UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE DIREITO

Letícia Seibel Siqueira

PROTEÇÃO E SIGILO DOS DADOS MÉDICOS: UMA ANÁLISE SOB A ÓTICA DO DIREITO À INTIMIDADE E À VIDA PRIVADA DOS PACIENTES

Santa Maria, RS
2017

Letícia Seibel Siqueira

PROTEÇÃO E SIGILO DOS DADOS MÉDICOS: UMA ANÁLISE SOB A ÓTICA DO DIREITO À INTIMIDADE E À VIDA PRIVADA DOS PACIENTES

Monografia apresentada ao Curso de Direito, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Direito**.

Orientador: Prof. Dr. Rafael Santos de Oliveira

Santa Maria, RS
2017

Letícia Seibel Siqueira

PROTEÇÃO E SIGILO DOS DADOS MÉDICOS: UMA ANÁLISE SOB A ÓTICA DO DIREITO À INTIMIDADE E À VIDA PRIVADA DOS PACIENTES

Monografia apresentada ao Curso de Direito, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Direito**.

Aprovado em 12 de dezembro de 2017:

Rafael Santos de Oliveira, Dr. (UFSM)
Presidente/Orientador

Bruno Barros, Me. (FAMES)

João Pedro Seefeldt, Mestrando. (UFSM)

Santa Maria, RS
2017

DEDICATÓRIA

À minha avó, Luecy Leonardo Siqueira, sempre presente em minha memória e coração, e aos meus pais, Ernani e Adelaide, suportes e símbolos de amor, altruísmo e garra.

RESUMO

PROTEÇÃO E SIGILO DOS DADOS MÉDICOS: UMA ANÁLISE SOB A ÓTICA DO DIREITO À INTIMIDADE E À VIDA PRIVADA DOS PACIENTES

AUTOR: Letícia Seibel Siqueira
ORIENTADOR: Rafael Santos de Oliveira

Este trabalho apresenta um estudo do nível de proteção e de sigilo conferido aos dados médicos a partir do enfoque do direito à intimidade e à vida privada dos pacientes. Por meio deste, procura-se analisar condutas e estratégias para a proteção dos dados pessoais dos usuários de sistemas de saúde, relacionando-as à eventual necessidade de criação de uma legislação brasileira que tutele as informações de caráter pessoal da população, considerando a lacuna temática existente na legislação pátria. Através da utilização do método de abordagem dedutivo, a pesquisa parte da análise ampla e geral das perspectivas europeias e brasileiras sobre a proteção da privacidade e do tratamento de dados, e adentra nos possíveis riscos, desafios e limites à garantia da privacidade dos pacientes. A concretização do trabalho é realizada, também, a partir da utilização dos métodos de procedimento comparativo e monográfico, analisando-se o ciclo vital completo dos dados médicos, aplicando-se as técnicas de pesquisa bibliográfica e documental. Os resultados obtidos demonstraram que normas éticas e setoriais não se demonstram mais suficientes para a proteção de dados médicos, urgindo-se a necessidade de regulação legislativa específica da matéria, em face dos desafios contemporâneos surgidos em decorrências das novas tecnologias.

Palavras-chave: Dados pessoais. Informações de saúde. Direito à privacidade.

ABSTRACT

MEDICAL DATA PROTECTION AND CONFIDENTIALITY: AN ANALYSIS UNDER THE OPTICS OF THE PATIENT'S RIGHT TO INTIMACY AND PRIVATE LIFE

AUTHOR: Letícia Seibel Siqueira
ADVISOR: Rafael Santos de Oliveira

This paper presents a study of the level of protection and confidentiality given to medical data based on the patient's right to intimacy and private life. The purpose of this study is to analyze behaviors and strategies for personal data's protection of healthcare systems users, relating them to the possible creation of a Brazilian legislation that protects population's personal information, considering the country's thematic gap. Through the use of the deductive approach, the research starts from the general analysis of the European and Brazilian perspectives on the protection of privacy and data processing, and adresses the possible risks, challenges and limits to the guarantee of patient's privacy. The work is also carried out by using the comparative and monographic procedures, analyzing the complete life cycle of the medical data, as well as applying bibliographic and documentary research techniques. The results showed that ethical and sectoral rules do not prove to be sufficient for the medical data protection. Thus, it is urgent the need for specific legislative regulation of the subject, due to the contemporary challenges arisen from the new technologies.

Keywords: Personal data. Health information. Right to privacy.

SUMÁRIO

1 INTRODUÇÃO

A preocupação com o tratamento conferido aos dados pessoais, diferentemente do ocorrido nos países europeus, que atribuem amplo respeito à proteção e à privacidade das informações pessoais dos indivíduos, garantidas por meio de uma sólida normatização, revela-se ainda incipiente no Brasil, haja vista o país silenciar legislativamente acerca do assunto.

A crescente estruturação em rede da sociedade, com a sedimentação, em grande volume, das informações em bancos de dados informatizados e interconectados, alertou para o uso indevido e para o acesso descontrolado aos dados de caráter pessoal. A consequência inevitável de tal processo foi a banalização do direito à privacidade, na medida em que o indivíduo desconhece totalmente o destino que será atribuído aos seus dados, que não raro desvirtua-se do fim que legitimou sua coleta.

Importantes e sensíveis ramificações dos dados pessoais são os dados médicos, também chamados de dados clínicos ou, simplesmente, de informações de saúde. O alto potencial discriminatório e lesivo de tais dados é o que impulsiona a imprescindibilidade de sua proteção e preservação, como forma de garantir o direito à dignidade, ao sigilo e à vida privada de seus titulares.

A inviolabilidade da intimidade e da vida privada é um direito humano fundamental constitucionalmente previsto, entretanto, a falta de transparência em relação ao concreto uso e destino dos dados médicos da população imprime significativa sensação de vulnerabilidade e risco à efetividade de tais comandos constitucionais. Existe, por conseguinte, a importante e pulsante necessidade de investigação, por meio da presente pesquisa, do efetivo tratamento atribuído aos dados médicos e pessoais, a fim de que a proteção à privacidade e à vida particular dos indivíduos seja realidade prática e não somente mero conceito teórico e normativo.

Nesse sentido, o presente trabalho debruça-se sobre o manejo e a utilização das informações dos usuários dos sistemas de saúde e a necessidade de proteção e sigilo de seus dados médicos e pessoais, uma vez que, no contexto brasileiro, o armazenamento e o posterior uso dos dados médicos revestem-se de certa obscuridade e conduzem em incertezas os pacientes que utilizam clínicas, hospitais e laboratórios, quanto ao destino das informações lá depositadas.

A problemática apresentada nesta análise leva em consideração a importância e a sensibilidade inerente aos dados médicos, considerados ramificações dos dados pessoais, preocupando-se com sua potencial exposição indevida e com a garantia do direito à intimidade e à privacidade dos pacientes. Tal preocupação e decorrente anseio pela devida reflexão técnica sobre o assunto fundamentou-se em experiências vivenciadas em um estágio extracurricular realizado pela autora do presente trabalho, no setor jurídico de um hospital público, onde eram frequentes as tentativas – e até mesmo quebras – da barreira da privacidade.

Assim, objetiva-se a investigação das condutas e estratégias empregadas para a garantia da proteção e do sigilo dos dados médicos e pessoais dos pacientes, relacionando-as à eventual necessidade de criação de uma legislação brasileira que tutele as informações de caráter pessoal da população. Para tanto, é apresentado o atual panorama normativo europeu e brasileiro acerca da proteção dos dados pessoais e aprofundada a classificação e a inserção dos dados médicos e de saúde no contexto da conceituação dos dados pessoais.

Ademais, é examinado o processo de coleta, armazenamento e manipulação dos dados médicos, identificando-se as possibilidades de ofensa à intimidade e à vida privada dos pacientes no seu manejo. Ao final, são investigadas as vantagens e os malefícios do uso de tecnologias de informação e comunicação (TICs) no processamento e tratamento dos dados de saúde e analisada a necessidade latente de criação de uma legislação específica, no Brasil, como instrumento de proteção dos dados médicos e pessoais.

Este trabalho está estruturado na utilização do método de abordagem dedutivo. A partir de uma análise ampla e geral do tratamento conferido aos dados pessoais no âmbito dos países integrantes da União Europeia, adentra-se na perspectiva brasileira, considerando-se os possíveis riscos, desafios e limites à garantia da privacidade dos pacientes, e concluindo-se sobre a possível necessidade de criação de uma normativa de proteção aos dados pessoais. Ainda, para a concretização do estudo, são utilizados os métodos de procedimento comparativo, expondo-se o avançado quadro europeu de proteção em relação ao incipiente panorama brasileiro e o monográfico, analisando-se a completa trajetória dos dados médicos, desde a sua coleta até seu posterior manejo, e examinando-se,

para tanto, casos concretos de desrespeito à privacidade em decorrência da divulgação errônea de tais informações.

São utilizadas, ainda, as técnicas de pesquisa bibliográfica e documental, aliando-se a colheita de informações em artigos, teses, dissertações, livros e publicações anteriores sobre a temática à utilização de documentos informativos de hospitais, clínicas, laboratórios, bem como de repartições públicas e privadas relacionados ao assunto proposto.

A pesquisa está estruturada em dois capítulos, o primeiro subdividido em três partes, a fim de explorar as perspectivas europeias e brasileiras da normatização da proteção de dados pessoais, além de conceituar e inserir os dados médicos e de saúde na visão jurídica. O segundo, subdividido igualmente em três partes, dedica-se à análise da trajetória das informações de saúde, a partir da sua coleta até o posterior armazenamento, incluindo a perspectiva da *e*-saúde e dos bancos de dados informatizados, com a posterior reflexão acerca da necessidade de criação de legislação específica no ordenamento brasileiro.

2 A PROTEÇÃO E O SIGILO DOS DADOS PESSOAIS E MÉDICOS: PERSPECTIVAS EUROPEIAS E BRASILEIRAS

Atualmente, cerca de 120 países – incluindo múltiplos Estados latino-americanos -, norteados pelas normativas europeias, já editaram legislação específica de proteção dos dados pessoais, em clara percepção dos riscos inerentes à ampla disseminação e ao tratamento desenfreado das informações de caráter pessoal.

Os países integrantes da União Europeia, pioneiros na tutela estatal do tema, atribuem amplo respeito à proteção e à privacidade dos dados pessoais, garantidos por meio de uma sólida normatização, motivo pelo qual essa receberá dedicação e estudo próprios em subcapítulo do presente trabalho.

O Brasil, por outro lado, apresenta-se em um patamar inferior, haja vista que, até os dias atuais, não possui leis que assegurem de forma ampla a segurança de dados.

Desse modo, visando à confecção de uma análise sobre a existência de regras definidas, nacionais e internacionais, que englobem garantias e direitos aos cidadãos acerca de suas informações pessoais, neste capítulo será realizada uma breve exposição a respeito da legislação europeia (2.1), seguida pelo estudo de possíveis normativas e disposições brasileiras sobre o tema (2.2). Por fim, para introdução do estudo sobre o tratamento e o sigilo dos dados médicos e de saúde, realizar-se-á sua contextualização e conceituação como ramo importante dos dados pessoais (2.3).

2.1 O EFICIENTE SISTEMA EUROPEU DE PROTEÇÃO DE DADOS

A evolução tecnológica, o uso massivo e crescente dos computadores, e o surgimento da *internet* e das tecnologias de informação e comunicação, em meados da década de 70 do século passado, foram contemporâneos às primeiras reflexões jurídicas e consequentes legislações existentes sobre o tema da proteção dos dados pessoais.

Registra-se, desde já, que o sistema protetivo criado para as bases de dados e para as informações de caráter pessoal é fruto do direito geral de personalidade, dentro do qual está inserido o direito à vida privada, igualmente inspirador para o

advento do tratamento legislativo da privacidade e da proteção dos dados em escala mundial.

A Declaração Universal dos Direitos Humanos, adotada e proclamada pela Assembleia Geral das Nações Unidas em 10 de dezembro de 1948, já havia previsto, em seu artigo 12[1], o direito humano à proteção da lei contra interferências ou ataques à vida privada, à família, ao lar, à correspondência, à honra ou à reputação.[2]

Do mesmo modo, a Convenção Europeia dos Direitos do Homem, adotada pelo Conselho da Europa em 04 de novembro de 1950, corroborou, por meio do artigo 8º[3], o direito ao respeito pela vida privada e familiar[4], integrando referida proteção a um conjunto de direitos indispensáveis para a vida humana, em claro aporte ao princípio da dignidade humana.

No entanto, o emprego de *softwares*, equipamentos e computadores para o tratamento de dados pessoais, o processamento desses de maneira intensa, e a criação de bancos ou bases de dados elevaram a importância da informação pessoal a tal patamar que ela passou a se tornar o núcleo principal da temática da privacidade e intimidade, desintegrando seu conceito clássico ao efetuar atualizações, impor contornos próprios e dar continuidade à sua disciplina. Segundo dicção do doutrinador Danilo Doneda:

> A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das

---

[1]Cujo teor é o seguinte:
Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[2]ONU. Organização Das Nações Unidas. **Declaração Universal dos Direitos Humanos**. ONU: 1948. Disponível em: <http://www.onu.org.br/img/2014/09/DUDH.pdf>. Acesso em: 22 set. 2017.

[3]De seguinte teor:
1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

[4]CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**. Roma: 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 22set. 2017.

> informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.[5]

Assim, o desenvolvimento das tecnologias informacionais e a sucessiva ressignificação do conceito de proteção da privacidade, como além do direito de ser deixado ou de estar só - "*right to be alone*"[6] -, também o direito de manter controle sobre as próprias informações, atualizando-o para uma proteção específica do tratamento autônomo dos dados pessoais, demandou dos países novos perfis jurisprudenciais e legislativos.

Os ordenamentos jurídicos comunitários e nacionais dos Estados integrantes da União Europeia, portanto, foram vanguardistas na reformulação das leis de proteção das informações de caráter pessoal, a partir do novo enfoque formulado para o tópico da privacidade e intimidade, seguidos por ordenamentos nacionais de múltiplos países não europeus.

Mencionado enfoque, construído ao longo de aperfeiçoamentos legislativos iniciados na década de 70, pode ser descortinado com o estudo da teoria evolutiva das leis de proteção de dados pessoais criada por Viktor Mayer-Scönberger, que "vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento dos de dados (...)"[7].

A título exemplificativo da primeira dessas quatro gerações, cita-se a lei editada pelo Estado alemão de Hesse, em 1970 – que se preocupava com o manejo mecânico dos dados pela administração pública -, e o *Datalegen* da Suécia (Lei 289 de 11 de maio de 1973). A partir dos ensinamentos de José Adércio Leite Sampaio, compreende-se que, considerando a intimidação dos juristas frente ao surgimento de novas tecnologias, computadores e *internet*, a elaboração das primeiras legislações focou em imaginários grandes centros concentradores e elaboradores de

---

[5]DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

[6]Este conceito e construção jurídica surgiu, originalmente, em um artigo publicado por dois juristas norte-americanos, Samuel D. Warren e Louis D. Brandeis, na *Harvard Law Review*, intitulado *The Right to Privacy*. BRANDEIS, Louis D.; WARREN, Samuel D. The Right to Privacy. **Harvard Law Review**, v. IV, 1980. Disponível em: < http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>. Acesso em: 16 dez. 2017.

[7]DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

dados, normatizando a concessão de autorização para sua criação e a posterior regulação por órgãos públicos.[8]

Os primeiros ordenamentos existentes, por conseguinte, concentraram seus esforços na aplicação de princípios gerais e abstratos de proteção dos dados pessoais, condicionando sua estrutura exclusivamente à ótica dos notáveis bancos de dados. Contudo, a multiplicação e a resultante fragmentação dos centros de processamento e tratamento de dados informatizados inviabilizaram a continuação da condução jurídica do tema sob o prisma exarado nas primeiras legislações.

Surge, assim, a segunda geração, representada por leis como a *Bundesdatenschutzgesetz*, a lei federal da Alemanha sobre proteção de uso ilícito de dados pessoais, de 1977, a *Informatique et Libertées* (Lei 78-17 de 6 de janeiro de 1978), lei francesa de proteção das informações de nível pessoal, além das legislações austríaca (Lei 565 de 18 de outubro de 1978) e dinamarquesas (Leis 243 e 244, ambas de 08 de julho de 1978) de regulamentação da matéria.

Frisa-se que o impasse com relação ao uso do fenômeno informático e o necessário resguardo dos dados pessoais alcançaram status constitucional, a nível europeu, a partir do artigo 35 da Constituição Portuguesa de 1976[9] e do artigo 18.4 da Constituição Espanhola de 1978[10].

---

[8]SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais da vida e da morte. Belo Horizonte: Del Rey, 1998.

[9]O artigo 35 da Constituição de Portugal no seguinte sentido determina acerca da utilização da informática e da proteção de dados:

"Artigo 35.º - Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei." PORTUGAL. **Constituição da República Portuguesa, de 2 de abril de 1976**. Disponível em <http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 04 nov. 2017.

[10] O artigo 18.4 da Constituição da Espanha previu que:

A terceira fase de leis, por sua vez, surgiu no início da década de 1980, e é apropriadamente sinalizada por meio da Convenção nº 108 do Conselho da Europa (também conhecida, simplesmente, como Convenção de Estrasburgo), instituída a nível de Comunidade Europeia em 28/01/1981. Referido documento é considerado o marco inicial do reconhecimento da proteção dos dados pessoais como um direito humano fundamental. Evidencia-se, a partir de seu artigo 1º, o objetivo e a finalidade da Convenção:

> A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).[11]

O período da terceira geração de leis é caracterizado pela tentativa de garantia efetiva dos direitos dos cidadãos sobre seus próprios dados pessoais, incluindo a participação ativa do indivíduo no processo de tratamento das suas informações, buscando colocar em prática, desse modo, um eficaz direito à autodeterminação informativa. Mencionado ciclo preocupa-se, ainda, com o desenvolvimento pleno do setor da informática, garantindo a sua não obstrução. Além da Convenção de Estrasburgo, são exemplos dessa geração a Lei da Grã-Bretanha de 12/7/1984 e a nova Lei alemã de 20/12/1990[12].

Frisa-se que o nascimento do pensar de um direito à autodeterminação e a privacidade informacional – ou seja, o direito e a capacidade de um indivíduo ponderar, desde o princípio, acerca da obtenção, uso, exibição e transmissão dos seus dados pessoais - ocorreu no Tribunal Constitucional Federal Alemão (TCFA), em sentença proferida em 15 de dezembro de 1983, sobre a Lei do Censo – a

---

"Artículo 18. [...]
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." ESPANHA. **Constituição Espanhola, de 27 de dezembro de 1978**. Disponível em <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Acesso em: 04 nov. 2017.

[11]UNIÃO EUROPEIA. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Diretiva 108 de 1980. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 23 set. 2017.

[12] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

chamada *Volkszahlunsurteil* – declarada parcialmente inconstitucional. Conforme explicita o professor Danilo Doneda:

> A autodeterminação informativa, de fato, surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa para a utilização de seus dados pessoais, porém procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros; estas leis incluem também garantias específicas como o dever de informação.[13]

Ou seja, o conceito de autodeterminação pressupõe uma liberdade de decisão e de controle do indivíduo sobre as suas informações, as quais, na sociedade atual, ditam nuances e características da personalidade exterior e objetiva de cada pessoa. O cidadão, para tanto, necessita do direito de acesso aos seus dados, obtendo, assim, o fator de julgamento próprio e individual sobre as ações ou omissões que realizará ou não.[14]

Constatou-se, contudo, que a autodeterminação informacional possuía caráter extremamente exclusivista, visto que os altos custos sociais e econômicos para o exercício efetivo de tal prerrogativa condicionava-a a um privilégio de uma minoria, restando aos demais a simples aquiescência com as situações, condições e tratamentos oferecidos aos seus dados pessoais.[15]

Em decorrência de manifesta desigualdade, a quarta geração de leis de proteção de dados desponta visando superar a abordagem, até então, meramente individualista fornecida à questão. Os ordenamentos posteriores passam a fornecer, dessa maneira, instrumentos que elevam o patamar das decisões e escolhas coletivas de proteção, concretizando de maneira objetiva o direito à autodeterminação informativa.

---

[13]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
[14]SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.
[15]DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

A partir da análise da Diretiva 95/46/CE – relativa à proteção de pessoas físicas quanto ao tratamento e livre circulação de seus dados pessoais - do Parlamento Europeu e do Conselho da Europa, instituída em 24/10/1995, e da Diretiva 2002/58/CE (posteriormente substituída pela Diretiva 2009/136/CE) – que normatiza direitos dos usuários em relação às comunicações eletrônicas, serviços de redes sociais e *e-commerce* -, percebem-se as técnicas utilizadas por referido grupo legislativo para o fortalecimento do padrão coletivo de proteção. Dentre os artifícios aplicados, passíveis de citação são a decadência da importância das decisões individualistas de autodeterminação, o reconhecimento da relação de desequilíbrio existente entre indivíduo e empresas de coleta e processamento de dados, a criação de órgãos exclusivos e independentes para garantir o cumprimento e a eficácia das normas de proteção, além da importante segmentação das áreas, com o surgimento de normativas complexas, com regras próprias de processamento de dados para setores específicos, como para o setor de saúde (objeto concreto do presente trabalho), por exemplo[16].

Quanto a Diretiva 95/46/CE (*Personal Data Protection Directive*), em específico, importante consignar que foi por meio dela que os países europeus passaram a se organizar, em nível comunitário, na montagem de um sistema mínimo de proteção de dados pessoais e de segurança, haja vista que nem todos os Estados-Membros já haviam adotado, à época, uma legislação referente à proteção das informações de caráter particular[17]. Sintetiza-se em dois os propósitos da Diretiva, em total consonância com os pressupostos da integração europeia: a concretização de um mercado interno, no caso, por meio da livre circulação de dados, e, ao mesmo tempo, a proteção dos direitos fundamentais dos cidadãos. Conforme acertadamente explicita Têmis Limberger:

> Os fluxos de dados não ocorrem somente nas fronteiras de um país, por isso a necessidade da DC 95/46, que colabora para a resolução dos problemas nos países comunitários, mas ainda não contempla os demais

[16] UNIÃO EUROPÉIA. Directiva 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. **Official Journal**, Luxemburgo, L 281, 23 Nov. 1995, p. 0031 – 0050. Disponível em: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 19/09/2017.

[17] Conforme previa o artigo 1º: "1. Os estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

> Estados. O comércio e o intercâmbio de informação e de dados são necessários, são quase uma demanda da sociedade atual, e por isso impõe-se a tutela dos direitos fundamentais. A globalização pressupõe e propõe uma economia sem fronteiras e sem regulamentação. No entanto, não se pode desprezar anos de construção de direitos fundamentais e mudar tudo isso por uma única lei: a lei de mercado e a ilusão de que o mercado tudo regulará. O grande desafio que se impõe no plano dos direitos fundamentais é como fazer com que não somente o capital e os bens de consumo circulem em todo o mundo, mas também os direitos. O ideal seria a universalização dos direitos nos cinco continentes.[18]

A autora utiliza-se da expressão "globalização" como fator motivador do fluxo internacional de dados e informações entre os países. Contudo, a globalização como um fenômeno "*está se impondo como uma fábrica de perversidades*"[19], como bem conceitua o geógrafo Milton Santos, pois gera, como sua consequência, a mercantilização das informações e dos dados pessoais dos cidadãos, agregando-lhes fator monetário.

A Diretiva 9546, segundo Têmis Limberger, foi gradualmente sendo transcrita pelos países europeus aos seus próprios ordenamentos nacionais, apontando-se, como exemplo, o caso da Espanha, que internacionalizou a DC 95/46 por meio da *Ley Orgánica 15/1999*, sobre a *Protección de Datos de Carácter Personal (LOPD)*. Consigna-se que o dia 01/01/1999 foi delimitado como marco final para o cumprimento das disposições previstas na Diretiva pelas instituições comunitárias europeias.

Todavia, ainda que a DC 95/46 seja um marco normativo na proteção e segurança dos dados pessoais, e, consequentemente, da privacidade e intimidade, os cidadãos ainda consideravam-na ineficiente, visto que havia uma lacuna entre o disposto no texto legal e a sua real aplicação efetiva. Havia, também, queixas de disparidades e divergências entre a legislação comunitária e as ordenações internas de cada Estado-Membro da União Europeia, o que dificultava a uniformização de uma política pan-europeia de proteção de dados[20].

Desse modo, após cerca de quatro anos de negociações, o Jornal Oficial da União Europeia publicou, no dia 04 de maio de 2016, o Novo Regulamento Geral de Proteção de Dados – Regulamento 2016/679 do Parlamento Europeu e do

---

[18]LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.
[19]SANTOS, Milton. **Por uma outra globalização**: do pensamento único à consciência universal. Rio de Janeiro: Editora Record, 2001, p. 19.
[20]LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

Conselho, que revoga a Diretiva 95/46/CE[21] -, que entrou em vigor no dia 25 de maio do mesmo ano, possuindo, como período transitório para sua total aplicação e adaptação, dois anos.

Mencionada normativa supera a problemática de uniformização apresentada pela DC 95/46, uma vez que, como se trata de um Regulamento, torna-se aplicável de maneira direta aos 28 países-membros da EU, não apresentando necessidade de transposição para cada jurisdição interna. Por conseguinte, a sonhada harmonização legislativa em todos os países da União Europeia, em nível de proteção das informações pessoais, torna-se, finalmente, factível. Grifa-se que o Novo Regulamento instaura mudanças significativas às normas previamente apresentadas pela Diretiva 95/46/CE, tendo em vista que impõe às instituições e organizações novas obrigações, estabelecendo elevadas multas em caso de descumprimento, além de introduzir novos conceitos e princípios que devem nortear o tratamento dos dados.

Visualiza-se, finalmente, que na comunidade europeia:

> [...] se reforça a metodologia do consentimento expresso e a posição jurídica da pessoa afetada, prestigiando-se os direitos fundamentais e criando instrumentos de apoio na proteção como a figura do Data Protection Officer como uma entidade protetora de dados a exemplo da Agencia Española de Protección de Datos (AEPD).[22]

Neste particular, destaca-se o papel essencial desenvolvido pelas Autoridades Garantidoras – *National Data Protection Supervisory Authority* – que desenvolvem políticas públicas, monitoram e adotam critérios para a aplicação e

---

[21]O artigo 1º, cujo teor encontra-se abaixo colacionado, explicita o objeto e objetivos do Regulamento 2016/679:
"1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais."

[22]SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. "Big Data" Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.

para a interpretação das leis de proteção de dados, haja vista a evolução constante das tecnologias e a necessária adaptação da norma vigente a tais avanços[23].

Verifica-se, de forma convincente, que os diversos ordenamentos jurídicos apontados no presente subcapítulo demonstram uma tendência para o tratamento autônomo da proteção de dados pessoais, vindo a formar bases sólidas para o nascer de um direito fundamental humano à proteção das informações. As soluções legislativas encontradas pelos países europeus, dessa maneira, convergem rumo ao robustecimento de princípios básicos de proteção (v.g., princípio da publicidade, da finalidade e do livre acesso), indo ao encontro dos direitos fundamentais e da proteção da intimidade e da privada da pessoa.

Os Estados europeus, reverberando seu *status* de sociedade plural e democrática, reconheceram a importância do livre desenvolvimento da personalidade de seus cidadãos e, consequentemente, avançaram nas construções legislativas com o intuito de proteger os indivíduos de intromissões indevidas a seus dados pessoais. Posição diferente é adotada pelo Estado brasileiro, como restará melhor explicitado no subtítulo seguinte.

2.2 O PANORAMA BRASILEIRO SOBRE A PROTEÇÃO DA PRIVACIDADE E O TRATAMENTO DE DADOS

No Brasil ainda perdura um silêncio legislativo quanto ao pontual tema da proteção dos dados pessoais, indo o país de encontro à relevância da problemática, uma vez que as informações pessoais, nos dias atuais, assumem o papel dos próprios indivíduos no espaço informático. A inexistência de leis no Brasil está em sentido contrário aos mais de 120 países que já proporcionaram aos seus cidadãos garantias e direitos sobre os dados de caráter pessoal.

A leitura do item 2.1 deste trabalho permite a visualização do contexto no qual ocorreu o desenvolvimento histórico e legislativo da proteção de dados, em especial no continente europeu, a partir da década de 1970. A *contrario sensu*, pertinente a reflexão acerca da situação institucional enfrentada pelo Brasil na mesma época:

---

[23]LIMA, Cíntia Rosa Pereira de. O Conceito de Tratamento de Dados Após o Caso Google Spain e sua Influência na Sociedade Brasileira. **Conpedi Law Review**, v. 1, n. 9, p. 117-140, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/42/39>. Acesso em: 01 out. 2017.

> Se se questionar o porquê desse desenvolvimento na Europa, especialmente, e também nos Estados Unidos (e não no Brasil, por exemplo), sob o ponto de vista das condições político institucionais que passava o país nas décadas de sessenta a oitenta, em uma ditadura militar, cujo último interesse é fortalecer a posição jurídica dos cidadãos enquanto detentor de direitos, pode-se chegar à conclusão de que é necessário um ambiente de razoável estabilidade democrática, como gozava (e goza) o continente europeu, para que o debate sobre a proteção de dados enquanto proibição de intromissão do Estado na esfera privada.[24]

Não obstante, passados cerca de 50 anos de aludido espaço temporal, o Brasil ainda não regulamentou, especificamente, a matéria da proteção de dados pessoais, possuindo apenas algumas previsões na Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet -, e outras na Lei nº 9.507, de 12 de novembro de 1997 – Lei do *Habeas Data* -, além de disposições gerais sobre privacidade encontradas na Constituição Federal e em outras leis esparsas.

Ainda que a Constituição brasileira tenha sido diretamente influenciada pelas Cartas Portuguesa e Espanhola, que contemplam o resguardo da intimidade defronte à informática e ao uso sensível dos dados através das novas tecnologias, comando semelhante não é abrangido pela normativa constitucional brasileira.

A Carta Magna brasileira estabelece, em seu artigo 5º[25], um rol meramente exemplificativo de direitos fundamentais garantidos a todos os cidadãos. Entre eles, são pertinentes ao objeto do presente estudo o disposto no inciso X, que assegura a inviolabilidade a vida privada e a intimidade, no inciso XII, acerca da interceptação de comunicações telefônicas, telegráficas ou de dados e no inciso LXXII, que instaurou o *habeas data*.

Ainda, passível de citação a Declaração de Santa Cruz de La Sierra, redigida em decorrência da XIII Cumbre Ibero-Americana de Chefes de Estado e do

---

[24]ASSMAN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro**. Florianópolis: UFSC, 2014. 65 p. Monografia, Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2010.

[25]"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; [...]

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

LXXII - conceder-se-á *habeas data:*

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [...]"

Governo, evento que possuía como tema “A inclusão social, motor do desenvolvimento da Comunidade Ibero-Americana”. A declaração foi assinada pelo Estado brasileiro no dia 15/11/2003, sendo que, em referido documento, há menção explícita à proteção de dados pessoais como um direito fundamental das pessoas[26].

A nível infraconstitucional, observa-se que o texto do Código de Defesa do Consumidor (Lei nº 8.078/1990), através dos artigos 43 e 44, prevê um conjunto de regras e princípios aos detentores dos bancos de dados, dando guarida às informações pessoais dos consumidores lá armazenadas ou em cadastros. Ocorre o amparo, portanto, aos dados introduzidos em processos de consumo[27]. Na legislação pátria, o CDC é considerado o principal instrumento de tutela da dimensão objetiva do direito à autodeterminação, haja vista disciplinar a necessidade de acesso do usuário (consumidor) aos dados arquivados sobre ele em fichas, cadastros, registros e ações de consumo, bem como sobre as respectivas fontes competentes[28]. Salienta-se que alguns doutrinadores declaram o CDC como o marco normativo inicial, no contexto brasileiro, dos princípios básicos de proteção de dados pessoais.

O artigo 43, parágrafo 4º, do CDC aponta que “os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público”[29]. Logo, interpretando-se de maneira conjunta o dispositivo, chega-se à conclusão de que o acesso às bases de dados pessoais integrados em relações de consumo é assegurado por meio da ação de *habeas data*, considerando restar explícito nas normativas (CDC e

---

[26]O item 45 da Declaração estabelece que:
“45. Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras iberoamericanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.”

[27]O caput do artigo 43 do CDC define-se no seguinte sentido: “O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.” BRASIL. **Lei 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 30 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 20 out. 2017.

[28]KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães . A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei n. 12.965/2014). In: Newton De Lucca; Adalberto Simão Filho; Cíntia Rosa Pereira de Lima. (Org.). **Direito & Internet III - Tomo I: Marco Civil da Internet (Lei n. 12.965/2014)**. São Paulo: QuartierLatin, 2015.p. 291-367.

[29]BRASIL. Lei 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 30 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 20 out. 2017.

Lei do *Habeas Data*) a natureza pública conferida aos registros ou banco de dados (destaca-se, aqui, que o sentido conferido a esse "caráter público" inclui também bancos de dados administrados por entidades privadas)[30].

Como já acima assinalado, o *habeas data* foi inicialmente instituído a nível constitucional, a partir do artigo 5º, LXXII, da Constituição de 1988, surgindo como um instrumento para assegurar o acesso e possível retificação de informações pessoais que estejam em posse da Administração Pública, tanto direta quanto indireta. Posteriormente, houve a regulamentação do instituto pela Lei nº 9.507/1997, que determina a ocorrência de uma prévia fase administrativa em face do órgão ou banco de dados pertinente, além de prescrever as fases do processo, o rito da ação, e as demais particularidades atinentes ao instrumento constitucional[31].

O direito à autodeterminação informativa, em sua dimensão negativa, é entendido como a faculdade que possui o indivíduo de, no seu âmbito informacional e pessoal, limitar a atuação e intromissão estatal, e, assim, proteger sua esfera íntima. Mencionado direito pode ser concretizado através do *Habeas Data*[32]*,*tendo em vista que o remédio protege o cidadão contra a inserção abusiva ou ilícita de seus dados em registros, contra a manutenção de informações errôneas ou falsas, além de coibir a introdução de dados considerados passíveis de discriminação pública.

Entretanto, parte da doutrina tece críticas ao instituto, justamente por considerar que sua proteção é exercida tão somente para as liberdades negativas, possuindo amplitude de alcance muito restrita, e apresentando-se como um instrumento ineficaz à proteção dos dados pessoais frente ao atual estado vivenciado pela Sociedade da Informação[33]. Nesse sentido, compreende-se que a

---

[30]LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, v. 2, n. 1, p. 60-76, 2013. Disponível em: <http://revistas.ufpr.br/atoz/article/view/41320/25261>. Acesso em: 20 out. 2017.

[31] BRASIL. **Lei nº 9.507 de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>. Acesso em: 29 out. 2017.

[32]ASSMAN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro**. Florianópolis: UFSC, 2014. 65 p. Monografia, Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2010.

[33]DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

dimensão subjetiva do direito à autodeterminação informativa demonstra-se incompatível às garantias ofertadas pela ação de *Habeas Data*.

O Código Civil Brasileiro (Lei nº 10.406/2002), que representa a esfera civilista do ordenamento pátrio, fixa em seu Capítulo II o rol de direitos de personalidade, não admitindo qualquer limitação voluntária sobre o exercício desses direitos, determinando sua irrenunciabilidade e intransmissibilidade[34]. A inviolabilidade da vida privada da pessoa natural inclui-se nos direitos de personalidade por meio do artigo 21 do CCB[35], havendo as possibilidades de cessação e impedimento de possíveis violências por meio de determinação judicial.

Segundo entendimento da jurista Têmis Limberger, constitui-se um verdadeiro avanço a inserção dos direitos de personalidade na Parte Geral do diploma civilista brasileiro, haja vista tal seção assegurar unidade ao sistema legislativo, norteando a Parte Especial do código e os demais microssistemas, como o CDC. A autora acredita, ainda, em uma integração do sistema normativo mediante uma interpretação conjunta da Constituição Federal, do Código Civil e do Código de Defesa do Consumidor, gerando, assim, a possibilidade de uma "responsabilidade civil por danos à pessoa no tocante aos direitos da personalidade, inclusive quando houver relação de consumo"[36].

Ainda no plano infraconstitucional, cabível a citação de algumas disposições de natureza tributária e comercial, como o artigo 198 do Código Tributário Nacional (Lei nº 5.172/1966)[37], e a Lei nº 9.296/1996, que regulamentou o inciso XII do artigo

---

[34]Consoante expresso no artigo 11 do diploma civilista: "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.". BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002.** Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 26 out. 2017.

[35]O artigo 21 do Código Civil expressa que: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.".

[36]LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

[37]O qual possui, no *caput*, o seguinte teor: "Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.". BRASIL. **Lei nº 5.172 de 25 de outubro de 1966.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm>. Acesso em: 03 nov. 2017.

5º da Constituição Federal, popularmente conhecida como “lei da interceptação telefônica”[38].

Oportuna a referência, igualmente, da Lei Complementar nº 105/2011, que confere tratamento específico ao sigilo sobre as operações de instituições financeiras. Consoante disposto na referida norma, informações bancárias como aplicações em fundos de investimentos, operações com cartão de crédito, pagamentos e depósitos de valores são consideradas transações que devem estar guaridas pelo sigilo, excetuadas algumas situações, previstas na lei, que permitem às autoridades administrativas a quebra do sigilo bancário sem autorização judicial.

Entretanto, como bem observa Vinícius Borges Fortes:

> [...] metadados anônimos e até mesmo protegidos por normas de sigilo bancário, tal como prevê a lei brasileira, tornam-se dados pessoais vulneráveis, eis que passíveis de identificação da pessoa em questão, ainda que sujeitos às proteções legais, especialmente as relacionadas com a tutela constitucional e civilista da vida privada. Abrem-se, com isso, diversas possibilidades de registro e tratamento dos dados, inclusive de maneira ilícita, por governos, empresas e indivíduos. Apesar da tutela constitucional e infraconstitucional mencionada, acredita-se na necessidade de melhor compreensão da internet no âmbito jurídico, de modo a conferir maior eficácia à proteção dos direitos fundamentais [...][39].

O ordenamento jurídico brasileiro, dessa forma, iniciou sua “corrida legislativa” rumo à tutela de direitos no âmbito da Sociedade de Informação ao embraçar, finalmente, o contexto informático como um ambiente carecedor de compreensão e garantias jurídicas específicas[40]. Encontram-se vigentes, portanto, a Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei de Crimes Informáticos (Lei nº 12.737/2012) e o recente Marco Civil da internet (Lei nº 12.965/2014).

A Lei de Acesso à Informação surgiu para regulamentar o inciso XXXIII do artigo 5º, da Constituição Federal, e para assegurar, por consequência, o direito fundamental de acesso à informação. Apresentam pertinência ao tema da presente

---

[38]Consoante disposto no artigo 1º da Lei: “A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.”. BRASIL. **Lei nº 5.172 de 25 de outubro de 1966.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm>. Acesso em: 03 nov. 2017.

[39]FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

[40]Ibidem.

pesquisa as conceituações elencadas no artigo 4º de mencionado diploma normativo, destacando-se o sentido conferido ao termo “informação”, “informação pessoal” e “tratamento da informação”[41]. Registra-se a rigorosidade com que a lei disciplina o tratamento das informações pessoais, impondo restrições ao acesso dessas por terceiro, exigindo, para sua divulgação ou liberação, o prévio consentimento do detentor das informações. Ao mesmo tempo, prevê exceções legais à exigência de referido consentimento, como em caso de indispensabilidade da informação para a confecção de prevenção e diagnóstico de saúde[42].

A Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, foi a primeira normativa, de caráter genérico, a disciplinar juridicamente o

---

[41]O artigo 4º da Lei encontra-se disposto da seguinte maneira:
“Art. 4º Para os efeitos desta Lei, considera-se:
I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
[...]
IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; [...]”.

[42]Mediante previsão expressa no artigo 31 da Lei:
“Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante. [...]”BRASIL. **Lei nº 12.527 de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 nov. 2017.

uso do ambiente virtual no território nacional, além de ser a única a possuir previsões específicas de proteção de dados pessoais no espaço cibernético[43].

O artigo 2º de referido diploma permite a visualização dos fundamentos para a disciplina do uso da *internet* no Brasil. Destacam-se, dentre as previsões insertas nos dispositivos, o fundamento dos direitos humanos, do desenvolvimento da personalidade e do exercício da cidadania em meios digitais.

As previsões acima elencadas clarificam a escolha do legislador, no ainda incipiente sistema de proteção brasileiro, pela adoção do princípio à autodeterminação informativa, uma vez que visam que legislações futuras sobre o tema permitam ao detentor dos dados pessoais o controle sobre sua coleta, processamento e compartilhamento. Apontada escolha, designada como um dos objetivos primordiais do Marco Civil da Internet, é claramente constatada pela leitura do rol de direitos dos usuários previstos no seu artigo 7º, dentre os quais se ressalta os especificados nos incisos I, II, III, VII, VIII, IX e X[44].

Os princípios para a disciplina do uso da *internet* estão elencados no artigo 3º de mencionada legislação, merecendo destaque, em decorrência da pertinência para o presente estudo, a "proteção da privacidade", do inciso II, e a "proteção dos dados pessoais, na forma da lei", do inciso III.

---

[43]SILVA, Felipe Stribe da. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria: UFSM, 2015. 167p. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade Federal de Santa Maria, Santa Maria, 2015.

[44]O artigo 7º da Lei encontra-se no seguinte sentido:

"Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

[...]

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; [...]."

Todavia, Felipe Stribe da Silva aponta ressalvas à interpretação de referido rol principiológico:

> Nesta previsão princiológica, destacam-se dois pontos negativos. Inicialmente cinde a proteção à privacidade da proteção aos dados pessoais, o que pode enfraquecer este segundo valor, considerando que ele, na realidade, seria uma nova forma de proteção da privacidade, portanto, melhor seria uma previsão que afirmasse que é um princípio à proteção da privacidade por intermédio da proteção aos dados pessoais. Em um segundo momento, a previsão aparentemente condiciona a proteção específica dos dados pessoais à existência de uma Legislação sobre a temática, quando na realidade ela poderia ter elencado como princípio a mera proteção aos dados pessoais.[45]

Ainda assim, verifica-se um avanço na legislação brasileira com a entrada em vigor do Marco Civil da Internet, pois, ainda que esse não seja uma normativa geral sobre a proteção de dados pessoais, haja vista não garantir a privacidade e a proteção das informações de forma abrangente, estruturada e completa, abordou regras inovadoras, ao limitar, por exemplo, a utilização dos dados a uma série de finalidades específicas, com requisitos prévios a serem cumpridos, além de garantir a confidencialidade da comunicação, independente da natureza do provedor do serviço e a confidencialidade no armazenamento.

Visualiza-se, ainda, que o Marco Civil da Internet remeteu questões jurídicas específicas a diferentes legislações. Entretanto, para a situação de remissão a uma possível lei de proteção de dados pessoais, ainda persiste uma lacuna legislativa no ordenamento brasileiro.

Ressalta-se, no entanto, que existem propostas de regulação da proteção de dados pessoais em trâmite no complexo brasileiro. Atualmente, tramitam no Congresso Nacional dois Projetos de Lei sobre o tema: o Projeto de Lei nº

[45]SILVA, Felipe Stribe da. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria: UFSM, 2015. 167p. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade Federal de Santa Maria, Santa Maria, 2015.

5.276/2016 (apensado ao Projeto de Lei nº 4.0260/2012)[46], na Câmara dos Deputados, e o Projeto de Lei do Senado nº 330/2013, no Senado Federal[47].

Revela-se oportuno salientar que o Projeto de Lei nº 5.276/2016 é resultado de um amplo debate público promovido pelo Ministério da Justiça, por meio da Secretaria Nacional do Consumidor (Senacon), em parceria com o Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil (CGI.br). O Anteprojeto de Lei de Proteção de Dados Pessoais, durante a realização de dois debates públicos efetivados via *internet*, obteve mais de 2000 contribuições dos setores público e privado, universidades e organizações não-governamentais. Os debates ocorreram, respectivamente, nos anos de 2010 e 2015, sendo que os subsídios foram analisados, discutidos e posteriormente consolidados em um texto final[48].

A estrutura de citados projetos foi balizada por regras de diversos outros países, especialmente os europeus, atinentes à temática. Princípios como os da finalidade, transparência, segurança, necessidade, livre acesso, prevenção, qualidade e não discriminação no tratamento de dados são encontrados nos Projetos de Lei. Eles garantem, ainda, ao cidadão o controle sobre seus dados pessoais, tanto por meio de seu consentimento livre e inequívoco, como por outros instrumentos garantidores. A legitimação para o tratamento de dados encara uma série de previsões específicas, como para a proteção da vida e tutela da saúde, ou para o exercício regular de direitos em um processo judicial ou administrativo. Ao indivíduo também serão atribuídos os direitos de acesso, oposição, retificação, bloqueio, cancelamento e dissociação sobre suas informações pessoais.

Ademais, os Projetos de Lei também preveem o auxílio de uma autoridade competente, como uma espécie de órgão especializado, na tutela dos direitos e garantias sobre os dados pessoais, além de prever a ocorrência de transferência

---

[46]BRASIL. **Projeto de Lei nº 5.276/2016, de 13 de maio de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 15 out. 2017.

[47]BRASIL. **Projeto de Lei do Senado nº 330/2013, de 13 de agosto de 2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 15 out. 2017.

[48]PROTEÇÃO de Dados Pessoais. **Pensando o direito**, Ministério da Justiça, 21 outubro 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/2015/10/conheca-a-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 16 out. 2017.

internacional de dados pessoais em hipóteses peculiares[49]. Registra-se que, se aprovado, o Projeto de Lei aplicar-se-á a qualquer tratamento de dados pessoais de pessoas naturais, tanto para o setor público quanto para o privado.

Ao final, constata-se que, no ordenamento brasileiro, a proteção de dados e as garantias do tratamento automatizado desses não se estruturam com base em um único complexo legislativo. A efervescência da temática, no entanto, está acordando o Brasil da apatia vivenciada até então, sendo constatado um movimento nacional para o estabelecimento de marcos regulatórios específicos de proteção de dados pessoais.

O enfoque do trabalho sobre os dados de saúde, em específico, será garantido de maneira apropriada no subtítulo seguinte, bem como no capítulo posterior, haja vista que, até então, a presente monografia objetivou expor o atual quadro normativo europeu e brasileiro acerca da proteção dos dados pessoais.

2.3 A CONCEITUAÇÃO E INSERÇÃO DOS DADOS MÉDICOS E DE SAÚDE NO SISTEMA PROTETIVO

Preludialmente, significativa, para a assimilação do presente estudo, a especificação da diferença conceitual entre os termos “dado” e “informação”. Ainda que a carga semântica de ambos seja de fato similar, o que justifica a inexatidão, em diversas circunstâncias, na sua utilização, cada vocábulo “carrega um peso particular a ser considerado”[50].

Desse modo, a expressão “dado” possui sua finalidade baseada em uma conotação mais rudimentar, primitiva, classificando-se como o estágio anterior ao da informação, prévio ao processo de interpretação, estruturação e formação dessa. De acordo com Danilo Doneda, o dado seria setorizado a uma espécie de “pré-informação”[51]. A expressão “informação”, por seu turno, aplicar-se-ia ao estágio posterior ao da interpretação e elaboração do dado, resultando como o produto final após o processo de aquisição do conhecimento. Ou seja, “[...] a informação carrega

---

[49]DONEDA, Danilo. A proteção de dados está chegando (tarde) ao Brasil. **Gazeta do Povo**, Curitiba, 01 outubro 2017. Disponível em:<http://www.gazetadopovo.com.br/opiniao/artigos/a-protecao-de-dados-esta-chegando-tarde-ao-brasil-7kehelgsg36gs0twvvvxr63d5>. Acesso em: 15 out. 2017.
[50]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
[51] Ibidem.

também um estado instrumental, no sentido da redução de um estado de incerteza”[52].

Muitos doutrinadores, não raras vezes, utilizam os termos – dado e informação – de maneira sinônima, opção essa replicada no presente estudo monográfico, que optou por manusear de modo equivalente os vocábulos. Não obstante, para melhor visualização dos contextos e conceitos que serão trabalhados no atual subcapítulo, revelar-se-á útil a especificação acima apresentada.

Os dados, de forma genérica, são considerados como nova fonte de riqueza e poder, e formam, a partir de bancos ou bases de dados, um verdadeiro ativo imaterial. Qualifica-se como dado, segundo Simão Filho e Schwartz:

> Toda e qualquer informação numérica, alfabética, gráfica, fotográfica, acústica, midiática ou de qualquer outra espécie que sofre tratamento tecnológico com vistas a possibilitar tráfego em auto estrada de informação, é considerada genericamente como dado.[53]

Uma base ou banco de dados, por outro lado, designa-se como o conjunto de informações devidamente agrupadas a partir de algum tipo de metodologia ou preceito. Consoante os mesmos autores acima citados, uma base de dados é estruturada:

> [...] a partir da seleção prévia, inserção de conteúdos, elementos e informações relacionados a uma quantidade de bens de diversas naturezas e organização estrutural racional e eficiente, buscando em seu contorno atender a uma finalidade ou conjunto de finalidades específicas relacionadas a sua utilização.[54]

Nesse sentido, para a conceituação jurídica dos dados médicos e de saúde, oportuno, ainda, o apontamento da existência de dados, considerados no sentido lato, e de dados pessoais, esses sim relacionados à vida privada, rastreadores de quaisquer características, ações ou relações desenvolvidas pelo indivíduo em âmbito econômico, social, profissional, criativo, médico, *et cetera*.

---

[52] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
[53]SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.
[54]Ibidem.

As informações pessoais, segundo apontado pela doutrina majoritária e descrito nas normativas existentes[55], são assim consideradas quando relacionadas a alguma pessoa singular, reconhecida ou suscetível de reconhecimento. Isto é, uma informação será pessoal quando seu objeto é o próprio sujeito de direitos, exibindo ou representando algum vínculo ou aspecto objetivo deste.

Outrossim, os dados pessoais também podem ser classificados como públicos ou privados. Públicos são os dados de notório conhecimento, amplamente divulgados na sociedade, sendo que o titular desconhece a origem da sua difusão, não possuindo meios, portanto, para impedi-la. Por outro lado, dados privados são os dados pessoais e particulares de foro íntimo de cada pessoa, passíveis de divulgação e processamento tão somente a partir do consentimento expresso de seu titular[56].

Fundamentada no princípio da monetização de dados – utilização, processamento e transformação de dados com o objetivo de formação de um elemento imaterial como fonte de riquezas - e estritamente voltada para a formação de bancos de dados, ainda há a classificação das informações em estruturadas ou não estruturadas. Essas denotam os rastros deixados pelo cidadão na *internet*, em cadastros ou fichários, que foram captados, *a priori*, sem um objetivo pré-definido. Aquelas, de outro modo, foram coletadas para um fim específico, integrando-se e complementando-se a bases de dados igualmente específicas[57].

A teoria dos círculos concêntricos, criada por Heinrich Hubman em 1953, e, posteriormente evidenciada por Heinrich Henkel em 1957, procurou construir critérios racionais e objetivos para a medição do sentimento e da invasão da privacidade de cada indivíduo. Tal teoria, igualmente denominada de “teoria da pessoa como uma casca de cebola”, faz uso de três esferas concêntricas e distintas para representar as noções de vida privada, intimidade e vida pública de cada cidadão, entendendo-se que a valoração da gravidade da invasão da privacidade

---

[55]A partir da leitura do artigo 2º da Convenção de Estrasburgo, de 1981, do Conselho Europeu - já detalhada no subcapítulo 2.1 deste trabalho - depreende-se que dado pessoal é “qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação (“titular dos dados”)”. UNIÃO EUROPEIA. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Diretiva 108 de 1980. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 23 set. 2017.

[56]SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.

[57] Ibidem.

apresenta-se inversamente proporcional ao tamanho da esfera. Ou seja, quanto mais se atinge a esfera central, mais grave revela-se a violação[58].

No círculo maior encontra-se a esfera pessoal, da vida pública do cidadão, abrangendo circunstâncias individuais e particulares que são, entretanto, relevantes e pertinentes para a comunidade. O círculo pessoal retrata, portanto, o acesso público restrito, passível de ocorrência tão somente em ocasiões de interesse público. O círculo do meio representa a esfera da intimidade e confidencialidade, protegendo-se situações e relações íntimas, mas não ocultas, a saber, o sigilo domiciliar, o telefônico, o de alguns dados informáticos e o profissional. Por fim, o círculo mais central e profundo contém a esfera do segredo, guardiã do direito de isolamento do indivíduo, resguardando suas confidências e reservas, como as opções políticas, crenças e escolhas sexuais. Em referido círculo concentram-se as opiniões, escolhas, comportamentos, informações e ações das quais o cidadão possui, em tese, controle único e exclusivo[59].

Na atual era informacional que se vivencia, carimbada pelo avanço das tecnologias e pela evolução constante das relações pessoais e comerciais nos meios digitais, a teoria das esferas de Hubman demonstrou-se insuficiente para enfrentar ataques cada vez mais sofisticados e variados à vida privada do cidadão. A visão fragmentada e segmentada do conceito de privacidade cede lugar, assim, a um tratamento mais unitário de referido mandamento constitucional.

Como acertadamente explicita Felipe Stribe da Silva:

> Desta forma, não é possível compreender a estrutura da intimidade, da vida privada ou da privacidade de forma independente – ou na forma de círculos concêntricos. Tanto por que a estrutura externa de proteção da privacidade carrega um conteúdo de personalidade interna e, portanto, de intimidade, como pelo fato de que a intimidade atualmente, sobretudo tendo em conta as violações que o avanço das TIC e pode ocasionar, também pode ter um conteúdo externo de proteção e controle sobre informações íntimas, uma autodeterminação informativa.[60]

Nesse contexto, surgiram novos levantamentos teóricos que tentaram capacitar à prática a proteção da vida privada do indivíduo, a exemplo da alegoria do

---

[58]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 67.
[59]Ibidem.
[60]SILVA, Felipe Stribe da. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria: UFSM, 2015. 167p. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade Federal de Santa Maria, Santa Maria, 2015.

mosaico, criada por Fulgencio Madrid Conesa, que entendeu como fator mais preponderante, para a forma de proteção, a personalização do sujeito no contexto de uma relação informativa. Pensamento similar foi explicitado por Daniel J. Solove, que cita a criação de “dossiês digitais” a partir do cruzamento de informações entre bancos de dados e cadastros, ressaltando como fator predominante para o refúgio da privacidade o real uso que será concedido aos dados coletados[61].

Não obstante, ainda que a teoria dos círculos concêntricos já esteja superada e já tenha sido abandonada pela doutrina, o seu conteúdo apresenta-se pertinente para a presente análise. A ideia da existência de uma gradação no nível de importância das informações e dados pessoais, sendo alguns qualificados como mais relevantes e significativos para o indivíduo, e carecedores, portanto, de maior resguardo e sigilo, coaduna-se perfeitamente com a conceituação dos denominados dados sensíveis.

Nessa perspectiva, ainda existe, no contexto dos dados pessoais, os dados considerados sensíveis. Os dados sensíveis compreendem um complexo de informações pessoais que apresentam alto potencial discriminatório ou recriminatório ao seu titular, ostentando maiores riscos que a média para o indivíduo e, até mesmo, para a coletividade[62]. Devido ao elevado grau de lesividade dos dados sensíveis, sua coleta, processamento e tratamento devem ocorrer somente após a anuência e o consentimento expresso do titular, pois, fato contrário, estar-se-ia violando a esfera do segredo, das confidências e reservas do ser.

São tidas como informações sensíveis, entre outras, aquelas que desvelam a origem racial ou étnica do titular, os seus princípios políticos, morais, filosóficos ou religiosos, filiações partidárias ou sindicais, antecedentes criminais, orientações sexuais, além, é claro, dos dados médicos e de saúde. Dentre as categorizações acima já expostas, os dados sensíveis enquadram-se, igualmente, como dados privados, e inserem-se dentro do círculo dos segredos e intimidades do indivíduo.

Ressalta-se que Adalberto Simão Filho e Germano Schwartz, em citação a Zygmunt Bauman e em análise ao nível de vigilância que a sociedade é submetida,

---

[61] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

[62] SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.

em contraponto à necessidade de proteção dos dados pessoais, alertam para a construção de perfis de minorias indesejáveis:

> Outro aspecto bem demonstrado por Bauman, refere-se a vigilância constante e intermitente da pessoa e ao processamento e canalização de dados sensíveis pessoais, como fatores que podem contribuir para a construção de perfis de minorias indesejáveis, gerando a potencialidade de exclusão social ou de normalização de grupos não excluídos que passariam a ter melhores condições de acessos a bens corpóreos ou incorpóreos de consumo.[63]

Constata-se, deste modo, que a depender da classificação do dado como sensível, o nível de proteção obrigatoriamente necessita ser maior, haja vista o grau de risco, em todos os sentidos, ser igualmente mais elevado. Esse é o motivo pelo qual as legislações existentes, a exemplo da argentina e uruguaia, imprimirem tratamento diferenciado e delimitado às informações consideradas sensíveis. O Anteprojeto de Lei Brasileiro sobre a Proteção de Dados Pessoais, da mesma forma, discorre especificamente sobre dados sensíveis, apresentando-os como conceito-chave para o entendimento do texto, e tutelando-os de maneira a evitar o acesso por terceiros não-autorizados.

Esta classificação de dados em sensíveis manifesta-se essencial para o presente trabalho, e, em especial, para o subcapítulo em análise, posto que os dados médicos e de saúde encaixam-se perfeitamente na descrição dedicada às informações sensíveis, em razão do elevado potencial discriminatório que guardam caso sejam revelados, em determinadas situações, sem o devido consentimento do paciente.

Dessa forma, com a execução da presente pesquisa, pode-se afirmar que os dados médicos revelam-se como importante ramificação dos dados pessoais e consistem-se em informações de saúde depositadas em hospitais, após internações ou cirurgias, em laboratórios, após a coleta de exames, em clínicas, após a realização de procedimentos, em consultórios médicos, odontológicos, fisioterapêuticos, psicológicos ou psiquiátricos, após a realização de consultas e sessões, ou até mesmo em cadastros de planos de saúde, após a solicitação de autorização para realização de exames ou procedimentos. Salienta-se que, além

---

[63]SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>. Acesso em: 21 set. 2017.

dos dados de saúde, os registros dos pacientes em citados estabelecimentos contêm inúmeras informações de cunho pessoal, incluindo nomes, registros de nascimento, endereços, números de seguro e de planos de saúde de cada indivíduo.

Frisa-se que o processamento e a transmissão dos dados médicos podem variar entre a simples comunicação de casos entre médicos, enfermeiros, técnicos e fisioterapeutas de um estabelecimento hospitalar, até o compartilhamento mais complexo de dados entre instituições de atenção à saúde, por meio de bancos de dados, por exemplo, transmitidos pela rede local ou via *internet*[64].

Ainda que a temática específica da proteção dos dados privados de saúde passe a ser trabalhada com clareza de detalhes no segundo capítulo deste estudo, constata-se, de antemão, a importância de um tratamento adequado contra a ameaça de acessos ou vazamentos indesejados das informações médicas, com o intuito de garantir a proteção da privacidade do paciente, e a própria reputação da instituição responsável pela guarda dos dados.

[64]KAMEDA, Koichi; PAZELLO, Magaly. e-Saúde e desafios à proteção da privacidade no Brasil. **PoliTICs**, v. 16, p. 31-40, 2013. Disponível em: <https://politics.org.br/edicoes/esa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil>. Acesso em: 20 out. 2017.

3 A ANÁLISE DO TRATAMENTO CONFERIDO AOS DADOS MÉDICOS SOB A ÓTICA DO DIREITO À INTIMIDADE E À VIDA PRIVADA DOS PACIENTES

A inviolabilidade da intimidade e da vida privada é direito inserto constitucionalmente no rol de garantias fundamentais do cidadão. A análise concretizada no item 2.2 desta pesquisa proporcionou o entendimento de que, no ordenamento brasileiro, não há proteção dos dados pessoais integrada e alinhada aos comandos constitucionais, mas sim atuações fracionadas em focos específicos, a exemplo da tutela exercida no Código de Ética Médica, que será melhor analisado posteriormente.

Os dados médicos, igualmente conhecidos como dados de saúde, ou, simplesmente, informações de saúde, enquadram-se em uma subcategoria especial dos dados pessoais, qual seja, a dos dados sensíveis. A imprensa brasileira rotineiramente comprova a fragilidade e a vulnerabilidade a que estão submetidos os dados médicos no Brasil, estampando frequentes vazamentos de informações de cidadãos comuns, artistas, esportistas, políticos e figuras públicas.

Nesse sentido, propondo-se à elaboração de um diagnóstico quanto ao destino e ao nível de proteção conferido aos dados dos usuários de sistemas de saúde, defronte ao desenvolvimento de novas e mais avançadas tecnologias, neste capítulo será analisada a trajetória percorrida pelas informações médicas, desde sua coleta até seu posterior armazenamento e destino final (3.1), seguido pela observação do impacto das inovações tecnológicas na área da saúde a partir da *e*-saúde e dos bancos de dados informatizados (3.2). Para finalizar, como objetivo final do presente estudo monográfico, refletir-se-á acerca da eventual necessidade de criação de legislação específica, no Brasil, que tutele as informações de caráter pessoal da população (3.3).

3.1 DA TRAJETÓRIA DAS INFORMAÇÕES DE SAÚDE: DA COLETA AO POSTERIOR ARMAZENAMENTO

Ainda que compreensível no plano teórico, a imprescindibilidade de proteção dos dados pessoais dos pacientes e dos usuários dos sistemas de saúde verifica-se pouco factível no plano prático, haja vista que, no contexto brasileiro, o armazenamento e o posterior uso dos dados médicos revestem-se de certa

obscuridade, não proporcionando o dimensionamento correto, ao usuário, quanto a potencial lesividade ao direito fundamental humano da privacidade em caso de possíveis vazamentos ou acessos indevidos.

Nessa senda, já no ano de 1995, o Ministro Ruy Rosado de Aguiar, em decisão proferida no Superior Tribunal de Justiça, salientou a primordialidade na efetivação da proteção dos dados pessoais a partir de uma ótica mais abrangente, vinculada às variadas formas de controle que se tornam possíveis com o tratamento e a manipulação desenfreada dos dados:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número intenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador[65].

O mesmo entendimento foi concretizado, em âmbito norte-americano, com a divulgação de um estudo, no longínquo ano de 1973, editado por uma comissão de especialistas reunida pela *Secretary for health, education and welfare*. A área da saúde foi pioneira na demonstração de justificado receio com a manipulação de dados médicos por sistemas informatizados, ao passo que referido estudo igualmente concluiu pelo estabelecimento de relação direta entre o tratamento de dados e o direito de privacidade, além da criação de necessárias normas para o exercício de controle, pelo indivíduo, sobre as próprias informações:

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu

[65]BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 22337/RS**. José Orivaldo Moreira Branco e Clube de Diretores Lojistas de Passo Fundo-RS. Relator: Ministro Ruy Rosado de Aguiar. 20 de março de 1995. Disponível em: <https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Acesso em: 21 out. 2017.

> respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei[66]. (tradução nossa)

Nessa perspectiva, diante dos múltiplos atores que demonstram interesse e cercam os dados de saúde da população, a exemplo de empresas seguradoras, planos de saúde, laboratórios, *hackers* e estelionatários, e, até mesmo diante dos riscos inerentes a fragilidade das informações médicas, a participação do indivíduo no seu processamento deve ter início a partir da coleta de seus dados.

Assim sendo, a autodeterminação informativa do paciente inaugura-se com o preenchimento do termo de consentimento esclarecido e informado, documento necessário tanto para a realização de intervenções cirúrgicas ou procedimentos, como para a prática de pesquisa, fatos que desencadeiam, por si só, a colheita de dados de saúde do indivíduo. Os termos de consentimento devem conter avisos claros relativos ao grau de confiabilidade de exames, alertas de possíveis riscos, consequências fisiológicas e complicações, além do caráter, objetivos e benefícios da intervenção. O termo deve estar escrito em linguagem simples e decodificada do jargão médico ou científico, de forma que o paciente esteja livre e plenamente consciente do teor da sua permissão.

Infelizmente, o mesmo zelo acima delineado não é dedicado às informações de saúde. Escassos são os termos de consentimento que alertam o paciente quanto aos possíveis usos, destino e armazenamento a que serão submetidos os seus dados de saúde. Alerta-se, desse modo, para os riscos e ameaças veladas ao direito de privacidade e intimidade do indivíduo que acabam sendo legitimados a partir de sua assinatura em documentos que buscam o consentimento:

> [...] o que se tem verificado, em alguns momentos, é a habilidade e o esforço dissimulador da intenção abusiva, escamoteada tantas vezes por motivações “justas” e “necessárias”. A licitude de um ato dessa natureza não está só no consentimento, mas na sua necessidade e na sua legitimidade. Assim, mesmo que a permissão tenha todas as aparências e

[66]ESTADOS UNIDOS DA AMÉRICA. **Records, computers and the rights of citizens**. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 07 de janeiro de 1973. Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>. Acesso em: 21 out. 2017.

> justificativas de idoneidade, e mesmo que exista aquiescência por escrito, chega-se à conclusão que a vida e a saúde de um indivíduo são bens irrecusáveis e inalienáveis, os quais o bem comum tem interesse em resguardar de forma irrestrita e incondicional. As ciências necessitam mais e mais progredir. Algumas vezes até pela ousadia de suas intercessões, de resultados tão fantásticos e inesperados. Todavia, isso não justifica a violência sobre um só homem, qualquer que seja sua condição, qualquer que seja o progresso pretendido[67].

Grifa-se que os médicos, da mesma forma, possuem o dever legal, em concordância com o Código de Ética Médica, de obter o consentimento do paciente previamente a realização de procedimentos ou pesquisa[68]. Sugestiona-se, desde já, que tal conduta igualmente deveria tornar-se obrigatória em relação às informações de caráter pessoal, exigindo-se o consentimento do indivíduo quanto à coleta, processamento e compartilhamento de seus dados médicos que ocorrerão posteriormente a tais intervenções.

O prontuário médico, mais adequadamente alcunhado de prontuário do paciente, expõe-se como o representante primário mais significativo e emblemático do modo de armazenamento de dados médicos no Brasil, e caracteriza-se como sendo uma coletânea de arquivos que contemplam o histórico de pacientes em instituições hospitalares ou médicas. O prontuário do paciente representa, portanto, o conjunto de documentos que se destinam ao registro das informações e dos cuidados de saúde prestados aos pacientes pelas instituições e pelos profissionais. O prontuário compreende, assim, evidências da história de vida do paciente e de sua(s) doença(s), escritas de modo legível, claro e conciso por especialistas, buscando-se garantir uma uniformidade estatística[69].

O Conselho Federal de Medicina (CFM), por intermédio do artigo 1º da Resolução nº 1.638, publicada em 09 de agosto de 2002, definiu como prontuário "o documento único constituído de um conjunto de informações, sinais e imagens

---

[67]FRANÇA, Genival Veloso de. **Direito médico**. 14. ed. rev. e atual. Rio de Janeiro: Forense, 2017. [Minha Biblioteca]

[68]Consoante expresso nos artigos 22 e 101 do Código de Ética Médica: "É vedado ao médico: Art. 22. Deixar de obter consentimento do paciente ou de seu representante legal após esclarecê-lo sobre o procedimento a ser realizado, salvo em caso de risco iminente de morte. [...] Art. 101. Deixar de obter do paciente ou de seu representante legal o termo de consentimento livre e esclarecido para a realização de pesquisa envolvendo seres humanos, após as devidas explicações sobre a natureza e as consequências da pesquisa." CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**. Resolução CFM nº 1931, de 17 de setembro de 2009 (versão de bolso). Brasília: Conselho Federal de Medicina, 2010. Disponível em: <http://www.cremers.org.br/pdf/codigodeetica/codigo_etica.pdf>. Acesso em: 24 out. 2017.

[69]RICARTE, Ivan Luiz Marques; GALVÃO, Maria Cristiane Barbosa. **Prontuário do Paciente**. Rio de Janeiro: Guanabara Koogan, 2012.

registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico”[70].

Da conceituação do Conselho Federal de Medicina depreende-se que o prontuário do paciente, equivocadamente nomeado de prontuário “médico”, é um documento único, não sendo possível sua fragmentação entre os diversos setores que eventualmente terão contato com o paciente.

Visualiza-se, contudo, que referido documento contém dados individualizados de saúde dos pacientes, sendo que seu depósito e consequente dever de guarda são incumbência das instituições de saúde. Dessa forma, ainda que o prontuário seja peça integrante do ato médico, resta a dúvida de a quem pertence sua “propriedade”, questionamento pertinente, tendo em vista os diários requerimentos a hospitais, para obtenção de cópias, advindos de familiares, empresas seguradoras, advogados particulares, terceiros interessados, planos de saúde e autoridades públicas como Polícia Civil, Defensorias Públicas e Poder Judiciário. Lamentavelmente, a falta de normativas de proteção aos dados pessoais e a ainda incipiente reflexão doutrinária acerca do tema estabelecem a resposta a mencionado questionamento como trabalho de difícil precisão.

Nesse sentido, recorre-se a normativas éticas e setoriais para a tentativa de solução do imbróglio. De acordo com o disposto na Resolução nº 1.821/2007 do Conselho Federal de Medicina (CFM):

> [...] o prontuário do paciente, em qualquer meio de armazenamento, é propriedade física da instituição onde o mesmo é assistido − independente de ser unidade de saúde ou consultório −, a quem cabe o dever da guarda do documento;
> [...] os dados ali contidos pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa;
> [...] o prontuário e seus respectivos dados pertencem ao paciente e devem estar permanentemente disponíveis, de modo que quando solicitado por ele ou seu representante legal permita o fornecimento de cópias autênticas das informações pertinentes[71].

[70]CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.638/2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, 09 ago. 2002, Seção I, Brasília, p. 184-185, 2002. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638>. Acesso em: 18 out. 2017.

[71]CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. **Diário Oficial da União**, 23 nov. 2007, Seção I, Brasília, p. 252, 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.pdf>. Acesso em: 18 out. 2017.

Infere-se, assim, que o titular do prontuário é o próprio paciente, que possui direito de acesso livre a todas as informações sobre sua saúde, além do direito de ser informado e de restringir o acesso indesejado de terceiros aos arquivos nele contidos, em resguardo à sua intimidade e privacidade. Ainda assim, à instituição de saúde onde foi projetado, cabe o dever de guarda do documento físico e original, o qual serve, também, como prova da sua prestação de serviços.

Fato recente, noticiado pela imprensa em janeiro de 2017, comprova a fragilidade e a vulnerabilidade a que estão submetidos os dados médicos contidos em prontuários hospitalares, no Brasil. Informações sigilosas do estado de saúde da ex-primeira dama Marisa Letícia foram divulgados por uma médica do Hospital Sírio-Líbanes, hospital de referência da capital paulista, em um grupo de aplicativo de conversas, o que motivou manifestações de ódio entre os profissionais da saúde[72]. O vazamento dos dados médicos de mencionada figura pública suscitou, novamente, em âmbito nacional, o debate pela necessidade de conferir proteção e sigilo aos dados pessoais e de saúde, os quais são diariamente violados em decorrência do manejo errôneo, do acesso indevido de terceiros ou mesmo pela quebra de sigilo profissional.

Com efeito, o sigilo médico apresenta-se como um dever “prima-facie” decorrente da natureza confidencial da relação médico-paciente. Segundo o melhor ensinamento de Maria Helena Diniz:

> A preservação do segredo pelo profissional da saúde é um pilar fundamental para assegurar um relacionamento médico-paciente tranquilo, baseado na confiança e no respeito mútuos, e um tratamento eficaz, pois a discrição e a reserva de certos fatos evitarão repercussões econômico-sociais que, porventura, possam surgir do estado de saúde pessoal. As informações dadas pelo paciente ao seu médico, os resultados de exames realizados com finalidade terapêutica, diagnóstica ou prognóstica, os dados contidos no prontuário, arquivo ou boletim médico são de propriedade daquele paciente; logo, os profissionais da saúde e as instituições que tenham contato direto ou indireto com as informações recebidas ou obtidas são seus depositários, e só podem usá-las para atender a necessidade de ordem profissional e em benefício do paciente[73].

[72]HERDY, Thiago. Após compartilhar dados sigilosos de Marisa, médica do Sírio é demitida. **O Globo**, Rio de Janeiro, 02 fevereiro 2017. Disponível em: <https://oglobo.globo.com/brasil/apos-compartilhar-dados-sigilosos-de-marisa-medica-do-sirio-demitida-20864217>. Acesso em: 01 jul. 2017.
[73]DINIZ, Maria Helena. O Estado Atual do Biodireito. São Paulo: Saraiva, 2009, p. 649-650.

Segundo a Organização Mundial da Saúde (OMS) define-se como confidencialidade médica o dever dos profissionais de "proteger a informação do paciente e não divulgá-la sem autorização". O direito à confidencialidade impõe-se, portanto, como um segmento da privacidade informacional existente no âmbito de uma relação entre o profissional de saúde e seu paciente. Nessa perspectiva, afirma-se que as informações de saúde obtidas em decorrência dessa relação devem conservar-se fora do alcance externo, a menos que haja autorização expressa do titular para que sejam reveladas. O direito à confidencialidade implica, assim, na confiança que o paciente irá depositar no profissional de saúde de que qualquer informação compartilhada no âmbito da relação médica será respeitada e utilizada somente para o propósito para o qual foi produzida, mantendo-se em sigilo caso não ocorra permissão para sua divulgação[74].

Constata-se, dessa maneira, que para além da proteção pela observância dos direitos à intimidade, privacidade e confidencialidade, o prontuário médico e todas as demais informações coletadas para fins de tratamento de saúde são, igualmente, resguardadas pelo dever de sigilo (ou segredo) profissional exigido dos expertos da saúde.

O segredo médico impõe-se como uma espécie de segredo profissional, é universalmente respeitado e existe, acima de tudo, para resguardo do paciente, constituindo-se como um dever inerente ao desempenho da profissão médica. Importante mencionar que o dever do sigilo médico estende-se, além do médico, a todos os profissionais da saúde, que por atribuição de seu ofício tenham acesso aos dados confidenciais do paciente.

O Código de Ética Médica, normatizado pela resolução n. 1931, de 17 de setembro de 2009 do Conselho Federal de Medicina, impõe a atenção ao sigilo profissional no Capítulo IX, e determina ser vedado ao médico "revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente"[75].

Do mesmo modo, o Código Internacional de Ética Médica, da Associação Médica Mundial, dispõe que o médico deverá guardar segredo absoluto de tudo o

---

[74]RICARTE, Ivan Luiz Marques; GALVÃO, Maria Cristiane Barbosa. **Prontuário do Paciente**. Rio de Janeiro: Guanabara Koogan, 2012.

[75]CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**. Resolução CFM nº 1931, de 17 de setembro de 2009 (versão de bolso). Brasília: Conselho Federal de Medicina, 2010. Disponível em: <http://www.cremers.org.br/pdf/codigodeetica/codigo_etica.pdf>. Acesso em: 24 out. 2017.

que foi a ele confiado, mesmo depois da morte do paciente[76], ratificando o dever dos médicos e das instituições de garantir a confidencialidade em respeito ao direito à intimidade do paciente.

Tanto é verdade o acima exposto que se constitui como crime, devidamente tipificado no Código Penal, em sua Seção IV, intitulada “Dos Crimes Contra a Inviolabilidade do Segredo”[77], a violação ao segredo profissional, leia-se, no caso, o sigilo médico. Ainda, a revelação dos dados médicos sem autorização expressa do paciente poderá ensejar o pagamento de condenação civil por dano moral ou patrimonial do profissional ou da instituição de saúde, consoante melhor jurisprudência[78], além de punição por falta ética.

Frisa-se, ao fim, que o Código de Ética Médica é cirúrgico ao dispor em seu artigo 89 ser vedado ao médico “liberar cópias do prontuário sob sua guarda, salvo

---

[76]ASSOCIAÇÃO MÉDICA MUNDIAL. **Código Internacional de Ética Médica**. Londres: Assembleia Geral da Associação Médica Mundial, 1949. Disponível em: <https://history.nih.gov/research/downloads/ICME.pdf>. Acesso em: 24 out. 2017.

[77]Consoante expresso nos artigos 153 e 154 do diploma legal:

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena - detenção, de um a seis meses, ou multa.

§ 1º Somente se procede mediante representação.

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:

Pena - detenção, de três meses a um ano, ou multa.

Parágrafo único - Somente se procede mediante representação. BRASIL. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940.** Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 02 nov. 2017.

[78]INDENIZAÇÃO. DANOS MATERIAIS. DANOS MORAIS. DIVULGAÇÃO DE PRONTUÁRIO. PACIENTE COM AIDS. Incidência do CDC. Art. 14, § 3º. O hospital é fornecedor de serviços de saúde. Prontuário de paciente que tem o vírus HIV positivo divulgado a terceiros, servindo para a instrução de processo judicial. Não autorização da autora para entrega do prontuário. Violação da intimidade. Infração ao art. 5º, inciso X da CF. Ilicitude da conduta. Nexo causal. Prejuízo. Dano moral configurado. Valor da indenização. Necessidade de eficácia punitiva e coativa. Fixação em 30 salários-mínimos Danos materiais não comprovados. Deram parcial provimento. BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Acórdão de decisão que deu parcial provimento ao pedido de indenização por divulgação de prontuário sem autorização da paciente**. Apelação Cível nº 70017144478. Julia Patrícia Medeiros da Costa e Estado do Rio Grande do Sul e Sociedade Educação e Caridade. Relator: Desembargador Carlos Rafael dos Santos Júnior. 08 de outubro de 2007. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70017144478&as_q=+#main_res_juris>. Acesso em: 26 out. 2017.

quando autorizado, por escrito, pelo paciente, para atender ordem judicial ou para a sua própria defesa”[79].

Logo, conforme já amplamente alastrado, o paciente impõe-se como o verdadeiro detentor das informações contidas em seu prontuário e em quaisquer outros mecanismos de armazenamento de seus dados de saúde, possuindo acesso a eles em qualquer momento, podendo, inclusive, realizar cópias, se assim desejar. A instituição de saúde ficará obrigada a liberar o acesso do usuário a seus dados médicos a partir de sua própria requisição ou de pessoa por ele formalmente autorizada, bem como de seu representante legal, em caso de óbito.

Ressalta-se que, em relação à reserva de informações de saúde em bancos ou bases de dados, o presente trabalho debruçar-se-á de maneira apropriada no subtítulo seguinte.

3.2 A E-SAÚDE E OS BANCOS DE DADOS INFORMATIZADOS

A evolução das tecnologias, o progresso na capacidade de transmissão de informações, a expansão do acesso ao conhecimento, o surgimento da *internet* e a decorrente criação de espaços sociais virtuais: elementos que penetraram nos poros visíveis da área da saúde e que, combinados, modificaram a estrutura operacional do setor, a maneira de armazenamento e tratamento dos dados médicos e a consequente reflexão jurídica sobre o assunto.

A expressão e-Saúde, acolhida pela Organização Mundial da Saúde, e comumente denominada como telessaúde ou telemedicina, existe para designar as atividades, no campo da atenção à saúde, que fazem uso das Tecnologias de Informação e Comunicação (TICs), a fim de aprimorar e proporcionar alta qualidade de atendimento médico à população. São consideradas práticas de e-Saúde o teleatendimento, o telediagnóstico, os prontuários digitais, os bancos de dados médicos informatizados, as teleconsultorias, as videoconferências, as telecirurgias, a tele-educação, as bibliotecas virtuais de vídeos e imagens, o desempenho de segundas opiniões formativas, dentre inúmeros outros exemplos[80].

---

[79]CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**. Resolução CFM nº 1931, de 17 de setembro de 2009 (versão de bolso). Brasília: Conselho Federal de Medicina, 2010. Disponível em: <http://www.cremers.org.br/pdf/codigodeetica/codigo_etica.pdf>. Acesso em: 24 out. 2017.

[80] REZENDE, Edson José Carpintero, et al. Ética e Telessaúde: reflexões para uma prática segura. **Panam Salud Publica**, v. 28, p. 58-65, 2010. Disponível em:

No Brasil, a prática da e-Saúde encontra-se em estado de ascensão. O Programa Nacional de Telessaúde é parte integrante do Sistema Único de Saúde (SUS), preza pela ampliação da resolutividade da Atenção Básica, auxilia na educação de profissionais recém-formados, promove sua integração às demais políticas públicas de saúde e apresenta-se como exemplo prático da mudança que está ocorrendo nas formas convencionais de atendimento na área da saúde. Mencionado programa, capitaneado pelo Ministério da Saúde, é posto em prática por meio dos Núcleos de Telessaúde, que:

> [...] desenvolvem atividades técnicas, científicas e administrativas para planejar, executar, monitorar e avaliar as ações de Telessaúde, em especial a produção e oferta de teleconsultoria, telediagnóstico e tele-educação. Essas atividades são registradas em plataformas online, onde é possível cadastrar usuários e estabelecimentos que utilizam esses serviços[81].

As justificativas apresentadas para a implementação da rede foram de que os profissionais médicos possuem receio em fixar-se em localidades remotas do país, devido a insegurança frente a casos clínicos ou cirúrgicos, a afirmação de que a capacidade de transmissão de dados, no país, encontra-se subutilizada, de que o custo para transporte de um paciente apresenta-se cem vezes superior ao da telessaúde, além da necessidade contínua de aperfeiçoamento e capacitação das equipes de saúde[82].

A Rede Universitária de Telemedicina (RUTE), implantada em 2006 pelo Ministério da Ciência, Tecnologia e Inovação, foi criada com o propósito de unir faculdades de medicina e hospitais universitários de diferentes regiões do território brasileiro, possui coordenação da Rede Nacional de Ensino e Pesquisa (RNP), e conta, atualmente, com 131 unidades em operação em todo o Brasil. As instituições superiores participantes contam com a colaboração, ainda, de redes-parceiras na América Latina, Europa, Japão, Austrália e Estados Unidos. A RUTE, que possui

---

<https://scielosp.org/scielo.php?pid=S1020-49892010000700009&script=sci_abstract&tlng=pt>. Acesso em: 28 out. 2017.

[81]BRASIL. Ministério da Saúde. **Nota Técnica nº 50/2015-DEGES/SGTES/MS**. Diretrizes para oferta de atividades do Programa Nacional Telessaúde Brasil Redes. Brasília, 15 de outubro de 2015. Disponível em: <189.28.128.100/dab/docs/portaldab/noyas_tecnicas/Nota_Tecnica_Diretrizes_Telessaude.pdf>. Acesso em: 28 out. 2017.

[82]REZENDE, Edson José Carpintero, et al. Ética e Telessaúde: reflexões para uma prática segura. **Panam Salud Publica**, v. 28, p. 58-65, 2010. Disponível em: <https://scielosp.org/scielo.php?pid=S1020-49892010000700009&script=sci_abstract&tlng=pt>. Acesso em: 28 out. 2017.

como objetivo promover o intercâmbio colaborativo de conhecimento médico especializado, a discussão de diagnósticos e tratamentos de pacientes, a realização de cursos de capacitação à distância e videoconferências, além da melhoria no atendimento de populações carentes, igualmente simboliza-se como uma prática de e-Saúde recentemente introduzida como política pública de saúde no Brasil. Conforme resta explícito no portal da RUTE:

> Sua implantação traz impactos científicos, tecnológicos, econômicos e sociais para os serviços médicos já existentes, permitindo a adoção de medidas simples e de baixo custo, como a implantação de sistemas de análise de imagens médicas com diagnósticos remotos, que pode contribuir muito para diminuir a carência de especialistas, além de proporcionar treinamento e capacitação de profissionais da área médica sem deslocamento para os centros de referência[83].

A adoção do prontuário eletrônico ostenta, de maneira semelhante, o título de uma iniciativa de e-Saúde considerada bem sucedida no país. Sucessivamente, os prontuários físicos, arquivados em pastas e escritos à mão pelos profissionais de saúde, estão sendo substituídos por aplicativos e sistemas eletrônicos de arquivos médicos digitais, que possuem ciclo vital – caminho percorrido pelos documentos desde a sua produção até a sua destinação final – considerado eterno, tendo em vista a infindável capacidade de armazenamento das máquinas e sistemas de computação[84].

O Ministério da Educação (MEC) em clara percepção à necessidade de modernização dos recursos e acompanhamento das tendências tecnológicas para o melhoramento e alinhamento dos processos, desenvolveu, a partir do ano de 2009, como parte integrante do Programa Nacional de Reestruturação dos Hospitais Universitários Federais (REHUF), o Aplicativo de Gestão para Hospitais Universitários (AGHU). O sistema foi criado para possibilitar a padronização das práticas administrativas e assistenciais dos hospitais universitários federais, e para

[83]O que é a Rede Universitária de Telemedicina (Rute)?. **Portal da RUTE**, 2017. Disponível em: <http://rute.rnp.br/arute>. Acesso em: 01 nov. 2017.

[84]VALCARENGHI, Emily Vivian. **Gestão de Arquivos Médicos**: uma análise dos arquivos médicos das Universidades federais da região sul do Brasil. Santa Maria: UFSM, 2009. 72 p. Monografia de Especialização, Especialização de Gestão em Arquivos do Programa de Pós-Graduação à Distância – EAD, Universidade Federal de Santa Maria, Santa Maria, 2009.

permitir a formação de indicadores de saúde nacionais, a fim de facilitar a adoção de projetos de melhorias comuns para os hospitais[85].

Ademais, atribui-se pontos positivos ao aplicativo na medida em que propicia, de maneira rápida e instantânea, o histórico de consultas ambulatoriais, exames e procedimentos cirúrgicos do paciente, auxiliando no exercício das funções dos profissionais de saúde, vez que facilita a compreensão das histórias médicas pregressas. Da mesma forma, os pacientes internados, as consultas realizadas nos ambulatórios, as prescrições médicas e da enfermagem, os controles dos fármacos e do estoque, o pedido de exames e a realização e descrição de cirurgias, devem restar inseridos no AGHU, oportunizando o controle do hospital universitário acerca de toda a sistemática diária, com fundamento em indicadores padronizados, a partir do apontamento do número de cirurgias, criação de estatísticas de casos, quantidades de exames requeridos, *etc*.

O AGHU qualifica-se, dessa forma, como um sistema de armazenamento, processamento e monitoramento de dados, que visa aumentar a segurança do usuário do SUS por meio da rapidez na consulta de seus prontuários digitais, além de incrementar a segurança da informação por meio de perfis de acesso[86].

Constata-se, novamente, que as normas éticas advindas do Conselho Federal ou dos Conselhos Regionais de Medicina encontram-se na vanguarda das legislações aplicadas à temática. A Resolução n° 1.643/2002 do CFM define e disciplina a prestação de serviços através da telemedicina. Na promulgação dessa resolução, o CFM declara que as informações de saúde sobre pacientes identificados só podem ser transmitidas a outro experto com a prévia permissão do detentor dos dados, mediante seu consentimento livre e esclarecido e sob severas normas de segurança[87]. No mesmo sentido, a Resolução nº 1.821/2007 do CFM, já citada no presente trabalho, regulamenta a utilização dos prontuários eletrônicos, e aprova “as normas técnicas concernentes à digitalização e uso dos sistemas

---

[85] O que é o AGHU. **Empresa Brasileira de Serviços Hospitalares (EBSERH)**, 2015. Disponível em: <http://www.ebserh.gov.br/web/aghu/sobre/o-que-e>. Acesso em: 15 dez. 2017.

[86]SILVA, Helen Ribeiro da; FARIAS, Josivania Silva. Adoção de Tecnologia em Hospitais: o caso da adoção do Sistema AGHU pelos Hospitais Universitários do Brasil. **Revista de Administração Hospitalar e Inovação em Saúde**, v. 13, n. 4, p. 95-111, 2017. Disponível em: <http://revistas.face.ufmg.br/index.php/rahis/article/view/95%20-%20111/1923>. Acesso em: 01 nov. 2017.

[87]CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.643/2002. Define e disciplina a prestação de serviços através da Telemedicina. **Diário Oficial da União**, 26 ago. 2002, Seção I, Brasília, p. 205, 2002. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2002/1643_2002.pdf>. Acesso em: 01 nov. 2017.

informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde”[88].

Alinha-se, nessa lógica, à interpretação exposta por Edson Rezende et al:

> A telessaúde aparece como novo contexto nos serviços de saúde e faz ressurgir a preocupação com os aspectos éticos e legais pertinentes a essa pratica, principalmente no que se refere a confidencialidadedas informações prestadas e ao uso do TCLE. Tornam-se necessários alguns cuidados, tais como o uso de senhas e o controle do acesso as informações dos usuários, para se evitarem problemas futuros, mas, acima de tudo, preservar o paciente e a sua dignidade. Outros aspectos importantes referem-se a abertura de espaço nos serviços de saúde para a discussão e capacitação dos profissionais envolvidos no uso da telessaúde. Normatizações referentes a pratica da telessaúde devem ser ainda mais difundidas internacionalmente e também pelos conselhos de classe profissionais. Muitas inovações na área das tecnologias de informação e comunicação estão surgindo e é necessário refletir sobre protocolos e normas nacionais e internacionais para autilização de dados, imagens e registros de pacientes[89].

Hodiernamente, o diagnóstico e o prognóstico médico restam computadorizados, havendo a utilização do recurso do processamento eletrônico de dados biomédicos e de exames laboratoriais dos usuários dos sistemas de saúde, os quais se expõem aos riscos de manipulação por interesses dominantes, vez que, “por mais frias e racionais que sejam as formas de análise e computação das informações biomédicas, elas não são impessoais, colocando em jogo a proteção da confidencialidade e da privacidade”[90].

Os bancos de dados descrevem-se não somente como um repositório armazenador de informações, mas também como uma estrutura muito bem elaborada, formada a partir de um modelo, ao qual se acoplam recursos para auxiliar tanto no armazenamento quanto na consulta de dados[91]. Na área da saúde, visualiza-se a criação de bancos de dados para o registro e acompanhamento dos

---

[88]CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. **Diário Oficial da União**, 23 nov. 2007, Seção I, Brasília, p. 252, 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.pdf>. Acesso em: 18 out. 2017.

[89]REZENDE, Edson José Carpintero, et al. Telessaúde: confidencialidade e consentimento informado. **Revista Médica de Minas Gerais**, v. 23, p. 367-373, 2013. Disponível em: <http://www.rmmg.org/artigo/detalhes/223>. Acesso em: 04 nov. 2017.

[90] DINIZ, Maria Helena. O Estado Atual do Biodireito. São Paulo: Saraiva, 2009, p. 657.

[91]CARDOSO, Virgínia; CARDOSO Giselle. **Sistema de Banco de Dados:** uma abordagem introdutória e aplicada. São Paulo: Saraiva, 2012. [Minha Biblioteca]

pacientes, com a inserção de informações demográficas e fisiológicas dos usuários, a formação de bases de dados de DNA ou de material genético, bem como de resultados de pesquisas clínicas e acadêmicas.

Nesse contexto, Rafael Rocha e Marcos d'Ornellas esclarecem que:

> Ao mesmo tempo em que os bancos de dados médicos são extremamente benéficos para a profissão médica, a sua própria natureza prejudica a confidencialidade dos dados. No sentido de promover a proteção dos direitos de confidencialidade do paciente, deve-se aumentar a segurança dos bancos de dados através de medidas técnicas e também legais. Embora isto possa causar um esforço adicional para os profissionais da área médica, é sempre necessário preservar a relação médico paciente[92].

Sobremaneira, os bancos de dados informatizados estruturam-se em acordo com uma lógica utilitarista, visando à formação de valor ao dado coletado, e à composição de um verdadeiro ativo imaterial. Tal afirmação resulta clara ao verificar-se a utilização maciça de bases de dados de saúde pela indústria farmacêutica, como forma de mapeamento de doenças e consequente utilização dos fármacos, prática que resulta na criação e indexação de perfis e indicadores regionais.

Constata-se, desse modo, a manifesta imprescindibilidade da proteção à privacidade e aos dados pessoais dos pacientes e dos usuários dos sistemas de saúde, frente aos desafios que emergem do uso das novas tecnologias, no registro e no tratamento, em grande volume, das informações de caráter pessoal. Observa-se, portanto, que:

> A ausência de uma política de administração dessas informações permite que a sua manipulação ocorra de modo descuidado e em quantidades excessivas, facilitando a sua difusão pública, acidental ou intencional. Os casos de vazamento de dados pessoais, ao se tornarem públicos, acabam provocando uma sensação de desconfiança por parte dos cidadãos e dos consumidores em relação à instituição que permitiu a difusão das informações. E ainda que não se torne pública, a difusão indevida dos dados é capaz de provocar danos concretos em diversas situações, com potencial de discriminação no caso de dados sensíveis[93].

---

[92] D'ORNELLAS, Marcos Cordeiro; ROCHA, Rafael Port da. Acesso e Privacidade: Em Busca da Segurança das Informações em Bancos de Dados Médicos. In: VII CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, São Paulo, 2000. Anais do VII Congresso Brasileiro de Informática em Saúde. São Paulo, 2000, p. 76-81.

[93] KAMEDA, Koichi; PAZELLO, Magaly. e-Saúde e desafios à proteção da privacidade no Brasil. **PoliTICs**, v. 16, p. 31-40, 2013. Disponível em: <https://politics.org.br/edicoes/esa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil>. Acesso em: 20 out. 2017.

A exploração de dados de maneira maciça, todavia, não é sinônimo fiel de um panorama negativo ou depreciativo. Pesquisas realizadas por Viktor Mayer-Schönberger e Kenneth Cukier na área da saúde pública concluíram que o cruzamento de dados pode detectar e prevenir o crescimento de doenças e possíveis invasores à saúde, como vírus e bactérias. A partir da navegação *online* dos cidadãos a respeito de sintomas físicos e as doenças a eles relacionadas, em *sites* de buscas, criam-se padrões de dados que contribuem para a detecção da localização de tais pessoas e para o posterior exercício de políticas públicas de contenção ou prevenção[94].

Ainda assim, as recentes revoluções tecnológicas, que redundaram na criação de bancos ou bases de dados, e no tratamento desses de forma maciça, desafiam e banalizam a ótica da proteção dos dados médicos e pessoais tão somente pelo modelo individualista do consentimento informado e esclarecido. A doutrina moderna, em razão da dificuldade no controle do uso que será feito da informação pessoal, haja vista a amplitude no tratamento indiscriminado dessa, já sugere a criação de um modelo de proteção a partir de uma visão coletiva, que abranja o bem comum social e efetive a tutela dos dados de maneira ampla e condizente com a realidade prática.

3.3 DA NECESSIDADE DE CRIAÇÃO DE LEGISLAÇÃO ESPECÍFICA NO BRASIL

O exame do subitem 2.2 desta pesquisa indica que o Brasil ainda não conferiu a devida relevância jurídica e legislativa à necessidade de instituição de marcos regulatórios específicos que assegurem a inviolabilidade dos dados pessoais e a proteção do direito fundamental à intimidade e à vida privada dos cidadãos.

Sabe-se que, ainda que a atual geração tecnológica vivencie a era do exibicionismo e do culto às postagens nas redes sociais, compartilhando imagens, vídeos e detalhes da vida cotidiana, comportamento semelhante não é dedicado aos dados particulares, informações pessoais e registros de saúde, carecedores do mais elevado nível de sigilo, a julgar por sua excessiva potencialidade lesiva. A dúvida que aqui se origina, portanto, é quanto à real necessidade de estabelecimento de

[94] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kennet. **Big Data**: la revolución de los datos masivos. Madrid: Turner Publicaciones, 2013.

um marco legal, pelo ordenamento brasileiro, haja vista a onipresença, no mundo contemporâneo, da *internet*, seus desdobramentos e ferramentas.

Lênio Streck, em reflexão à logística da solução de complexos conflitos sociais pela Lei, sustenta que o Direito não se presta mais a atender tais embates.

> [...] não porque tal "complexidade" não estaria prevista no sistema jurídico, mas, sim, porque há uma crise de modelo [...] que se instala justamente porque a dogmática jurídica, em plena sociedade transmoderna e repleta de conflitos transindividuais, continua trabalhando com a perspectiva de um direito cunhado para enfrentar conflitos interindividuais, bem nítidos em nossos Códigos [...][95]

Frente a tal premissa, e, ainda que à parte de normativas e legislações, indubitavelmente o Direito encontra-se imerso em uma nova e intrincada realidade conceitual do ciberespaço e do compartilhamento simultâneo de dados e informações por meios virtuais. A doutrina, aponta, nesse sentido, que a promoção do direito fundamental à intimidade, de forma efetiva no âmbito da *internet*, visando a proteção da inviolabilidade dos dados pessoais, deve ser construída a partir da incorporação das regras de privacidade de maneira conceitual, explícita e expressiva nas legislações aplicáveis ao uso da *internet* existentes no Brasil, possibilitando o monitoramento daqueles que monitoram, a eliminação das informações pessoais e a proteção da identidade construída online[96].

Diante da realidade vivenciada na atual sociedade da informação, com a monetização dos dados, e a veiculação diária, na mídia, de notícias relativas a vazamentos de dados pessoais, financeiros, médicos e cadastrais, a lacuna legislativa de tutela específica das informações pessoais oportuniza ao Poder Judiciário o comando decisório sobre as controvérsias expostas em casos fáticos relacionados à temática. Os magistrados, ao fim e ao cabo, legislam diariamente nas inúmeras disputas relacionadas à privacidade, à *internet* e à proteção de dados que desembocam, diariamente, nos gabinetes e mesas do Judiciário. Ou seja, na falta de lei, as decisões a eles pertencem.

---

[95] STRECK apud FORTES, Vinícius Borges; BOFF, Salete Oro. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência (Florianópolis)**, v. 68, p. 109-127, 2014. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109/26949>. Acesso em: 20 nov. 2017.

[96] FORTES , Vinícius Borges; BOFF, Salete Oro; AYUDA, Fernando Galindo. O Direito Fundamental à Privacidade no Brasil e os Direitos de Privacidade na Internet na Regulação da Proteção de Dados Pessoais. **Revista Eletrônica do Curso de Direito da UFSM**, v. 11, n.1, p. 24-48, 2016. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/19706/pdf>. Acesso em: 20 nov. 2017.

Coaduna-se, nessa senda, com o ensinamento doutrinário que garante papel protagonista ao próprio cidadão:

> Assim, o maior beneficiário da estipulação de um marco legal é o cidadão, que é elo mais frágil, mormente quando posto diante de conglomerados empresariais e do Estado. Em um marco regulatório, o usuário (ou seja, o jurisdicionado) tem as informações que compõem suas esferas de intimidade e de privacidade tratadas adequadamente e, apenas o que é do seu interesse pode ser revelado ou utilizado por terceiros; o que garante a aplicação de seus direitos fundamentais[97]

Certifica-se, assim, que, ainda que tenha legislado recentemente sobre o uso da *internet*, o Brasil permanece apresentando-se em contexto institucional de desprestígio protetivo frente à temática da inviolabilidade de dados, imprimindo verdadeira sensação de vulnerabilidade e incerteza à população. Não é demasiado ressaltar, novamente, que, no contexto atual, "as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas mediante a representação de sua personalidade, fornecida pelos seus dados pessoais"[98], fato que demanda uma tutela efetiva aos dados pessoais, haja vista a grandeza de importância, no presente, do tema.

O atual estado tecnológico, a quantidade inimaginável de dados que são diariamente coletados dos indivíduos, o uso abusivo desses por interesses dominantes e o processamento maciço das informações constituem-se como os elementos que, combinados, não mais permitem um cenário apático do ordenamento brasileiro quanto à proteção desses dados. As atuais regras existentes, baseadas em um conceito de privacidade antiquado e inflexível, não mais se demonstram efetivas para a proteção do cidadão contra os abusos, tendo em vista as inovadoras formas de invasão da intimidade e da vida privada alheia.

Aliás, não só o cidadão, como também empresas e instituições públicas e privadas, clamam por um padrão normativo que dê guarida a investimentos econômicos, desenvolvimento tecnológico, e que fomente a atividade empresarial e econômica, possibilitando a concorrência igualitária com empresas estrangeiras,

---

[97] LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ:** novas práticas em informação e conhecimento, v. 2, n. 1, p. 60-76, 2013. Disponível em: <http://revistas.ufpr.br/atoz/article/view/41320/25261>. Acesso em: 20 out. 2017.

[98] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

muito mais familiarizadas à correta proteção de dados pessoais, além de incrementar o nível de confiança e fidelização do consumidor às empresas.

Nesse sentido, objetivando-se segurança jurídica no campo brasileiro, demonstra-se imprescindível a criação de um pacto que possibilite ao cidadão ferramentas de controle e transparência quanto à real utilização de seus dados pessoais, frente ao direcionamento exponencial de aspectos pessoais, profissionais, empresarias e administrativos para os meios digitais. O tratamento de dados deve estar embasado em uma legislação ampla, geral e efetiva sobre proteção de informações pessoais, que demonstre especial zelo quanto aos dados sensíveis, aí incluídas as informações de saúde.

A cidadania integral do brasileiro e do usuário de sistemas de saúde, na atual Sociedade de Informação, impõe a atualização e modernização do ordenamento jurídico do país, fato que oportunizará a abertura de consciência quanto à dimensão e importância do tema, renovando-se o conceito tradicional de intimidade e privacidade. Uma normativa de proteção de dados balizará, ainda, posicionamentos jurisprudenciais condizentes à dinâmica hoje vivenciada, e fomentará a produção literária e doutrinária sobre o tema, refinando-se conceitos e teorias e estabelecendo-se regras cada vez mais claras e protetivas ao cidadão.

4 CONCLUSÃO

Esta monografia teve como objetivo investigar o nível de proteção oferecido aos dados médicos e de saúde da população, observando, para tanto, as condutas e estratégias que possibilitariam a defesa do sigilo dos dados pessoais do paciente.

O que restou evidente, no decorrer da construção desta pesquisa, foi que a mesma apatia protetiva conferida aos dados pessoais, no geral, é vivenciada no campo dos dados de saúde. O Brasil, na contramão dos países europeus, que possuem sólidas construções legislativas de proteção dos dados pessoais dos indivíduos, analisadas no primeiro subtítulo deste trabalho, não dispõe de regulamentação específica sobre o assunto, observando-se um sistema protetivo baseado nas já conhecidas normas gerais de privacidade, advindas dos comandos constitucionais abrangentes, e das legislações infraconstitucionais esparsas, como o Marco Civil da Internet e a lei do *Habeas Data*.

Na área da saúde, em específico, a tutela das informações de caráter pessoal dos pacientes é concebida por normas éticas e setoriais da classe médica, expostas em regulamentos e Códigos de Ética publicizados e adotados pelo Conselho Federal e pelos Conselhos Regionais de Medicina, os quais não abrangem os demais profissionais da saúde que igualmente possuem contato direto com os dados médicos das pessoas.

Restou manifesta, ainda, e especialmente a partir da elaboração do segundo capítulo deste estudo, a chegada e a introdução das Tecnologias de Informação e Comunicação (TICs) no oferecimento, entrega e administração dos serviços de saúde, a exemplo das teleconsultorias, da educação permanente à distância, do telediagnóstico e da formação de redes colaborativas. A adoção da chamada e-Saúde reverberou, também, no procedimento de coleta, tratamento, uso e posterior armazenamento dos dados de saúde, a partir das iniciativas da aplicação de prontuários digitais e eletrônicos, bancos de dados de saúde informatizados e do tratamento das informações de maneira maciça como estratégia de gestão empresarial e hospitalar.

A análise da possível trajetória das informações de saúde, e da recente inserção de protocolos e processos tecnológicos na tradicional área médica, proporcionou a percepção da urgente necessidade de pensar-se além do simples direito de confidencialidade oportunizado ao paciente, ou do primário dever de sigilo

médico existente na relação médico-paciente, considerando a visível sensibilidade e vulnerabilidade inerente aos dados de saúde do indivíduo, que se apresenta em posição desfavorável e inferior na relação de poder.

Ainda, da pesquisa acerca do panorama brasileiro de proteção, detecta-se a exigência, no âmbito jurídico, da superação do conceito estático de privacidade, dissociado do contexto fático vivenciado pela sociedade e da necessidade de adoção da proteção dos dados pessoais como um direito fundamental humano, haja vista sua influência na formação da personalidade exteriorizada pelos indivíduos. A interpretação das normas constitucionais atinentes aos direitos de privacidade e intimidade deve ser fiel ao tempo presente, vivenciado pela Sociedade da Informação, reconhecendo-se a relação direta entre tais direitos e a comunicação e o tratamento dos dados pessoais.

O direito à autodeterminação informativa, em suas dimensões subjetivas e objetivas, identificado como a capacidade de formação de decisões próprias acerca dos limites dos dados pessoais que podem ser relevados, também foi pauta deste estudo e aclarou sua veemência na importância da pesquisa jurídica sobre a proteção das informações pessoais.

A introdução de um marco normativo próprio sobre a problemática da proteção de dados pessoais é, portanto, apresentada como uma solução que beneficiaria o cidadão e concederia o efetivo sigilo necessário aos dados médicos da população, uma vez que se estabeleceria, de maneira ampla e preventiva regras acerca da obtenção, manipulação e armazenamento de dados. Entretanto, enquanto mencionado tratamento jurídico não é levado a cabo, e apenas para introito da proteção que poderá ser futuramente conferida, entende-se que o acesso aos dados de saúde deve ser baseado em dois princípios: necessidade e consentimento do paciente.

O estudo, dessa maneira, não se encerra aqui. O acompanhamento da mudança no cenário jurídico e político brasileiro quanto à preocupação com os dados pessoais deve ser constante e permanente, em decorrência da efervescência da temática. Futuramente, se algum dos Projetos de Lei apresentados forem aprovados, novas pesquisas poderão ser realizadas, embasadas, nesse turno, nas regras brasileiras efetivamente postas e no nível de resguardo dos dados por elas alcançado.

REFERÊNCIAS

ASSMAN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro**. Florianópolis: UFSC, 2014. 65 p. Monografia, Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2010. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/117169>. Acesso em: 20 set. 2017.

ASSOCIAÇÃO MÉDICA MUNDIAL. **Código Internacional de Ética Médica**. Londres: Assembleia Geral da Associação Médica Mundial, 1949. Disponível em: <https://history.nih.gov/research/downloads/ICME.pdf>. Acesso em: 24 out. 2017.

BRASIL. **Constituição Federal de 1988.** Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 17 jun. 2017.

BRASIL. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940.** Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 02 nov. 2017.

BRASIL. **Lei 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 30 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 20 out. 2017.

BRASIL. **Lei Complementar nº 105 de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 26 out. 2017.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002.** Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 26 out. 2017.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 nov. 2017.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 set. 2017.

BRASIL. **Lei nº 5.172 de 25 de outubro de 1966.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em:

<http://www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm>. Acesso em: 03 nov. 2017.

BRASIL. **Lei nº 9.296 de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 02 nov. 2017.

BRASIL. **Lei nº 9.507 de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>. Acesso em: 29 out. 2017.

BRASIL. Ministério da Saúde. **Nota Técnica nº 50/2015-DEGES/SGTES/MS**. Diretrizes para oferta de atividades do Programa Nacional Telessaúde Brasil Redes. Brasília, 15 de outubro de 2015. Disponível em: <189.28.128.100/dab/docs/portaldab/noyas_tecnicas/Nota_Tecnica_Diretrizes_Telessaude.pdf>. Acesso em: 28 out. 2017.

BRASIL. **Projeto de Lei do Senado nº 330/2013, de 13 de agosto de 2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 15 out. 2017.

BRASIL. **Projeto de Lei nº 5.276/2016, de 13 de maio de 2016.** Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 15 out. 2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 22337/RS**. José Orivaldo Moreira Branco e Clube de Diretores Lojistas de Passo Fundo-RS. Relator: Ministro Ruy Rosado de Aguiar. 20 de março de 1995. Disponível em: <https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Acesso em: 21 out. 2017.

BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Acórdão de decisão que deu parcial provimento ao pedido de indenização por divulgação de prontuário sem autorização da paciente**. Apelação Cível nº 70017144478. Julia Patrícia Medeiros da Costa e Estado do Rio Grande do Sul e Sociedade Educação e Caridade. Relator: Desembargador Carlos Rafael dos Santos Júnior. 08 de outubro de 2007. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70017144478&as_q=+#main_res_juris>. Acesso em: 26 out. 2017.

CARDOSO, Virgínia; CARDOSO Giselle. **Sistema de Banco de Dados:** uma abordagem introdutória e aplicada. São Paulo: Saraiva, 2012. [Minha Biblioteca]

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**. Roma: 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 22 set. 2017.

CONSELHO FEDERAL DE MEDICINA. **Resolução nº 1.638/2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Diário Oficial da União, 09 ago. 2002, Seção I, Brasília, p. 184-185, 2002. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638>. Acesso em: 18 out. 2017.

CONSELHO FEDERAL DE MEDICINA. **Resolução nº 1.643/2002**. Define e disciplina a prestação de serviços através da Telemedicina. Diário Oficial da União, 26 ago. 2002, Seção I, Brasília, p. 205, 2002. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2002/1643_2002.pdf>. Acesso em: 01 nov. 2017.

CONSELHO FEDERAL DE MEDICINA. **Resolução nº 1.821/2007**. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Diário Oficial da União, 23 nov. 2007, Seção I, Brasília, p. 252, 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.pdf>. Acesso em: 18 out. 2017.

CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**. Resolução CFM nº 1931, de 17 de setembro de 2009 (versão de bolso). Brasília: Conselho Federal de Medicina, 2010. Disponível em: <http://www.cremers.org.br/pdf/codigodeetica/codigo_etica.pdf>. Acesso em: 24 out. 2017.

D'ORNELLAS, Marcos Cordeiro; ROCHA, Rafael Port da. Acesso e Privacidade: Em Busca da Segurança das Informações em Bancos de Dados Médicos. In: VII CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, São Paulo, 2000. **Anais do VII Congresso Brasileiro de Informática em Saúde**. São Paulo, 2000, p. 76-81.

DINIZ, Maria Helena. **O Estado Atual do Biodireito**. São Paulo: Saraiva, 2009.

DONEDA, Danilo. A proteção de dados está chegando (tarde) ao Brasil. **Gazeta do Povo**, Curitiba, 01 outubro 2017. Disponível em:<http://www.gazetadopovo.com.br/opiniao/artigos/a-protecao-de-dados-esta-chegando-tarde-ao-brasil-7kehelgsg36gs0twvvvxr63d5>. Acesso em: 15 out. 2017.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 30 set. 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ESPANHA. **Constituição Espanhola, de 27 de dezembro de 1978**. Disponível em <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Acesso em: 04 nov. 2017.

ESTADOS UNIDOS DA AMÉRICA. **Records, computers and the rights of citizens**. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 07 de janeiro de 1973. Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>. Acesso em: 21 out. 2017.

FORTES , Vinícius Borges; BOFF, Salete Oro; AYUDA, Fernando Galindo. O Direito Fundamental à Privacidade no Brasil e os Direitos de Privacidade na Internet na Regulação da Proteção de Dados Pessoais. **Revista Eletrônica do Curso de Direito da UFSM**, v. 11, n.1, p. 24-48, 2016. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/19706/pdf>. Acesso em: 20 nov. 2017.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

FORTES, Vinícius Borges; BOFF, Salete Oro. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência (Florianópolis)**, v. 68, p. 109-127, 2014. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109/26949>. Acesso em: 20 nov. 2017.

FRANÇA, Genival Veloso de. **Direito médico**. 14. ed. rev. e atual. Rio de Janeiro: Forense, 2017. [Minha Biblioteca]

HERDY, Thiago. Após compartilhar dados sigilosos de Marisa, médica do Sírio é demitida. **O Globo**, Rio de Janeiro, 02 fevereiro 2017. Disponível em: <https://oglobo.globo.com/brasil/apos-compartilhar-dados-sigilosos-de-marisa-medica-do-sirio-demitida-20864217>. Acesso em: 01 jul. 2017.

KAMEDA, Koichi; PAZELLO, Magaly. e-Saúde e desafios à proteção da privacidade no Brasil. **PoliTICs**, v. 16, p. 31-40, 2013. Disponível em: <https://politics.org.br/edicoes/esa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil>. Acesso em: 20 out. 2017.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães . A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei n. 12.965/2014). In: Newton De Lucca; Adalberto Simão Filho; Cíntia Rosa Pereira de Lima. (Org.). **Direito & Internet III - Tomo I: Marco Civil da Internet (Lei n. 12.965/2014)**. São Paulo: QuartierLatin, 2015.p. 291-367.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ:** novas práticas em informação e conhecimento, v. 2, n. 1, p. 60-76, 2013. Disponível em: <http://revistas.ufpr.br/atoz/article/view/41320/25261>. Acesso em: 20 out. 2017.

LIMA, Cíntia Rosa Pereira de. O Conceito de Tratamento de Dados Após o Caso Google Spain e sua Influência na Sociedade Brasileira. **Conpedi Law Review**, v. 1, n. 9, p. 117-140, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/42/39>. Acesso em: 01 out. 2017.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kennet. **Big Data**: la revolución de los datos masivos. Madrid: Turner Publicaciones, 2013.

O que é a Rede Universitária de Telemedicina (Rute)?. **Portal da RUTE**, 2017. Disponível em: <http://rute.rnp.br/arute>. Acesso em: 01 nov. 2017.

ONU. Organização Das Nações Unidas. **Declaração Universal dos Direitos Humanos**. ONU: 1948. Disponível em: <http://www.onu.org.br/img/2014/09/DUDH.pdf>. Acesso em: 22 set. 2017.

PORTUGAL. **Constituição da República Portuguesa, de 2 de abril de 1976**. Disponível em <http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 04 nov. 2017.

PROTEÇÃO de Dados Pessoais. **Pensando o direito**, Ministério da Justiça, 21 outubro 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/2015/10/conheca-a-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 16 out. 2017.

REZENDE, Edson José Carpintero, et al. Ética e Telessaúde: reflexões para uma prática segura. **Panam Salud Publica**, v. 28, p. 58-65, 2010. Disponível em: <https://scielosp.org/scielo.php?pid=S1020-49892010000700009&script=sci_abstract&tlng=pt>. Acesso em: 28 out. 2017.

REZENDE, Edson José Carpintero, et al. Telessaúde: confidencialidade e consentimento informado. **Revista Médica de Minas Gerais**, v. 23, p. 367-373, 2013. Disponível em: <http://www.rmmg.org/artigo/detalhes/223>. Acesso em: 04 nov. 2017.

RICARTE, Ivan Luiz Marques; GALVÃO, Maria Cristiane Barbosa. **Prontuário do Paciente**. Rio de Janeiro: Guanabara Koogan, 2012.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais da vida e da morte. Belo Horizonte: Del Rey, 1998.

SILVA, Felipe Stribe da. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria: UFSM, 2015. 167p. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade Federal de Santa Maria, Santa Maria, 2015. Disponível em: <http://repositorio.ufsm.br/handle/1/6381>. Acesso em: 01 out. 2017.

SILVA, Helen Ribeiro da; FARIAS, Josivania Silva. Adoção de Tecnologia em Hospitais: o caso da adoção do Sistema AGHU pelos Hospitais Universitários do Brasil. **Revista de Administração Hospitalar e Inovação em Saúde**, v. 13, n. 4, p. 95-111, 2017. Disponível em: <http://revistas.face.ufmg.br/index.php/rahis/article/view/95%20-%20111/1923>. Acesso em: 01 nov. 2017.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314/pdf> Acesso em: 21 set. 2017.

UNIÃO EUROPEIA. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Diretiva 108 de 1980. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 23 set. 2017.

UNIÃO EUROPÉIA. Directiva 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data ando n the free movement of such data. **Official Journal**, Luxemburgo, L 281, 23 Nov. 1995, p. 0031 – 0050. Disponível em: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 19/09/2017.

VALCARENGHI, Emily Vivian. **Gestão de Arquivos Médicos**: uma análise dos arquivos médicos das Universidades federais da região sul do Brasil. Santa Maria: UFSM, 2009. 72 p. Monografia de Especialização, Especialização de Gestão em Arquivos do Programa de Pós-Graduação à Distância – EAD, Universidade Federal de Santa Maria, Santa Maria, 2009.