Revista Jurídica vol. 01, nº. 54, Curitiba, 2019. pp. 292 - 316

DOI: 10.6084/m9.figshare.7841105

APLICATIVOS DE SERVIÇOS PARA SAÚDE E PROTEÇÃO DOS DADOS PESSOAIS DE USUÁRIOS

APPLICATIONS FOR HEALTH SERVICES AND PROTECTION OF PERSONAL DATA FROM USERS

IRINEU FRANCISCO BARRETO JUNIOR

Doutor em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo (2006), atualmente está cursando o Pós Doutorado em Sociologia na Universidade de São Paulo - USP. Mestre em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo (1999) e Bacharel em Sociologia e Ciência Política (1993). Docente de Metodologia da Pesquisa Científica e Didática do Ensino Superior no Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). Analista de Pesquisas da Fundação Sistema Estadual de Análise de Dados Seade. Professor da Escola Superior da Advocacia ESA OAB-SP. Professor dos Cursos de Pós Graduação do Instituto de Direito Público de São Paulo IDP-SP e dos Cursos de Pós Graduação do CERS Complexo de Ensino Renato Saraiva. Coordenador da Comissão Própria de Avaliação (CPA) da FMU e do do FIAM FAAM Centro Universitário (2015-16). Docente fundador do Programa de Mestrado em Sociologia Política da Universidade Vila Velha - ES (2010-2016). Foi Coordenador Adjunto do Curso de Graduação em Direito (2012-2016) e coordenador da Comissão de Iniciação Científica da FMU (2013-2016). Membro do Conselho Editorial da Revista Saúde e Sociedade da Faculdade de Saúde Pública da USP e da Associação Paulista de Saúde Pública. Membro do Conselho Editorial e Científico Nacional e Internacional da Revista Brasileira de Direitos Emergentes na Sociedade Global - Universidade Federal de Santa Maria - RS. Membro do Conselho Editorial Científico Nacional e Internacional da Revista Eletrônica de Direito da UFSM - RS. Possui experiência nas áreas de Ciências Sociais e Direito, com ênfase em Sociedade da Informação, Metodologia e Técnicas de

DOI: 10.6084/m9.figshare.7841105

Pesquisa, Análise de Políticas Sociais, Análise de Dados Estatísticos e docência de Sociologia, Ciência Política, História e Didática do Ensino Superior.

ANDRÉ FAUSTINO

Mestre em Direito na Sociedade da Informação. FMU – 2017. Especialista em Direito Digital aplicado pela FGV - 2016. Extensão em Direito Digital - FAAP. Extensão em Law and Economics of Media Plataforms - University of Chicago - The Law School. Advogado.

RESUMO

Este artigo analisa aspectos jurídicos relacionados a aplicativos de serviços de saúde, dentro do conceito de e-Saúde (saúde eletrônica), e a efetividade da proteção legal de dados pessoais sensíveis processados nesses sistemas. Para tais finalidades, a pesquisa aborda o panorama atual relativo à proteção de dados pessoais no Brasil, com foco na legislação específica relacionada à área da saúde e o sigilo das informações de pacientes. Será discutida ainda a legislação americana, conhecido como HIPAA, que regula especificamente as questões relativas à proteção de dados pessoais sensíveis de saúde. A metodologia do artigo fundamenta-se na técnica analítica, na qual são avaliados os aspectos formalistas da sistematização das regras e normas jurídicas, com foco no ordenamento jurídico e suas relações internas, somado ao enfoque hermenêutico interpretativo, que busca compreender as condutas humanas por meio da atividade discursiva interpretativa. O artigo conclui que embora existam o Marco Civil da Internet e legislações esparsas, ainda não existe um aparato legal que assegure a efetiva proteção de dados pessoais no Brasil, e disso decorrem abusos nas operações que envolvam tratamento de dados pessoais sensíveis dos usuários de aplicativos de saúde.

PALAVRAS-CHAVE: Sociedade da Informação; Marco Civil da Internet; Dados Pessoais.

DOI: 10.6084/m9.figshare.7841105

ABSTRACT

This paper analyzes legal aspects related to health service applications, within the concept of e-Health (electronic health), and the effectiveness of legal protection of sensitive personal data processed in these systems. For this, the research addresses the current panorama regarding the protection of personal data in Brazil, focusing on the specific legislation related to the health area and the confidentiality of patient information. It will also discuss the US legislation, known as HIPAA, which specifically regulates issues related to the protection of sensitive personal health data. The methodology of the article is based on the analytical technique, in which the formalistic aspects of the systematization of legal rules and norms, focusing on the juridical order and their internal relations are evaluated, together with the interpretive hermeneutic approach, which seeks to understand human conduct through of the interpretive discursive activity. The article concludes that although there is a Civil Internet Framework and scattered legislation, there is still no legal apparatus to ensure the effective protection of personal data in Brazil, and this is due to abuses in transactions involving the processing of sensitive personal data of users.

KEYWORDS: Information Society; Brazilian Internet Law; Personal Data.

INTRODUÇÃO

O transcorrer do Século XXI tem assistido a um novo estágio do desenvolvimento histórico, econômico, cultural, social, jurídico e político, denominado por Manuel Castells como Sociedade em Rede (2001, p.73). Esta nova era apresenta, como marco inicial, a ruptura dos padrões de sociabilidade típicos do Século XX, provocada por uma série de eventos sistêmicos e concatenados em escala mundial, aos quais se convencionou denominar como Sociedade da Informação. Inaugura-se um novo estágio do modo de produção capitalista, instaurado pela convergência tecnológica e digital, pelo exponencial crescimento – e consequente diminuição dos

DOI: 10.6084/m9.figshare.7841105

custos da produção de equipamentos informáticos e, principalmente, pela disseminação em escala mundial da Internet.[1]

Dentro do contexto da Sociedade da Informação, cada vez mais surgem novas aplicações ou soluções de internet com as mais variadas finalidades, que vão desde aplicativos de pedidos de refeições, a de serviços de atendimento médico em domicílio. Nesse sentido, algumas possibilidades de lesão a direitos dos usuários aparecem, principalmente relacionadas à questão do tratamento dos dados pessoais dos usuários desses tipos de aplicativos, pois os proprietários e operacionalizadores dessas ferramentas ao oferecerem o seu serviço acabam construindo um banco de dados de todos os usuários que se cadastram, sendo que nos dias atuais esses dados pessoais podem ser comercializados, traduzindo-se em forma de obtenção de receita por parte dos proprietários desses mesmos aplicativos, sem o consentimento desses usuários ou muitas vezes disfarçados nos termos de uso ou políticas de privacidade desses aplicativos. Como contextualização, nos Estados Unidos, já na década de 90, cerca de 92% dos websites coletavam dados pessoais de seus usuários e os processavam segundo seus interesses comerciais (LESSIG, 1999. p. 153).

O mercado de exploração de dados pessoais cada vê mais cresce, devido à natureza do das relações que surgem no ciberespaço[2], segundo Castells (2003, p.145):

> As oportunidades de negócios nessa nova indústria do marketing do comportamento são ilimitadas. Nas eleições de 2000 nos EUA, uma companhia criou um banco de dados, chamado Aristotle, que, usando dados de diferentes fontes, fornecia perfis políticos de nada menos que 150 milhões

[1]Sobre esse contexto, Barreto Junior escreve que: este processo decorreu em razão de três fenômenos, inter-relacionados, que responderam pela gênese da transformação assistida: a) convergência da base tecnológica – possibilidade de poder representar e processar qualquer informação de uma única forma, a digital. Essa convergência teve profundas implicações no processo de mundialização da economia, das telecomunicações e dos processos sociais, pois, sem uma padronização tecnológica mínima, este novo paradigma de sociedade seria inimaginável; b) dinâmica da indústria – proporcionou contínua queda nos preços dos computadores, insumos tecnológicos, softwares, componentes de redes, permitindo maior acessibilidade à integração na rede. c) crescimento e expansão da internet: aumento exponencial da população mundial com acesso à rede e evolução da conectividade internacional." (BARRETO JUNIOR, 2007, p.62).

[2] O termo especifica não apenas a infra-estrutura material da comunicação digital, mas também o universo oceânico de informação que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo 'cibercultura', especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 1999, p. 17).

DOI: 10.6084/m9.figshare.7841105

> de cidadãos, vendendo esses perfis pela maior oferta, em geral dos escritórios de campanha de candidatos políticos.

No Brasil não existe uma legislação específica de proteção de dados pessoais que discipline o processo de tratamento desses dados e tutele as relações advindas desse tipo de processo, sendo, ainda, muito tímida essa questão. A lei 12.965/2014 que ficou conhecida como Marco Civil da Internet não se aprofundou de forma eficaz na questão da proteção dos dados pessoais, no processo de tratamento desses dados e muito menos o decreto 8.771/ 2015 que regulamenta o Marco Civil da Internet, deixando algumas lacunas importantes na forma de proteção e tutela desses dados pessoais no ambiente da internet, pois não especifica a extensão da proteção dos dados, a questão da possibilidade de comercialização deles e como isso deve ser feito, dentro de um ambiente de legalidade, boa fé e de aspecto regulatório, oferecendo riscos aos usuários com possibilidade de lesão às direitos fundamentais como a privacidade e intimidade, consagrados na Constituição Federal de 1988.

São inúmeras as possibilidades de utilização das aplicações de internet, bem como as possibilidades de lesão a direitos dentro desse mesmo ambiente, pois as interações sociais passam a ser cada vez mais velozes e dotadas de fluidez e liquidez (BAUMAN, 2001, p. 36), alguns episódios ficaram conhecidos por conta do vazamento ou da falha no tratamento dos dados pessoais de seus usuários, algumas dessas falhas ocasionaram severas lesões a uma grande quantidade de pessoas pelo mundo, como por exemplo, o vazamento dos dados de cartão de crédito dos usuários da rede PSN da SONY (DA REDAÇÃO, 2011), em 2011, por conta de uma invasão de hackers e o caso do vazamento de dados pessoais do site de relacionamentos extraconjugais Ashley Madison (GRAGNANI, 2015), sendo que esses episódios evidenciaram os riscos inerentes a própria internet e as consequências que podem surgir nos casos de falhas no processo de tratamento dos dados pessoais, gerando reflexos extremamente prejudiciais para todos os envolvidos nesse processo.

Nesse panorama surge no mercado uma série de aplicativos oferecendo serviços ligados à área da saúde, como por exemplo, consultas médicas em domicílio, possibilidade de confecção de prontuários médicos online e até mesmo a simples retirada de exames médicos através de um aplicativo específico ou site de internet, conhecidos e conceituados pela Organização Mundial da Saúde como e-Health ou e-

DOI: 10.6084/m9.figshare.7841105

Saúde[3], sendo que todas essas soluções possuem um processo de coleta de dados pessoais dos seus usuários, bem como possuem em seus bancos de dados essas informações relativas à saúde desses usuários, possibilitando aos proprietários desses aplicativos utilizarem esses dados ou até mesmo comercializarem esses bancos de dados com outras empresas do segmento, como é feito hoje em dia no mercado, sem o consentimento dos donos desses dados. Essas informações são sensíveis e possuem um risco para os usuários em casos de divulgação ou comercialização sem o seu consentimento, pois esses dados podem conter informações de caráter personalíssimo e a sua divulgação ou exposição pode ocasionar danos de extensão evidentemente danosa para o usuário.

O objetivo desse artigo é evidenciar alguns aplicativos ligados aos serviços de saúde existentes no Brasil, a existência de lei ou tutela estatal específica no sentido da proteção da privacidade e dos dados pessoais nesse caso e uma breve análise no diploma legal existente nos Estados Unidos que se chama HIPAA (*Health Insurance Portability and Accountability Act*) como forma de tutela direta e direcionada para os casos de proteção de dados pessoais envolvendo informações de saúde.

A metodologia do artigo fundamenta-se na técnica analítica, na qual são avaliados os aspectos formalistas da sistematização das regras e normas jurídicas, com foco no ordenamento jurídico e suas relações internas, somado ao enfoque hermenêutico interpretativo, que busca compreender as condutas humanas por meio da atividade discursiva interpretativa. Segundo Gustin e Dias (2006, p. 21-25), "[...] a interação entre esses modelos dá-se por meio de um processo dialético de inclusão/complementação/distinção."

2 PANORAMA DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Atualmente no Brasil não existe um diploma legal efetivo e específico voltado para a proteção de dados pessoais, ficando tal encargo por conta de legislações esparsas existentes no ordenamento jurídico, que tratam o assunto de forma

[3] E-Health é o uso das tecnologias da informação e comunicação (TIC) para a saúde.

DOI: 10.6084/m9.figshare.7841105

superficial, não é seguido o modelo existente em outros lugares do mundo como na Europa, por exemplo, que possui algumas diretivas específicas ligadas ao tema, como a Diretiva 95/46/CE de 1995, que será substituída pelo Regulamento Geral sobre a Proteção de Dados da União Europeia[4] que entrará em vigor em 25 de maio de 2018 ou nos Estados Unidos que trata o assunto por legislações específicas direcionadas para cada tipo de relação que possa oferecer riscos nos casos de tratamento de dados pessoais como é o caso do HIPAA, que será visto com mais detalhes adiante e do COPPA[5] (*Children's Online Privacy Protection Act),* que regula as questões relativas à coleta e tratamento de dados de crianças menores de 13 anos, impondo aos operadores de sites ou serviços online dirigidos para menores de 13 anos, uma série de obrigações como, por exemplo, exigir consentimento dos pais do menor para o uso ou coleta de qualquer informação pessoal.

De forma bem singela, no Brasil, a lei 8.078/1990 conhecida como o Código de Defesa do Consumidor (CDC), em seu art. 43 mostra de forma incipiente a proteção do consumidor em relação a proteção dos dados pessoais que estejam arquivados em bancos de dados – "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" - mostrando uma preocupação do legislador com essa questão, sendo que o referido artigo do CDC possui ligação direta com o art. 5º LXXII da Constituição Federal, ao prever o remédio constitucional do *habeas data*[6]*,* preceituando que*:* 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.

[4] O Regulamento Geral sobre a Proteção de Dados da União Europeia será extremamente rígido em relação ao tratamento dos dados pessoais, tratando desde a sua coleta até o descarte desses dados pessoais.

[5] "Impõe certos requisitos aos operadores de sites ou serviços on-line dirigidos a crianças menores de 13 anos e a operadores de outros sites ou serviços on-line que tenha conhecimento real de que eles estão coletando informações pessoais on-line de uma criança com menos de 13 anos de idade."

[6] "O *habeas data* é uma ação constitucional, de caráter civil, conteúdo e rito sumário, que tem por objeto a proteção do direito líquido e certo do impetrante em conhecer todas as informações e registros relativos à sua pessoa e constantes de repartições públicas ou particulares acessíveis ao público, para eventual retificação de seus dados pessoais". (MEIRELLES, 2004. p. 274).

DOI: 10.6084/m9.figshare.7841105

O Marco Civil tem sido de suma importância os defensores do desenvolvimento da Internet como ambiente aberto e livre. Com a sociabilidade humana tornando-se cada vez mais digital, temas como privacidade, liberdade de expressão (BARRETO JUNIOR; CÉSAR, 2017, p.65-88) e poderia ter resolvido a questão de forma mais direta, criando um ambiente de conformidade, não o fez. O referido diploma legal em seu art. 3º, inciso II preceitua que a proteção da privacidade é um dos princípios do uso da internet, mais a frente, em seu art. 7º, inciso I assegura que é direito dos usuários a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação, já nos incisos VII, VIII, XIX e X trata de questões genéricas ligadas ao tratamento de dados pessoais e por fim na seção II, que vai dos artigos 10 ao 12, procura tutelar de forma tímida o processo de tratamento de dados pessoais.

Em todos esses artigos mencionados o legislador não conceitua minimamente o que seriam os dados pessoais[7], muito menos questões específicas sobre a forma do consentimento[8] do usuário em relação ao processo de tratamento de seus dados pessoais, o que representa um cenário de clara insegurança jurídica, favorecendo o surgimento de abusos por parte de quem detém esses dados pessoais. Existe um projeto de lei em tramitação no Congresso Nacional, o projeto nº 5276/2016 (CAMARA DOS DEPUTATOS, 2016), que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, que será um marco inicial em relação à proteção e tutela de dados pessoais no Brasil, esse projeto sofreu influência clara da diretiva europeia 95/46/CE e deverá ser muito importante, pois traz em seu bojo a conceituação dos dados pessoais, dados sensíveis[9], do processo de tratamento dos dados pessoais, da forma que deve ser externado o consentimento por parte do usuário, etc. Um ponto importante desse projeto é que em relação ao consentimento do usuário para o tratamento dos seus

[7] "[...] qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social."

[8] " [...] qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento"

[9] "Dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filantrópico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos".

DOI: 10.6084/m9.figshare.7841105

dados pessoais, quando esses forem sensíveis, o mesmo deve ser dado de forma específica, no teor do art. 11:

> Art. 11. É vedado o tratamento de dados pessoais sensíveis, exceto: I – com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular: a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos em seu tratamento.

Direcionados para a proteção de dados pessoais na área da saúde, especificamente, existem alguns diplomas legais no Brasil como, por exemplo, a Portaria 940/2011 do Ministério da Saúde que regulamenta o Sistema Cartão Nacional de Saúde (Sistema Cartão), prevendo em seu art. 29[10] a proteção dos dados pessoais do usuário do cartão SUS e garantindo o sigilo dessas informações e por fim, a Resolução Normativa 305 (RN305) de outubro de 2012 da Agência Nacional da Saúde que estabelece um padrão obrigatório para troca de informações na saúde suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de planos privados de assistência à saúde, prevendo em seu art. 14[11] requisitos mínimos para a proteção de dados pessoais de atenção e saúde, garantindo sigilo e confidencialidade a esses dados.

Portanto observa-se que não existe um arcabouço jurídico efetivo e necessário para tutelar as relações que envolvam operações que realizem tratamento de dados pessoais, principalmente daquelas onde existam dados sensíveis, como é o caso de aplicativos de e-Saúde, evidenciando um ambiente de insegurança jurídica e possibilidade de abusos por parte daqueles que obtém esses dados pessoais de seus usuários por conta da falta dessa regulamentação.

[10] Art. 29. Os dados e as informações individuais dos usuários do SUS, captados pelo Sistema Cartão e disponibilizados de forma segura e exclusiva ao usuário devidamente identificado por meio do Portal de Saúde do Cidadão, deverão permanecer armazenados sob sigilo.

[11] Art. 14**.** O componente de segurança e privacidade estabelece os requisitos de proteção dos dados de atenção à saúde. **§ 1º** O componente de segurança e privacidade visa assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde. **§ 2º** O componente de segurança e privacidade baseia-se no sigilo profissional e segue a legislação vigente no País.

DOI: 10.6084/m9.figshare.7841105

3 PRIVACIDADE E DADOS PESSOAIS RELATIVOS À SAÚDE

Conforme já explicitado no capítulo anterior, os dados pessoais relativos à saúde são considerados sensíveis, pois evidenciam informações de cunho personalíssimo e que podem expor algo que fira frontalmente direitos da personalidade[12] desses usuários, como por exemplo, a exposição de pacientes acometidos por doenças que são estigmatizadas socialmente como a AIDS ou a hanseníase, a exposição de imagens desses pacientes ou resultados de exames, ocasionando uma lesão permanente e que em alguns casos irreparável, daí a importância de uma tutela específica direcionada para esses tipos de dados pessoais sensíveis.

Cabe destacar que dentro do processo de coleta de dados pessoais existem dois sistemas relativos à forma de manifestação do consentimento do usuário sobre a concordância com a forma que esses dados serão tratados, geralmente são externados nas políticas de privacidade e termos de uso. O primeiro sistema, adotado no Brasil e contido no Marco Civil da Internet, é o sistema *opt in,* que consiste na manifestação expressa e inequívoca do consentimento do usuário em relação à forma como seus dados pessoais serão tratados, não existe a presunção do silêncio como concordância, já o segundo sistema é o *opt out,* não adotado no Brasil, que consiste na manifestação do usuário no sentido em não concordar com a forma de coleta de seus dados, manifestando seu interesse em não permitir esse tratamento, porém nesse caso o silêncio é presumido como concordância.

No contexto da Sociedade da Informação e com o surgimento de novas tecnologias[13] da informação surgem inúmeras possibilidades de oferecimento de aplicações e serviços de internet, dentre elas aquelas direcionadas para a área da saúde, segundo o Instituto HealthCare Informatics, existem mais de 165 mil aplicativos

[12] "[...] o direito de personalidade, os direitos, as pretensões e ações que dele se irradiam são irrenunciáveis, inalienáveis, irrestringíveis. São direitos irradiados dele os de vida, liberdade, saúde (integridade física e psíquica), honra, igualdade". MIRANDA, Francisco Cavalcanti Pontes de. *Tratado de direito privado***.** Atual. Vilson Rodrigues Alves. 2. ed. Campinas: Bookseller, 2000. Tomo I. p. 206.

[13] "As novas tecnologias da informação estão integrando o mundo em redes globais de instrumentalidade. A comunicação mediada por computadores gera uma gama enorme de comunidades virtuais. Mas a tendência social e política característica da década de 1990 a construção social e das políticas em torno de identidades primárias". (CASTELLS, 2016. p.77).

DOI: 10.6084/m9.figshare.7841105

disponíveis para celulares, onde as soluções envolvendo saúde no ambiente digital movimentaram quatro bilhões de dólares, somente na primeira metade do ano de 2017 (LANDI, 2017), evidenciando um mercado extremamente lucrativo.

Em relação à proteção do sigilo dos dados pessoais, da privacidade dos pacientes, bem como a responsabilização dos atores envolvidos nessas relações, existem inúmeras legislações no Brasil que regulam essas questões, embora não exista em relação ao tratamento dos dados pessoais especificamente, a privacidade e a intimidade já são reguladas na Constituição Federal de 1988 em seu art. 5º, inciso X ao preceituar que: "[...] 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."

A privacidade está ligada a dignidade da pessoa humana, princípio também insculpido na Constituição Federal em seu art. 1º, inciso III e está intimamente ligada com a confidencialidade nos casos envolvendo dados sensíveis relativos à saúde das pessoas, onde no ambiente da internet e das aplicações de internet, a possibilidade da violação da privacidade ganha níveis exponenciais, quer seja pela falta de zelo daqueles que realizam o tratamento dos dados pessoais, quer seja dos próprios usuários, segundo Leonardi (2001, p.42) essa é uma das características desse ambiente:

> Esse quadro é particularmente preocupante em relação à privacidade, cuja violação é exponencialmente facilitada pelas mesmas características e peculiaridades que tornam a Internet tão atraente, a tremenda facilidade de disseminação, de busca e de reprodução de informações, em tempo real, sem limitações geográficas aparentes.

No âmbito internacional, existe uma série de diplomas legais que tratam a questão da proteção de dados pessoais, porém alguns são conhecidos e considerados basilares em relação à essa tutela devido o ineditismo, até então. O primeiro deles relaciona-se às Diretrizes ou *Guidelines* da OCDE, que datam do ano de 1980 e tratam sobre proteção de privacidade e fluxos transfronteiriços de dados pessoais, estabelecendo princípios importantes como, por exemplo, limitação de coleta dos dados pessoais, responsabilidade, limitação de uso, dentre outros e existe a Convenção nº 108 do Conselho da Europa para a proteção das pessoas singulares

DOI: 10.6084/m9.figshare.7841105

no que diz respeito ao tratamento automatizado de dados pessoais, que tem origem no ano de 1981 e que influenciou uma série de legislações posteriores pelo mundo, como por exemplo a diretiva 95/46/CE, a referida convenção trata em seu art. 1º sobre a sua abrangência:

> Art. 1. 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 («proteção dos dados»).

Ainda em relação à privacidade e a sua violação dentro do ambiente tecnológico que vivemos nos dias atuais Doneda (2006, p.60) elucida e propõe a necessidade de se adequar a essa nova realidade:

> Por difícil que seja cristalizar a problemática da privacidade em um único conceito, é, no entanto, razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade. Podemos inclusive aventar a hipótese de que o advento de estruturas jurídicas e sociais que tratam do problema da privacidade são respostas a uma nova condição da informação, determinada pela tecnologia.

Existe uma evidente ligação entre a privacidade e a confidencialidade das informações relativas aos dados sensíveis na medida em que a confidencialidade garante a não exposição dos dados ou informações que firam a privacidade dos pacientes ou usuários de aplicativo de saúde, uma das principais formas de externar essas informações ou dados é através dos prontuários médicos[14], quer sejam eles físicos ou eletrônicos. Nesse sentido existe a resolução n.º 1.638/2002, do Conselho Federal de Medicina que estabelece logo em seu art. 1º o aspecto de sigilo das informações lá contidas, a confidencialidade dessas informações busca proteger a privacidade dos pacientes e garantir que aquelas informações não sejam conhecidas

[14]"Definir prontuário médico como o documento único constituído de um conjunto de informações, sinais e imagens 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, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo." (CONSELHO FEDERAL DE MEDICINA, 2002),

DOI: 10.6084/m9.figshare.7841105

ou compartilhadas com pessoas não autorizadas, pois essas informações são de propriedade do paciente.

O próprio código de ética médica[15] prevê o dever de sigilo entre médico e paciente, estabelecendo um parâmetro legal para esse tipo de relação que envolve a circulação de uma série de informações sobre o paciente, forma de tratamento, tipo de doença, dentre outros, impondo obrigação legal àqueles que manipulam e recebem essas informações, além do próprio dever moral que abarca as possibilidades de informação nesse tipo de ambiente, a manutenção desse sigilo garante a gestão desses dados pessoais, que fica a cargo da própria pessoa que fará o juízo de valor sobre a conveniência e oportunidade de compartilhamento ou divulgação desses dados.

A proteção do sigilo das informações dos pacientes é tão forte que, inclusive, não podem ser divulgadas nem mesmo ao Judiciário sem a autorização do paciente, conforme expresso no código de ética médica: É vedado ao médico:

> Art. 73. 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. Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime o médico estar á impedido de revelar segredo que possa expor o paciente a processo penal.

Outros diplomas legais ligados à área da saúde tratam da questão do sigilo em relação à proteção dos dados dos pacientes, como o código de ética dos profissionais de enfermagem em seu art. 29 ao preceituar que os profissionais de enfermagem devem manter segredo sobre fato sigiloso de que tenha conhecimento em razão de sua atividade profissional, exceto nos casos previstos em Lei; o código de ética e deontologia da fisioterapia em seu art. 9º, inciso IV ao prever que manter segredo sobre fato sigiloso de que tenha conhecimento em razão de sua atividade profissional e exigir o mesmo comportamento do pessoal sob sua direção, salvo

[15] XI - O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei. Disponível em https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf. Acesso em 31 jul. 2017.

DOI: 10.6084/m9.figshare.7841105

situações previstas em lei. Em uma simples exegese verifica-se que os códigos de ética ligados à área da saúde repetem quase que literalmente o mesmo teor para os artigos relativos ao sigilo das informações dos pacientes.

Sob o ponto de vista criminal existe a tipificação da conduta de violação de segredo profissional, prevista no Código Penal Brasileiro, nos seguintes termos: 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. No Brasil, em um episódio lamentável, funcionários do hospital Sírio Libanês compartilharam dados sigilosos sobre o diagnóstico da esposa do ex-presidente Lula, evidenciando o risco que existe em utilização de tecnologia integrada com a área da saúde.

Por óbvio, existem exceções legais, conhecidas como "justa causa" para a quebra do sigilo e consequente possibilidade de divulgação de informações[16] ou dados pessoais dos pacientes, que devem envolver riscos para o próprio paciente, outras pessoas ou uma coletividade, bem como devem vir acompanhadas de plausível fundamento, se enquadrando nas hipóteses previstas na lei. Nesse sentido destaca-se a Portaria 1.271/2014, do Ministério da Saúde que define a lista nacional de notificação compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional, nos termos do anexo, e dá outras providências, que em seu art. 3º prevê, como obrigatória, a notificação compulsória; a Resolução CFM 1.605/2000 que preceitua em seu art. 2º que nos casos do art. 269 do Código Penal, onde a comunicação de doença é compulsória, o dever do médico restringe-se exclusivamente a comunicar tal fato à autoridade competente, sendo proibida a remessa do prontuário médico do paciente; o próprio art. 269 do Código Penal Brasileiro que prevê como conduta criminosa deixar o médico de denunciar à autoridade pública doença cuja notificação é compulsória.

[16] "A informação pessoal deve observar certos requisitos para a sua caracterização como tal. Uma determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Esse vínculo significa que a informação se refere às características ou ações dessa pessoa, que podem ser atribuídas a ela seja em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes, por exemplo, aos seus hábitos de consumo, sobre opiniões que manifesta, à sua localização e tantas outras" (DONEDA, 2004. p. 62).

vol. 01, nº. 54, Curitiba, 2019. pp. 292 - 316

DOI: 10.6084/m9.figshare.7841105

4 APLICAÇÕES DE INTERNET EM SERVIÇOS DE SAÚDE NO BRASIL

Com a definição e efetiva possibilidade do emprego de aplicações de internet voltadas para os serviços de saúde, acabam surgindo algumas propostas ou soluções voltadas para esse mercado, que devido à sua natureza, fatalmente, envolvem nas operações onde ocorra o tratamento de dados pessoais riscos para os usuários, serão listadas nesse capítulo as principais ferramentas existentes hoje no Brasil, seja de caráter particular ou de estatal, bem como o tipo de serviço que oferecem para os usuários.

4.1 O APLICATIVO E-SAÚDE

O Ministério da Saúde em primeiro de junho de 2017 lançou um aplicativo (GOVERNO DO BRASIL, 2017) de âmbito nacional que se chama e-Saúde, utiliza como nome do aplicativo o termo definido pela Organização Mundial da Saúde para designar as soluções de TIC (tecnologias de informação e comunicação) direcionadas para a área da saúde. Esse aplicativo ou solução oferece uma série de informações que possuem relação com os dados dos usuários do Sistema Único de Saúde (SUS) como, por exemplo, dados do cartão nacional de saúde, lista de medicamentos retirados em unidades de saúde, informações sobre o cartão de vacinação, lista de exames realizados, dentre outros.

As informações são centralizadas em um banco de dados e será possível o estreitamento e análise das informações dos usuários em consonância com a utilização de unidades de saúde pública espalhadas pelo Brasil. Esse aplicativo foi uma das primeiras ações do Estado direcionadas para a população utilizando tecnologia integrada com os serviços de saúde no formato conhecido como e-Health ou e-Saúde, com a possibilidade de operações que envolvem o ciclo completo de tratamento de dados pessoais, onde o aplicativo vai armazenar todo o histórico de saúde de cada usuário com base nos dados no cartão SUS. Embora bastante interessante a solução, em uma pesquisa básica no site do Ministério da Saúde ou no próprio aplicativo e-Saúde, não é possível localizar a política de privacidade e os termos de usos, descriminando de forma transparente como serão tratados os dados

DOI: 10.6084/m9.figshare.7841105

pessoais do usuário, que tipo de dado pessoal será armazenado efetivamente, quem terá acesso a esses dados, possibilidade de exclusão de dados por parte dos usuários, e, principalmente, a respeito do consentimento dos usuários (pacientes) no que tange à forma de tratamento desses dados pessoais.

Embora a solução seja bastante interessante como parte de uma política pública relacionada ao gerenciamento de dados de saúde dos usuários do sistema, esse aplicativo oferece claros riscos aos usuários, devido a não exposição de como esses dados pessoais serão tratados por parte do poder público e qual a extensão desse tratamento, ficando uma lacuna nesse sentido, dessa forma podendo surgir possibilidades de compartilhamento desses dados pessoais dos usuários, bem como episódios de vazamento de dados pessoais sensíveis nos moldes do que ocorreu na Prefeitura de São Paulo no ano de 2016 (HERNANDES, 2016), onde dados pessoais, e até mesmo dados de prontuário médico de pacientes da rede pública municipal de saúde foram expostos na internet sem a autorização, por conta de não estarem protegidos por mecanismos de segurança digital.

4.2 APLICATIVO PARA PESSOAS COM DIABETES

Ao digitar na appstore do Google, a Google Play, em busca de aplicativos que ajudam o controle da diabetes ou que monitoram glicemia, aparecem mais de 200 resultados, com aplicativos que variam desde dicionários sobre remédios de diabetes, com nomenclaturas específicas direcionadas a esse tipo de doença, até aqueles que prometem avaliar os níveis de glicemia no sangue com base em inúmeras tabelas que são alimentadas pelos usuários que inserem os dados das medições diárias de sua glicemia.

Todos os aplicativos oferecidos são bastante interessantes no formato de apresentação de suas funcionalidades, ainda, existindo a possibilidade de preenchimento de campos de dados pessoais que variam entre tipo sanguíneo, peso corporal, medicação que o usuário utiliza etc. Porém em todos os aplicativos que foram visitados (cerca de 30) e analisados, não existem termos de uso e políticas de privacidade adequadas para a natureza do serviço e em alguns casos, nem sequer existem tais documentos, não evidenciando condições mínimas para os usuários

DOI: 10.6084/m9.figshare.7841105

obterem conhecimento e decidirem como os seus dados pessoais serão tratados por parte do proprietário do software.

Embora essas soluções sejam bastante interessantes, a sua grande maioria não oferece condições mínimas de segurança jurídica para a utilização, pois não são transparentes em seus termos de uso e políticas de privacidade, oferecendo riscos para os seus usuários, pois a apresentação é confusa ou até mesmo inexistente, embora o Brasil não possua uma legislação específica que proteja as operações que envolvam tratamento de dados pessoais, ainda mais dados sensíveis de saúde, seria no mínimo razoável que essas empresas se preocupassem minimamente com as questões relativas ao processo de tratamento dos dados pessoais de seus usuários diante da natureza intrínseca que eles possuem, no sentido de serem comercializados pelos seus proprietários com laboratórios, hospitais ou até mesmo empresas do ramo farmacêutico, tudo isso sem o consentimento do dono dessa informação, que é o usuário final.

4.3 APLICATIVO DE MONITORAMENTO DA SAÚDE

Os aplicativos de monitoramento de saúde são os mais oferecidos na internet, pois através deles é possível que os usuários monitorem as suas informações de saúde em tempo real. O aplicativo permite que sejam inseridos todos os dados relacionados à saúde como, por exemplo, dietas feitas, exames médicos realizados, doenças que o usuário já foi acometido, medicações que toma, dentre outros. Dessa forma o aplicativo monitora todas as questões relacionadas à saúde do usuário, permitindo emitir alertas para horário de refeições, consultas médicas, momento de tomar remédios, pode ainda, calcular o peso ideal e mais uma gama de funcionalidades.

Esse tipo de aplicativo é bastante interessante, pois permite que seja montado um histórico do usuário, ficando disponível no banco de dados do proprietário do aplicativo e que pode ser consultado a qualquer hora, servindo como uma boa ferramenta para melhora na qualidade de vida de seus usuários, porém devido essa característica interativa e uma plataformas de utilização bastante amigável, essas soluções são oferecidas em grande volume através de páginas de comercialização de

DOI: 10.6084/m9.figshare.7841105

aplicativos, conhecidas como appstore. A empresa proprietária do aplicativo, dessa forma, consegue obter uma grande quantidade de dados pessoais sensíveis de seus usuários e de todos os aplicativos aqui mostrados, os de monitoramento de saúde são os que mais riqueza de dados coletados possui, pois ele abarca uma série de possibilidades relativas ao usuário, alguns são tão detalhistas que até a marca de tênis que o usuário utiliza é possível descobrir, pois existem campos para inserir esse tipo de dado, dessa forma fica evidente a possibilidade de lesão e de utilização desses dados de diversas formas.

Embora os aplicativos sejam oferecidos no Brasil e o usuário, em sua grande maioria, seja brasileiro, os termos de uso e políticas de privacidade são todos escritos em inglês, dificultando, mais ainda, a compreensão dos termos utilizados, bem como a possibilidade da manifestação do consentimento dos usuários em relação à forma que seus dados pessoais serão tratados pelo proprietário desses aplicativos, o que evidencia, mais uma vez, um grande risco e possibilidade de lesão a uma quantidade muito grande de pessoas.

5 O HIPPA E A EXPERIÊNCIA DOS ESTADOS UNIDOS NA PROTEÇÃO DE DADOS PESSOAIS DE SAÚDE

No ano de 1996 houve a aprovação de uma lei nos Estados Unidos direcionada para o mercado de seguros de saúde, o HIPAA (Health Insurance Portability and Accountability Act), que em linhas gerais regula a portabilidade e responsabilidade dos seguros de saúde. A sua aplicabilidade é direcionada para toda e qualquer empresa de saúde, seguro de saúde, centro de processamento de informações e, até mesmo, entidades híbridas como universidades ou pequenos negócios/ empresas como, por exemplo, cuidados direcionados à pacientes em home care e embora tenha tratado de outras questões relativas aos seguros de saúde, ficou bastante conhecida e teve a sua força efetiva direcionada à proteção de dados pessoais sensíveis, ligados principalmente a privacidade, bem como o uso e exposição de informações protegidas dos usuários do sistema de saúde.

DOI: 10.6084/m9.figshare.7841105

Antes da existência do HIPAA existia a cultura e entendimento, no mercado de saúde dos Estados Unidos, de que os dados pessoais constantes nos bancos de dados de organizações privadas pertenciam a essas organizações, existindo a possibilidade de monetização desses dados, trazendo severos prejuízos para os pacientes que tinham seus dados pessoais comercializados sem a sua autorização. Embora a norma trate da questão de portabilidade dos planos de saúde, o seu objetivo principal acabou sendo a proteção da privacidade dos dados pessoais dos pacientes, buscando garantir que informações de saúde protegidas sejam preservadas em um ambiente de conformidade e regulação.

Foram criadas várias regras de privacidade inseridas como princípios basilares estruturantes do formato de tutela dos dados pessoais da referida norma, em um conceito conhecido como *Safe Harbor*, que significa porto seguro, sendo que nessas regras estão delimitados e descritos todos os regulamentos que cuidam do processo completo do tratamento desses dados pessoais, estabelecendo, ainda, várias sanções nas áreas administrativa, cível e criminal.

A Regra de Privacidade busca proteger as informações de saúde pessoalmente identificáveis, que podem ser criadas ou recebidas por alguma organização abrangida pela norma. O conceito de informação de saúde pessoal identificável, no HIPAA, pode ser definida como uma informação que pode incluir dados demográficos, dados que relacionam-se com a saúde, condição física ou mental passada, presente e futura de um indivíduo; com a prestação de cuidados de saúde a um indivíduo ou passado, presente e futuro; ao pagamento para a prestação de cuidados de saúde para o indivíduo em relação à existência de uma base razoável que faça com que a informação possa ser utilizada para identificar o indivíduo.

A estrutura da norma possui uma série de capítulos que buscam estabelecer as condutas relativas às questões de portabilidade e responsabilidade relativa aos planos de saúde, porém em seu capítulo II (HIPAA, 2017), subtítulo C, seção 221 a norma trata especificamente sobre a coleta de dados estabelecendo um programa de integridade para evitar o abuso e fraudes no processo de coleta de dados pessoais dos usuários do sistema de saúde, porém no texto original da norma não existem preceitos muito específicos voltados para a questão da privacidade e proteção dos dados pessoais.

DOI: 10.6084/m9.figshare.7841105

Ao longo de quase uma década foram aprimoradas questões relativas às regras de privacidade do HIPAA, já que em seu texto inicial trava de forma superficial a questão da proteção dos dados pessoais, sendo que em 2004 houve a publicação da versão que apresentava as regras de privacidade relativas à proteção dos dados pessoais em todo seu tratamento, porém no ano de 2007 houve a inserção da parte 160 no capítulo 45 (GPO, 2007) no CFR (Code of Federal Regulation) do Departamento de Serviços Humanos e Saúde dos Estados Unidos, criando efetivamente as regras de privacidade.

Por fim no ano de 2013, houve mais uma alteração da referida norma, estabelecendo o HITECH (FEDERAL REGISTER, 2013) (Health Information Technology for Economic and Clinical Health Act), com essa modificação o HIPAA ganhou mais força e eficácia no que se refere à proteção da privacidade, inclusive informação genética, estando mais alinhado com as questões relativas à tecnologia e processos de tratamento de dados no formato digital, estabelecendo multas por violação dos preceitos contidos na norma que variam de cem dólares e podem chegar até um milhão e meio de dólares.

Os dados pessoais dos pacientes podem ser divulgados mediante autorização voluntária por qualquer motivo, inclusive para fins de pesquisa, porém a validade desse consentimento deve estar de acordo com a regra de privacidade, devendo a autorização ser específica e significativa, existindo formulários específicos para a manifestação desse consentimento, segundo Pritts (2008, p.31) existem complementos para que essa autorização seja válida:

> A autorização de acordo com a Regra de Privacidade difere do consentimento informado em pesquisa. A autorização indica como, por que, e para quem a informação pessoal de saúde será usada e / ou divulgada para pesquisa, e pede permissão para esse uso ou divulgação. Em contraste, o consentimento informado descreve os potenciais riscos e benefícios da pesquisa e busca permissão para envolver o assunto, embora também forneça aos participantes da pesquisa uma descrição de como a confidencialidade dos registros de pesquisa será protegida.

O HIPAA foi um divisor de águas na questão da proteção de dados pessoais sensíveis relacionados à saúde, pois tratou de forma efetiva e direcionada essa questão bastante crítica e que cada vez mais ganha importância com a evolução das

vol. 01, nº. 54, Curitiba, 2019. pp. 292 - 316

DOI: 10.6084/m9.figshare.7841105

ferramentas tecnológicas voltadas para a área da saúde, já que facilita a circulação da informação e a prestação efetiva e rápida de serviços essenciais, mas por outro lado ficando mais suscetível a violações, quer seja pelas próprias entidades que recebem esses dados, quer seja por terceiros mal intencionados que procuram obter essas informações e ganhar algum proveito econômico com a sua comercialização.

CONCLUSÃO

Embora existam operações, no Brasil, que realizem o tratamento de dados pessoais de forma efetiva, com isso obtendo lucros e oferecendo risco de lesão a direitos da personalidade de seus usuários, não existe no país um diploma efetivo e direcionado para a tutela desse tipo de relação jurídica, embora exista um esforço legislativo para a aprovação do projeto de lei que irá tratar essa questão de forma direcionada, o fato é que existe essa lacuna, tendo que o usuário que se socorrer ao Poder Judiciário que buscará uma solução com base no que existe hoje e que não atende as reais necessidades no sentido de proteção dos usuários que, por ventura, tenham seus dados pessoais utilizados de forma abusiva. Por óbvio que empresas sabem dessa realidade e acabam aproveitando o atual cenário para cometer abusos no processo de tratamento desses dados pessoais, principalmente na coleta e utilização desses dados.

Em relação aos dados pessoais sensíveis relacionados à saúde, o cenário é mais preocupante ainda, pois devido à natureza desses dados e a sua possibilidade de monetização eles são alvo de empresas dos mais diversos ramos da área da saúde como, por exemplo, laboratórios, empresas do ramo farmacêutico, planos de saúde etc. Nesse sentido a inexistência de uma legislação geral de proteção de dados é extremamente prejudicial e, mais ainda, a inexistência de um diploma legal que regule e tutele as questões relativas aos dados pessoais sensíveis relacionados à saúde, é algo que traz sérios prejuízos para os usuários desse tipo de aplicações de internet.

Cada vez mais com a evolução da tecnologia, surge a possibilidade de diversas aplicações de internet voltadas para a área da saúde e no Brasil, conforme mostrado nesse artigo, existem inúmeras soluções voltadas para o campo de

DOI: 10.6084/m9.figshare.7841105

cuidados da saúde ou monitoramento da saúde oferecidas para os usuários, sendo que a única garantia ou possibilidade de conhecimento de como os dados pessoais serão tratados é através dos termos de uso ou políticas de privacidade, que na maioria das vezes são inexistentes ou inadequados para informar de forma clara e precisa como será feito esse tratamento e, ainda, inexistindo a possibilidade de manifestação ou não, por parte do usuário, do seu consentimento em relação à essa forma de tratamento.

A experiência dos Estados Unidos é de grande valia, já que ao longo de quase vinte anos foram maturando o arcabouço legal de forma a fornecer uma tutela efetiva da proteção de dados pessoais relativos à saúde, o HIPAA foi evoluindo com o passar do tempo e transformou-se em uma regra de privacidade direcionada, acompanhando as evoluções tecnológicas e consequentes demandas que foram surgindo, oferecendo um ambiente claro de legalidade e regulação. A referida norma que começou tratando a questão da privacidade de forma incidental em seu início, foi se amoldando às necessidades que foram surgindo, às possibilidades de inserção na seara da proteção dos dados pessoais e tornou-se uma referência nesse sentido, sendo um ótimo ponto de referência para o Brasil, na árdua tarefa de buscar uma regulação adequada e que permita o desenvolvimento das tecnologias voltadas para a área da saúde, mas com as devidas salvaguardas regulatórias.

Dessa forma é possível verificar que, ainda, falta a criação de um diploma legal específico que discipline a questão da proteção de dados pessoais no Brasil de forma a permitir transparência e legalidade em todos os processos que envolvam tratamento de dados pessoais, principalmente por conta da agilidade no avanço das ferramentas tecnológicas, evitando que ocorram danos aos usuários ou abusos por conta dos proprietários dessas aplicações. A iniciativa do projeto de lei 5276/2016 é bastante positiva e deve vir acompanhada de uma discussão efetiva com a sociedade, da mesma forma que ocorreu no projeto 2126/2011 que mais tarde deu origem ao Marco Civil da Internet, de forma a permitir que nele estejam contidas as reais necessidades de proteção do indivíduo e seja um marco inicial na tutela da proteção da privacidade e proteção de dados pessoais na internet no Brasil.

Em relação às aplicações voltadas para a área da saúde, a atenção deve ser maior diante da natureza desse tipo de dado pessoal sensível, que se for mal utilizado

DOI: 10.6084/m9.figshare.7841105

ou divulgado de forma irresponsável pode lesionar de forma permanente uma grande quantidade de pessoas, sendo esse um desafio para o legislador no sentido de criar mecanismos legais de regulação dessa parte do mercado, gerando confiabilidade e credibilidade no oferecimento desse tipo de aplicação.

REFERÊNCIAS

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a Pesquisa Jurídica. In: PAESANI, Liliana Minardi (coord.). **Direito na Sociedade da Informação.** São Paulo: Atlas, 2007.

_____. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO; Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). **Direito & Internet III: Marco Civil da Internet.** 1ed.São Paulo: Quartier Latin, 2015, v. 2, p. 100-127.

_____. CÉSAR, Daniel. Marco Civil da Internet e Neutralidade da Rede: Aspectos Jurídicos e Tecnológicos. **Revista Eletrônica do Curso de Direito da UFSM**, v. 12, n. 1 / 2017 p.65-88.

BAUMAN, Zygmunt. **A Modernidade líquida.** Rio de Janeiro: Jorge Zahar, 2001.

BRASIL. Marco Civil da Internet. **Lei 12.964/14.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 jun. 2017.

CÂMARA, DOS DEPUTADOS. Projeto de Lei nº 5276/2016, 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.** Pl, v. 5276, 2016.

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

_____. **A sociedade em rede.** 17ª edição. São Paulo: Paz e Terra, 2016.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.638/2002.** Disponível em https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf. Acesso em 31 jul. 2017.

DA REDAÇÃO. Autoridades indagam Sony sobre vazamento de dados de brasileiros na rede PlayStation Network. In: **Veja.** 2011. Disponivel em:

DOI: 10.6084/m9.figshare.7841105

https://veja.abril.com.br/tecnologia/autoridades-indagam-sony-sobre-vazamento-de-dados-de-brasileiros-na-rede-playstation-network/. Acesso em 20 jul. 2017

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

_____. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coordenador). São Paulo: Atlas, 2014.

FEDERAL REGISTER. ***Department of Health and Human Services.*** 2013. Disponível em: https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Acesso em 30 Jul. 2017.

GPO. U.S. ***Government Printing Office.*** 2007. Disponível em <https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1.pdf>. Acesso em 30 Jul. 2017.

GRAGNANI, Juliana. Brasileiros no site de traição Ashley Madison temem ser descobertos após vazamento. In: **Folha de S.Paulo.** 2015. Disponível em <http://www1.folha.uol.com.br/cotidiano/2015/09/1678425-brasileiros-no-site-de-traicao-ashley-madison-temem-ser-descobertos-apos-vazamento.shtml>. Acesso em 20 jul. 2017.

GUSTIN, Miracy B.S.; DIAS, Maria Teresa Fonseca. **(Re)pensando a Pesquisa Jurídica.** 2.ed. ver., ampl. e atual. Belo Horizonte, Del Rey, 2006.

HERNANDES, Raphael. Gestão Haddad expõe na internet dados de pacientes da rede pública. In: **Folha de S.Paulo.** 2016. Disponível em <http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml>. Acesso em 30 jul. 2017.

HIPAA. ***Health Insurance Portability and Accountability Act.*** Disponível em <http://www.legalarchiver.org/hipaa.htm>. Acesso em 30 jul. 2017.

LANDI, Heather. *Digital Health Venture Capital Funding Tops $4 Billion in First Half of 2017.* 2017. *In:* ***Hea!thcare innovation.*** Disponível em: https://www.hcinnovationgroup.com/population-health-management/mobile-health-mhealth/news/13028921/digital-health-venture-capital-funding-tops-4-billion-in-first-half-of-2017. Acesso em 30 Jul.17.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo Ed. Saraiva. 2011. p. 42.

LESSIG, Lawrence. ***Code and other laws of cyberspace***. New York: Basic Books, 1999.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34. 1999.

DOI: 10.6084/m9.figshare.7841105

MEIRELLES, Hely Lopes. **Mandado de Segurança:** ação popular, ação civil pública, mandado de injunção, habeas data, ação direta de inconstitucionalidade. 27ª ed. São Paulo: Malheiros Editores, 2004.

MINISTÉRIO DA SAÚDE. Portaria n º 1.271, de 6 de junho de 2014. **Define a Lista Nacional de Notificação Compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional, nos termos do anexo, e dá outras providências.** Disponível em <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2014/prt1271_06_06_2014.html>. Acesso em 31 jul. 17.

MIRANDA, Francisco Cavalcanti Pontes de. **Tratado de direito privado.** Atual. Vilson Rodrigues Alves. 2. ed. Campinas: Bookseller, 2000. Tomo I.

GOVERNO DO BRASIL. **Aplicativo vai ampliar o acesso da população às informações de saúde.** 2017. Disponível em <http://www.brasil.gov.br/saude/2017/06/aplicativo-vai-ampliar-o-acesso-da-populacao-as-informacoes-de-saude>. Acesso em 30 jul. 2017.

PRITTS, J. ***The importance and value of protecting the privacy of health information:*** *Roles of HIPAA Privacy Rule and the Common Rule in health research*. 2008.

WHO. ***World Health Organization***. Disponível em <http://www.who.int/ehealth/en/>. Acesso em 18 jul. 2017.