimento de obrigação legal ou regulatória pelo controlador, administração pública, institutos de pesquisa, contratos e processos judiciais, além disto, temos a hipótese referente à proteção da vida e tutela da saúde, neste em especial faremos as seguintes considerações.

3. A COLETA DE DADOS PESSOAIS POR SERVIÇOS DE SAUDE, OFENSA A PRIVACIDADE DAS PESSOAS OU DIREITO DA SAÚDE ?

Dentre as hipóteses de excepcionalidade, nas quais é dispensado o consentimento para o tratamento de dados pessoais e dados pessoais sensíveis estão à necessidade de tratamento de dados para “tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”. Neste sentido,

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas

seguintes hipóteses:

I - Mediante o fornecimento de consentimento pelo titular;

(...)

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

(...)

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

(...)

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

Portanto, via de regra, nestas situações não é necessário coletar o consentimento dos pacientes para todo tipo de tratamento de dados pessoais. Na verdade, nem mesmo é recomendado, que na área da saúde pautem a coleta de dados na base do consentimento, haja vista que em diversas situações há urgência na coleta destes dados para a própria preservação da incolumidade física e da saúde do paciente.

Corroboram este entendimento, as determinações contidas nos arts. 7º, VIII e 11, II, “f”, respectivamente, para hipóteses de tratamento para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde, ou, ainda, para proteção da vida ou incolumidade física do titular ou de terceiros, previsto nos arts. 7º, VII e 11, II, “e” da LGPD.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro

(...)

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

Consoante salientado, tendo em vista as peculiaridades dos dados sensíveis, em especial os dados de saúde, a LGPD também previu uma relação de hipóteses em que estes poderão ser tratados sem o fornecimento de consentimento do titular, quais sejam,

art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, Sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- e) proteção da vida ou da incolumidade física do titular ou de terceiros;
- f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

Portanto, a LGPD também prevê que o tratamento de dados sensíveis poderá ser realizado sem o consentimento do titular dos dados pessoais nas hipóteses em que for indispensável para a proteção da vida ou da incolumidade física.

A legislação nacional não traz o conceito do que poderia ser compreendido como “proteção da vida”. Por sua vez, utilizando dos conceitos previstos na GDPR (Regulamento Geral sobre a Proteção de Dados), entendemos que, de uma maneira ampla, o conceito está adstrito à proteção da vida e à segurança pública.

Deste modo, a necessidade de tratamento de dados pessoais sensíveis se torna evidente quando estamos diante de uma situação que demande a atuação imediata da Administração Pública para salvar vidas como, por exemplo, nas catástrofes naturais.

Outro exemplo que possibilita o tratamento de dados com base na proteção da vida, é a utilização destas informações para a prevenção, a investigação e a repressão de infrações penais pelos agentes públicos responsáveis.

No mesmo sentido, a GDPR preceitua no art. 9º, II, “c”,”i” que não será necessário o consentimento do titular nos casos de prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, como no caso de médicos que estão submetidos aos preceitos éticos dispostos no Código de Ética Médica.

2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:

c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

É importante ressaltar que essa dispensa somente se dá para tratamentos de dados pessoais que forem exclusivos para a tutela da saúde de uma pessoa e desde que se dê em um procedimento realizado por profissionais da saúde, em serviços de saúde, ou no caso de proteção da vida ou incolumidade física do titular ou de terceiros. (<https://triplait.com/lgpd-na-saude/>)

Portanto, expressamente não há nenhum problema em coleta de dados pessoais e dados pessoais sensíveis quanto reativos à preservação da vida e da saúde.

Por outro lado, tanto o art 7º inciso VIII e o art. 11,II letra “f” não expressa quem se enquadraria nos conceitos expressos de “profissionais de saúde, serviços de saúde ou autoridade sanitário”, o que acaba por sujeitar o artigo a interpretações muito abertas que podem trazer prejuízo à privacidade dos pacientes.

De outro modo, empresas privadas do ramo da saúde são “serviços de saúde”? Qual autoridade sanitária teria acesso a dados? Quais dados? Como se realizaria a coleta destes dados de maneira a não apreender mais do que o necessário?

A resposta necessariamente deverá passar pelo cumprimento dos requisitos obrigatórios do art 6º da LGPD,

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I -Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II -Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização E prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Ou seja, ainda que não tutelado pelo consentimento, o paciente ao ter o dado pessoal, ou dado sensível, tratado deverá ter respeitados seus direitos que, resumidamente, se enquadrariam no entendimento que somente teriam os dados da finalidade específica do tratamento, no limite de suas necessidades e com toda a segurança sobre quem realizaria este tratamento.

Tal postura por parte dos agentes de tratamento é garantido pela possibilidade de, em caso de descumprimento do mesmo, estão sujeitos à aplicação de sanções administrativas, a serem aplicadas pela Autoridade Nacional de Proteção de Dados, previstas na legislação aplicável. Sanções serão aplicadas com exclusividade pela Autoridade Nacional, indo desde advertência até multas de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil em seu último exercício, excluídos os tributos, limitada ao total de R\$ 50.000.000,00 por infração.

Sobre a finalidade dos dados médicos, a ser observada na coleta sem consentimento, os mesmos devem atender a um propósito explícito e informado ao usuário, ainda que posteriormente. Ou seja, se previamente coletada a informação dada a urgência de saúde do paciente, posteriormente ao mesmo deve ser informado que específico dado foi coletado para determinado fim. Exemplo, se levantado determinado exame clínico ou histórico médico, o paciente tem que ser informado que tal

levantamento ocorreu para atender uma finalidade expressa, dita por quem o atende, com o fim de assegurar sua saúde.

Sobre a necessidade, o paciente deverá ter a garantia que somente dados médicos necessários ao atendimento foram tratados, não se permitindo utilização de dados não relacionados ou sem ligação direta ao tratamento.

Ainda, o paciente deve ter claramente e expressamente garantido pelo prestador do serviço de saúde a incolumidade de seus dados, bem como a garantia do manuseio do mesmo exclusivamente por quem o utiliza para o tratamento.

O Conselho Federal de Medicina (CFM) publicou em 2002 a resolução que estabelece o prazo mínimo de 20 anos partir do último registro, para a preservação dos prontuários médicos em suporte de papel. O papel só pode ser eliminado após o arquivamento dos dados, por microfilmagem ou de outra forma. Para isso, o CFM também determina que todas as instituições de saúde tenham uma Comissão de Revisão de Prontuários. Sua função é a de resguardar as informações contidas nos prontuários médicos, que representam documentos valiosos para o paciente e para o médico

RESOLUÇÃO CFM Nº 1.821/2007

Art. 8º Estabelecer o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmado ou digitalizado.

CONCLUSÃO

A proteção do direito constitucional à privacidade evoluiu juntamente com a sociedade, dando origem à ramificação autônoma da proteção de dados pessoais.

Tal derivação evoluiu paulatinamente na legislação e jurisprudência brasileiras, atingindo o status de autodeterminação informativa. É neste contexto, nacional e internacional, que surgiu a Lei Geral de Proteção de Dados, cuja entrada em vigor de direitos e obrigações relevantes a titulares de dados e agentes de tratamento deu-se em 16 de agosto de 2020.

A área da saúde será uma das mais atingidas pela Lei Geral de Proteção de Dados. Desde o conceito de dados sensíveis, bases legais restritas, até mesmo limitações ao compartilhamento, tudo o que se fizer com dados pessoais, ainda que apenas

armazená-los, deverá ter uma finalidade, necessidade justificável e seguranças assegurados e informados ao dono do dado.

Será necessário um novo compliance a fim de adequar profissionais de saúde, serviços de saúde ou autoridade sanitárias a se adequarem à nova realidade no tratamento pessoais. Isso envolve documentar e comprovar o cumprimento de todos os requisitos legais sobre a privacidade e a proteção de dados, intenso uso de algoritmos de inteligência artificial para fins de medicina preventiva e diagnóstica, o setor passará por profundas alterações, As atividades que são consideradas como atividades de tratamento estarão sujeitas à lei. Titulares poderão exigir informações e providências sobre o tratamento de seus dados pessoais, e terão que ser que atendidas no prazo.

Sobre a possibilidade de tratamento de dados pessoais e dados pessoais sensíveis para fins de tratamento de saúde sem o prévio consentimento do usuário paciente, dada a possibilidade de urgência, a mesma deve e pode ocorrer, desde que obedecidos os parâmetros legais apontados em lei para o tratamento de dados em geral.

Ou seja, a não exigência do consentimento apenas deverá significar autorização da coleta previamente, mas os direitos dos usuários deverão ser resguardados durante todo o tratamento dos dados e, posteriormente, o mesmo deverá ser totalmente informado de todos os dados utilizados, todos os procedimentos de tratamento operacionalizados e, caso seja de sua vontade, a garantia da eliminação posterior desses dados.

Diante de todo o exposto fica claro que os dados devem ser protegidos e a coleta não pode ser maior que identifique a pessoa, e que deve ser tratado de forma responsável, se for coletado além do necessário fica a empresa sujeita a comprovação da necessidade da coleta e caso não há faça fica sujeita a sanção.

REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, Augusto Paes de. Gestão de Risco. In CABRAL, Carlos; CAPRINO, Willian (org.). **Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados**. Rio de Janeiro: Brasport, 2015.

BRASIL. **Lei n. 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.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de outubro 2020.

EXAME.: **Bom para as empresas, adiamento da LGPD pode prejudicar o consumidor.** [s.l.]: Abril, 07 maio 2020.
Disponível em: <<https://exame.abril.com.br/tecnologia/bom-para-as-empresas-adiamento-da-lgpd-pode-prejudicar-o-consumidor/>>. Acesso em: 13 setembro 2020.

GRAY, David E.. **Pesquisa no mundo real.** 2. ed. Porto Alegre: Penso, 2012.
Disponível em:
<https://sagahcm.sagah.com.br/sagahcm/sagah_ua_dinamica/15266836#leia> Acesso em: 20 outubro 2020.

MARCONDES, Juliana. **Quem é o Data Protection Officer?** . Disponível em:
<<https://www.itchannel.pt/news/negocios/quem-e-o-data-protection-officer>>. Acesso em: 12 de maio de 2020.

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

OLIVEIRA, Ana Paula de et al. A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA NA PRÁTICA EMPRESARIAL. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, p. 172-200, maio 2019. Quadrimestral. Disponível em: <<http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-9.pdf#page=172>>. Acesso em: 11 outubro 2020.

OLIVEIRA, Sandro. **Guia inicial de aplicação da LGPD: Segurança em plataformas digitais.** 2019. Edição do Kindle. Disponível em: <<https://www.amazon.com/Guia-inicial-aplica%C3%A7%C3%A3o-LGPD-plataformas/dp/1672032261>>. Acesso em 11 de outubro de 2020.

PORTO, VIVIANE. **Descomplicando a Lei Geral de Proteção de Dados.** Goiânia: Amazon. 2020.

SILVA, Felipe. **Gestão de Identidades e Acessos.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção.** São Paulo: Saraiva, 2017.