A SOCIEDADE EM REDE E A INFORMAÇÃO EM SAÚDE: UM DIREITO EM CONSTRUÇÃO NO BRASIL

Fernanda Tavares Sonda[1]

RESUMO: O presente artigo tem como tema principal a informação em saúde inserida na sociedade em rede. Ao considerarmos que a informação em saúde se apresenta como um bem de alto valor, com potencial considerável de lucro, a problemática que impulsiona a pesquisa visa analisar qual a importância dessa informação no atual cenário social, denominado sociedade da informação. Adotou-se o método de abordagem dedutivo e como técnica a pesquisa bibliográfica. A temática é desenvolvida a partir da violação aos direitos de privacidade demandando, para tanto, a adoção de medidas protetivas efetivas. O tema mostra-se relevante no momento em que se verifica a possibilidade de monetarização da informação, gerando risco ao consumidor.

PALAVRAS-CHAVE: Informação em saúde. Sociedade em rede. Sociedade da informação.

SUMÁRIO: 1 Introdução. 2 A internet, a sociedade em rede e a disseminação de dados na sociedade da informação. 2.1 E-saúde e o mercado: um viés econômico da informação. 3 O problema da proteção da privacidade das informações em saúde. 3.1 Desafios à proteção de dados pessoais sensíveis no âmbito da Sociedade de Informação e a necessidade de um marco regulatório do tratamento de dados em saúde. 4 A economia de dados sensíveis: big data e a revolução na área da saúde. 4.1 A funcionalidade dos bancos de dados e cadastros de consumo em saúde e o abuso dos fornecedores ao comercializar informações e dados sensíveis de saúde. 5 Considerações finais. 6 Referências.

1 Analista Processual da Defensoria Pública do Estado do Rio Grande do Sul. Mestre em direito pelo Programa de Pós-Graduação em Direito – Mestrado e Doutorado da Universidade de Santa Cruz do Sul, na linha de pesquisa Constitucionalismo Contemporâneo. Bacharela em Direito graduada pela Universidade de Caxias do Sul. Farmacêutica graduada pela Universidade de Caxias do Sul.

1 INTRODUÇÃO

No contingente da sociedade da informação, é necessário desenvolver questões que possam equilibrar o direito fundamental à intimidade e à vida privada face aos avanços da tecnologia da informação. Tal contexto exige medidas que regulem expressamente questões específicas sobre a proteção de dados pessoais, os quais são alvos necessários dos inovadores recursos tecnológicos.

Considerando que o mercado de saúde movimenta quantidades gigantescas de recursos, pensar na coleta e venda desses dados enquanto negócio é um tanto quanto razoável. Nesse sentido torna-se indiscutível tratar os dados de saúde como dados pessoais sensíveis, e por isso sujeita-los a um regime especial de proteção, justificado pela necessidade de proteção da confidencialidade, que exigem a adoção de medidas de segurança adequadas. A fim de garantir que esse mercado ganhe transparência, foi sancionada a Lei Geral de Proteção de Dados, em meados de 2018, a qual ajuda a garantir a privacidade dos consumidores em saúde.

A preocupação dessa pesquisa foi reforçada a partir de março de 2018, quando da repercussão mundial acerca da notícia sobre o vazamento de informações de dezenas de milhões de perfis do Facebook, os quais ficaram à disposição da empresa de análise de dados Cambridge Analytica. Considerando que esse escândalo tomou proporções ainda maiores, uma vez que os dados foram coletados em sua grande maioria sem o consentimento dos usuários, de forma dissimulada, a partir da realização de um teste de personalidade (RAPÔSO et al., 2019, p. 59). Curiosamente o Facebook, vinha sondando hospitais e outras instituições de saúde dos Estados Unidos, propondo o compartilhamento de informações dos usuários. A ideia era cruzar os dados fornecidos pelas instituições (sexo, faixa etária, doença e prescrições) com o material existente no próprio Facebook, para em teoria, ajudar a identificar pacientes com necessidades de cuidados especiais. Entretanto, reitera-se que, em nenhum momento foi discutida a necessidade de informar os pacientes sobre o uso de seus dados, tampouco pediram-lhe sua permissão.

Embora breve, far-se-á uma contextualização sobre a sociedade da informação, com o propósito de identificar formas de prevenir ações atentatórias aos direitos e liberdades fundamentais referentes aos dados pessoais especialmente os

dados de saúde, o que justifica o uso do método dedutivo e, acessoriamente, o método dialético, amparados pela pesquisa em referencial bibliográfico pertinente, vez que a temática demanda um constante debate.

Essa pesquisa está comprometida em buscar uma tutela efetiva e eficaz aos direitos que estão destituídos de proteção devido ao descompasso entre o direito e a tecnologia. Nesse sentido, para enfrentar os problemas advindos da revolução tecnológica, faz-se mister que o direito à proteção de dados contemple um direito apto a ser protegido por norma específica. Em um mundo digital e globalizado, o acesso a informações de caráter pessoal torna-se um recurso utilizado em demasia, por isso a necessidade de estabelecer limites quanto à coleta e uso de dados pessoais como forma de proteção frente a eventuais abusos.

2 A INTERNET, A SOCIEDADE EM REDE E A DISSEMINAÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO

A internet é o fruto da convergência do desenvolvimento das telecomunicações e dos computadores. O telégrafo, o telefone, o rádio e o computador prepararam o palco para a integração de capacidades únicas da Internet, que é, concomitantemente, um mecanismo de disseminação de informações de alcance mundial e um meio para a interação e colaboração entre pessoas, independente de localização geográfica. Assim, a fluidez das relações sociais, em grande medida, se desenvolve no âmbito da Sociedade da Informação, por meio do acesso à internet.

A potencialidade da comunicação, a partir das modernas tecnologias da informação, permitiu, no plano das relações humanas, estabelecer comunicações em escala planetária, que transcende qualquer limite espacial, a uma velocidade de transmissão praticamente instantânea. A fluidez contextualizada é algo jamais visto até então na história das relações sociais (PEREZ-LUÑO, 2012, p. 22).

Ainda nesse sentido, importa considerar que os novos meios de comunicação são desenvolvidos, introduzidos e modificam a maneira pela qual o indivíduo se relaciona com os outros. Tal transformação é intermediada pela comunicação (THOMPSON, 2011, p. 09).

Nessa seara, destaca-se que a internet perfaz o meio que consolida a comunicação interpessoal, a partir da interação em ambiente virtual. “A internet é um

tecido da comunicação em nossas vidas: para o trabalho, os contatos pessoais, a informação, o entretenimento, os serviços públicos, a política e a religião" (CASTELLS, 2009, p. 100).

A internet passou a ser a base tecnológica para a forma organizacional da era da informação: a rede. Nesse sentido, a rede representa a nova morfologia social da sociedade. Importa destacar rede enquanto sujeito de modificação, responsável por processos produtivos e de experiência com impacto no poder e na cultura, reforçando a importância das redes nos processos produtivos e de experiência (CASTELLS, 2003, p. 07-08).

A rápida interação em rede, encontra fundamento no paradigma da sociedade em rede, onde a sociedade, impulsionada pela revolução das tecnologias da informação, altera suas bases materiais, tornando-se cada vez mais descentralizada, interconectada e interdependente (CASTELLS, 2005, p. 39).

As redes foram criadas para melhorar a comunicação. Em termos espaciais, a principal característica da sociedade em rede é a conexão entre o local e o global. Assim, quanto maior o poder de comunicação, proporcionalmente maior será o poder de dominação sobre a concorrência (CASTELLS, 2005, p. 109).

Esse conceito de rede nasce da necessidade de adaptação a uma nova estrutura social desenvolvida a partir das tecnologias que revolucionaram o planeta. Nesse contexto, vale destacar, que Lèvy trabalha a ideia de que nenhum tipo de conhecimento independe do uso de tecnologias intelectuais, ou seja, as novas tecnologias intelectuais apresentam base na informática (LÈVY, 2010, p. 75).

A rede informático-mediática é uma das faces dos múltiplos circuitos de comunicação e interação que estimulam a coletividade (LÈVY, 2010, p. 119).

A sociedade contemporânea pode ser representada pela sociedade em rede, enquanto aspectos voltados à flexibilidade e adaptabilidade como competências essenciais à inovação e à criatividade no mundo globalizado. Esse mesmo cenário, ainda pode ser descrito a partir de conceitos de ciberespaço e cibercultura. Assim, por ciberespaço desenvolve-se a ideia de um novo meio de comunicação permitido através da interconexão de computadores em escala global. Já a cibercultura, especifica um conjunto de técnicas materiais e intelectuais (de práticas e valores), que exsurgem no campo do ciberespaço (LÈVY, 1999, p. 17).

O termo ciberespaço também pode ser encarado como uma nova fronteira para coleta de dados e de informações pessoais, sendo a internet o seu principal suporte (SOLOVE, 2004, p. 22).

A comunicação no mundo moderno é cada vez mais global, as distâncias foram elipsadas pela proliferação de redes de comunicação eletrônica, podendo interagir uns com os outros, mesmo em diferentes partes do mundo (THOMPSON, 2011, p. 22).

Nossos dados de saúde estão disseminados em toda parte, quer na internet ou fora dela. Tratam-se de registros médicos, cadastros em farmácias, buscas em sites e histórico de navegação. Reitera-se, que não há aqui a tentativa de promover a demonização da tecnologia, mas, de chamar a atenção ao risco ao uso indevido desse tipo de dado pessoal.

Indiscutível, que a informação de saúde organizada, atualizada e acessível é essencial à promoção da saúde pública. O problema surge quando não sabemos que nossas informações estão sendo coletadas, quando não damos consentimento para seu uso ou quando não cogitamos sobre o modo em que foram coletadas nem a especificidade para que serão utilizadas. Nesse sentido, uma farmácia, por exemplo, pode criar um banco de dados a partir das informações a respeito dos hábitos de um determinado cliente. Tais dados podem servir para traçar o perfil de saúde desse consumidor, fato que evidentemente foge ao seu controle. Esse banco de dados teria um conteúdo extremamente rico e, que sem dúvida, interessaria a um rol infinito de empresas.

Os dados de saúde são considerados dados sensíveis, e podem, por isso causar discriminação, fato este, que justifica por si só a existência de uma regulação específica.

2.1 E-SAÚDE E O MERCADO: UM VIÉS ECONÔMICO DA INFORMAÇÃO

O uso de tecnologias de informação e comunicação para mediar a atenção à saúde é denominado de e-Saúde (e-Health). Observa-se que o campo da e-Saúde está diretamente relacionado às políticas de informação, informática e comunicação em saúde no Brasil e no mundo. Nesse sentido, tal afirmação é importante num contexto em que se constata a inseparabilidade cada vez maior entre informação e as tecnologias que lhe dão suporte (MORAES e VASCONCELLOS, 2005).

O e-saúde pode ser definido como a aplicação das tecnologias de informação e comunicação no setor de saúde, isto é, e-Saúde representa o contexto da prática de atenção à saúde facilitada e aperfeiçoada pelo uso das tecnologias de informação e comunicação na organização, gestão e agilização dos processos de atendimento ao paciente, no compartilhamento de informações, na garantia de maior qualidade e segurança das decisões clínicas, no acompanhamento de pacientes, em políticas de saúde pública, na compreensão dos fatores determinantes do bem-estar do cidadão, na detecção e no controle de epidemias, entre tantas outras possibilidades (VIEIRA, 2014, p. 34).

Hoje, o uso de tecnologias de informação integradas e a facilidade de acesso das informações produzidas, remodelaram radicalmente o mundo. Considerando a revolução da tecnologia da informação, destaca-se que esse fenômeno foi essencial para a implementação de uma reestruturação do sistema capitalista da década de 1980. Nesse processo, o desenvolvimento e as manifestações dessa revolução tecnológica foram esculpidos pelas lógicas e interesses do capitalismo avançado (CASTELLS, 2005, p.50).

Assim, a informação, através da potencialidade de difusão do computador, transformou-se em mercadoria. A organização produtiva transforma-se de unidade de tratamento de materiais em unidade de tratamento de informações e, essa informação, para poder ser valorada e valorizada, é então submetida a tratamentos sofisticados, pode ser guardada, manipulada como um objeto, cedida, ou até mesmo subtraída de forma ilícita (PAESANI, 2015, p.10).

A informação costuma ser referida como a “matéria-prima” de novos processos econômicos e sociais desencadeados na sociedade da informação. A informação pessoal, especificamente, desponta como uma verdadeira *commodity* em torno da qual surgem novos modelos de negócio que, de uma forma ou de outra, procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias da informação. Neste cenário, é mais do que natural que a informação assuma grande relevância, tanto como um bem jurídico ou econômico.

A sociedade da informação gera poder, isto é, a informação devidamente tratada gera conhecimento, passando a ostentar um aspecto econômico. Nesse sentido, uma das razões para se afirmar que vivemos numa sociedade da

informação é que a produção e comercialização de informações contribui de maneira considerável para as economias mais desenvolvidas (BURKE, 2003, p. 136).

Considerando o potencial mercadológico da informação, não perfaz mera coincidência a aproximação, por exemplo, entre o Facebook e os hospitais dos EUA. Em 2015, o Facebook implantou o Facebook Health, numa tentativa de aproximação com a gigante indústria farmacêutica. Em meados de 2017, aconteceu o Facebook Health Summit, tratou-se de um evento restrito e curiosamente pouco noticiado, direcionado aos profissionais de marketing das indústrias de medicamentos.

E o Facebook não é o único em busca por espaço na área da saúde. O Google já havia tentado uma iniciativa na área, criou uma plataforma denominada Google Health, onde os usuários poderiam armazenar todos os seus registros médicos, mas que acabou sendo encerrada em 2011 devido à baixa adesão.

Nesse sentido, destaca-se o fato de que o grupo Alphabet, conglomerado do qual o Google é subsidiário, mantém atuação em diversificadas frentes na área da saúde. Por exemplo, a Verily, que de acordo com informações disponíveis em seu site, dedica-se a criação de ferramentas para coletar e organizar dados de saúde. A Verily já fez parcerias para pesquisas com a farmacêutica Sanofi. No ano de 2017, a Verily iniciou um projeto ambicioso, o objetivo era de monitorar a saúde de 10 mil pessoas durante quatro anos.

Sem dúvida que o e-health trata-se de um mercado gigantesco e as possibilidades econômicas de monetizar os dados de saúde são também exponencialmente grandes. Nesse sentido, vale destacar o artigo intitulado Big data poderia ser o futuro da farmácia?, publicado no Pharmaceutical Journal. Em tese, todas as unidades de saúde que coletam dados de consumidores, potencialmente podem se tornam empresas de análise de dados, cujo produto de venda extrapolaria a mera comercialização de medicamentos e serviços. A possibilidade de comercializar dados de saúde, a partir da padronização de comportamentos e tratamentos transformaria hospitais e farmácias em unidades de big data.

3 O PROBLEMA DA PROTEÇÃO DA PRIVACIDADE DAS INFORMAÇÕES EM SAÚDE

A contextualização do advento da internet criou inúmeros desafios jurídicos, a fim de assegurar a efetiva proteção do direito fundamental à privacidade.

A internet, com o desenvolvimento das tecnologias de informação, entregou inúmeros benefícios à sociedade como a facilidade e a rapidez nas comunicações. Ao mesmo tempo, verificou-se que o progresso científico ensejou o surgimento de novas formas de violação da privacidade alheia. Nesse sentido, a própria internet é um ambiente propício à violação do direito à privacidade, na medida que, em sua grande maioria, os usuários ignoram os meios pelos quais seus dados pessoais são coletados e utilizados ao navegarem, despretensiosamente pela rede (MAGRANI *et al*., 2012, p. 51).

Nesse contexto de sociedade da informação, tanto a noção de privacidade quanto da sua proteção evoluiu. Abandonou-se a visão clássica centralizada no direito de estar só, de cunho individualista e preocupado em estabelecer um limite à intromissão do Estado na vida das pessoas. A concepção atual de privacidade está relacionada à necessidade de estabelecer um maior controle na utilização das informações pessoais (MAGRANI *et al*., 2012, p. 51-52).

Assim, o direito à privacidade assume características importantes em prol da proteção dos dados pessoais, permitindo controlar as inúmeras possibilidades de seu tratamento (coleta, armazenamento e utilização). De fato, tal controle serve para resguardar os titulares dos dados e a sociedade onde estão inseridos (MAGRANI et al., 2012, p. 52).

A Constituição Federal de 1988, em seu artigo 5°, inciso X, destaca a proteção constitucional a vida privada. O direito à intimidade refere-se à proteção da esfera privada ou íntima de uma pessoa, devendo esta, ser protegida contra ingerências externas, alheias e não requisitadas (BRASIL, 1988).

Embora o ordenamento jurídico brasileiro contemple a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental, uma análise dos instrumentos disponíveis revela a existência de uma proteção fracionada, direcionada a campos específicos em detrimento de uma estratégia integral de proteção de dados pessoais (DONEDA, 2006, p.16-17).

Nesse sentido, a proteção à saúde enquanto direito fundamental garantido constitucionalmente, reforça a interdependência e a mútua conformação de todos os direitos humanos e fundamentais. Evidentemente, no caso do direito à saúde, as informações geradas devem garantir à privacidade, tendo em vista a complexidade e o caráter sensível e pessoal estabelecidos.

Pode-se afirmar que o conceito clássico de intimidade é anacrônico. Reitera-se ainda, que o conceito habitual de privacidade está superado, isto é, se, tradicionalmente, o direito à privacidade vinculava-se ao direito de ser deixado só, contemporaneamente pode-se afirmar que a privacidade evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis, de seu controle pelo titular e de respeito à liberdade das escolhas pessoais de caráter existencial (LEWICKI, 2003, p. 09).

Ainda, vale destacar que as discussões teóricas e as experiências complexas dos últimos anos, foram determinantes para modernizar o conceito de privacidade. Considera-se que a tecnologia da informação foi essencial para a dinamização desse conceito, de modo que o conjunto das situações hoje ligadas à proteção da vida privada representa um conglomerado de interesses diversos, que acaba por configurar inúmeras e variáveis faces de um conceito em ampliação permanente (LEWICKI, 2003, p. 31).

Assim, a definição de privacidade enquanto direito a ser deixado só perdeu seu valor genérico. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. A privacidade pode ser definida mais precisamente como direito de manter o controle sobre as próprias informações (RODOTÁ, 2008, p. 92).

Sem dúvida, a utilização de novas tecnologias amplia as possibilidades de coleta, tratamento e circulação de informação, confrontando o interesse individual da proteção de informações frente aos interesses de entidades, públicas ou privadas, na eficiência das suas atividades (GONÇALVES, 2003, p. 82).

A informatização de dados amplia o grau de risco para o indivíduo, uma vez que essa interconexão de base de dados possibilita a reunião de informações diversas, as quais poderão ser utilizadas de forma abusiva, com intuitos repressivos ou restritivos da liberdade dos cidadãos, com fins discriminatórios ou de mero enriquecimento (GONÇALVES, 2003, p. 82).

Considerando o desenvolvimento das novas tecnologias e a evolução científica, o acesso e a divulgação dos dados sensíveis tornaram-se de fácil divulgação, o que pode potencializar a perpetração de danos. Com efeito, a tutela da privacidade passa a ser vista como o direito de ter controle sobre os dados pessoais, a fim de impedir sua circulação indesejada. Nessa seara, a privacidade passa a ser

considerada o direito de manter o controle sobre suas próprias informações e de determinar a construção de sua esfera particular.

3.1 DESAFIO À PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NO ÂMBITO DA SOCIEDADE DE INFORMAÇÃO E A NECESSIDADE DE UM MARCO REGULATÓRIO DO TRATAMENTO DE DADOS EM SAÚDE

No mercado de consumo, a todo instante surgem produtos e serviços inovadores, muitos dos quais, de alguma forma relacionados a internet. O advento da internet acabou alterando as relações interpessoais, haja vista que o espaço virtual não possui fronteiras. Computadores, celulares, tablets, entre outros tantos instrumentos eletrônicos, fazem parte desse ambiente e influenciam os mais variados campos, dentre eles o Direito, que se depara com novos desafios a serem enfrentados (JÚNIOR, 2015, p. 68-70).

Incontroverso associar a área da saúde como um dos setores que mais se valem de dados pessoais para oferecer seus serviços. Quando falamos em dados ou informações pessoais, referimo-nos a qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, como o seu nome, CPF ou número de identidade. Dentre os dados pessoais, uma subcategoria especial é a dos dados sensíveis, assim compreendidos aqueles tipos de informação que se conhecidos e processados podem ter utilização potencialmente discriminatória ou particularmente lesiva, apresentando maiores riscos que a média, para o indivíduo e até mesmo para a coletividade.

De fato, os tipos de dados pessoais utilizados nesse contexto são conceituados como dados sensíveis, por tratarem de informações que podem revelar traços íntimos do indivíduo.

O tratamento dispensado aos dados sensíveis de saúde, a depender do cenário pode sujeitar o indivíduo a práticas discriminatórias, por isso a importância de garantir seu uso adequado e sigiloso. Considerando tais aspectos, fica evidente que a violação de dados sensíveis é muito mais prejudicial para a pessoa em causa, podendo gerar danos mais intensos à sua personalidade (DONEDA, 2006, p. 163).

O avanço tecnológico trouxe consigo a possibilidade de registro e tratamento de informações em grandes quantidades, concomitantemente, trouxe desafios relacionados a difusão indevida de dados pessoais (MAGRANI *et al*., 2012, p. 53).

A ausência de uma política de administração desses dados permite que a sua manipulação ocorra de modo descuidado, o que facilita a sua difusão pública, acidental ou mesmo intencional (MAGRANI *et al.*, 2012, p. 53).

Nesse contexto, reitera-se a preocupação acerca da venda de dados, que têm se tornado uma prática comum, inclusive no Brasil, e que acaba criando uma sensação de desconfiança por parte do consumidor em relação à difusão de suas informações pessoais.

Ainda, outra preocupação que envolve a transferência de dados pessoais, é aquela caracterizada pela coleta sem consentimento de seu titular ou cuja utilização dos dados esteja vinculada a fins distintos dos que legitimaram sua coleta. Nesse sentido, podemos destacar o viés negativo acerca da chamada publicidade comportamental, que pode ser considerada como invasão de privacidade, na medida em que se baseia no levantamento de informações de correspondência pessoal, permitindo monitorar hábitos e interesses de determinado consumidor (MAGRANI *et al*., 2012, p. 55).

É evidente que a publicidade comportamental corresponde a um fenômeno irreversível, incorporado às relações de consumo e à prática publicitária, sendo lícita, nos termos da legislação brasileira atualmente posta, desde que respeitados os requisitos para coleta, uso e tratamento de dados pessoais, em especial o quanto disposto no Marco Civil, bem como as regras constantes da legislação consumerista acerca da identificação publicitária e da vedação à publicidade abusiva.

De fato, tais preocupações são relevantes no contexto de saúde, haja vista o potencial de identificar um consumidor a partir da expansão e aprimoramento de bases nominais e de integração entre bancos de dados, podendo promover informações de percurso desse consumidor.

Nessa seara é de suma importância a existência de regras claras sobre o tratamento dos dados pessoais, estabelecendo limites precisos que garantam a privacidade desses consumidores.

Internacionalmente, a preocupação com a proteção da privacidade e confidencialidade de dados de saúde manifestou-se de forma exponencial a partir da década de 1970 e deu origem a diversas declarações proclamadoras de direitos dos usuários de serviços de saúde, como a Declaração sobre os Direitos dos Pacientes (1981) (ASSEMBLÉIA GERAL DA ASSOCIAÇÃO MÉDICA MUNDIAL, 1981).

Mesmo com todo o aparato legal que o Brasil possui, até meados de 2018, não dispúnhamos de uma lei geral para proteção dos dados pessoais. Entretanto, o setor saúde já contava com regulamentações esparsas pertinentes ao tema, dentre as quais destacam-se:

1) Lei 8.078/90 (Código de Defesa do Consumidor), regulamenta bancos de dados consumeristas, considerando que existe uma relação de consumo entre pacientes e prestadores de serviços de saúde (BRASIL, 1990);
2) Portaria nº 5/2002 da SDE/MJ, que interpretou como abusivas cláusulas em contratos de consumo que autorizam o envio de dados pessoais sem o consentimento prévio dos consumidores (BRASIL, 2002);
3) Resolução CFM Nº 1.821/07, dispõe sobre o prontuário eletrônico de dados médicos, considerados sensíveis (BRASIL, 2007);
4) Resolução ANVISA da Diretoria Colegiada nº 44/2009, dispõe sobre Boas Práticas Farmacêuticas para prestação de serviços farmacêuticos, inclusive o uso de dados pessoais (ANVISA, 2009);
5) Lei 12.965/2014, conhecida como Marco Civil da Internet, responsável pelo estabelecimento de direitos, limites e obrigações de usuários e serviços de Internet, inclusive plataformas e aplicativos de saúde. Destaca-se que essa lei trata especificamente de questões ligadas ao uso de dados pessoais, tais como a necessidade de consentimento prévio, livre, específico e informado dos usuários/pacientes (BRASIL, 2014a);
6) Lei nº 13.021/2014, que dispõe sobre o exercício e a fiscalização das atividades farmacêuticas e trata do preenchimento de fichas farmacoterapêuticas com dados pessoais normais, que podem ser considerados dados consumeristas, e dados pessoais sensíveis, como os que revelam alguma característica fisiológica de pacientes (BRASIL, 2014b);
7) Decreto 8.771/16, que regulamentou aspectos do Marco Civil da Internet, inclusive sobre o uso de dados pessoais, estabelecendo limites, como a obrigação de se coletar dados somente para uma finalidade determinada, apenas na quantidade e nos tipos necessários para atingir esse propósito, devendo estes serem cancelados ao atingir a finalidade, caso não haja outra base legal para mantê-las (BRASIL, 2016).

Em 2011 foi finalizado o debate público da proposta de um marco normativo para a proteção da privacidade e dos dados pessoais. O anteprojeto de lei foi fruto

de uma parceria do Ministério da Justiça com o Observatório Brasileiro de Políticas Digitais, tendo como objetivo precípuo assegurar ao cidadão o controle e a titularidade sobre as suas próprias informações pessoais, o que concretizaria o direito constitucional à privacidade (MAGRANI *et al.*, 2012, p. 54).

Cabe destacar que esse anteprojeto foi de suma importância para o desenvolvimento das políticas digitais no país, permitindo viabilizar um tratamento adequado aos dados sensíveis.

Sem dúvida, a forma de limitar a coleta indiscriminada de dados pressupõem a existência de legislações que protejam os dados pessoais. Assim, quanto mais a legislação resguardar a privacidade das pessoas, menor é o espaço que o mercado encontra para a comercialização de dados.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) foi sancionada em 2018 e entrará em vigor em 2020. A LGPD brasileira (Lei n° 13.709/18) seguindo as diretrizes do Regulamento Geral de Proteção de Dados (RGPD) aprovado pela União Europeia, com as alterações trazidas pela Lei n° 13.853/19, estipula regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, acarretando uma maior proteção para a pessoa física, bem como impondo penalidades jurídicas face o não cumprimento das diretrizes estabelecidas (BRASIL, 2018; BRASIL, 2019).

Nesse sentido, vale destacar que a LGPD propôs o estabelecimento de uma série de regras para proteção de informações individuais, alcançando tanto atores públicos quanto privados, sendo que concomitantemente introduz medidas preventivas e repressivas, no intuito de fomentar as boas práticas na gestão de base de dados pessoais, buscando transparência (MONTEIRO e OTTONI, 2019).

O alcance desse marco digital refletirá em todos os modelos de negócio que operam com dados, sejam eles físicos ou virtuais, fazendo-se necessário uma mudança significativa em diversos setores organizacionais, impactando positivamente diversos aspectos de governança de dados. Nesse sentido, importa destacar que a conduta de compartilhamento de dados de saúde, para obter vantagem econômica, passa a ser proibida, exceto se o titular dos dados permitir expressamente.

4 A ECONOMIA DE DADOS SENSÍVEIS: BIG DATA E A REVOLUÇÃO NA ÁREA DA SAÚDE

A área de saúde tem registrado uma infinidade de dados oriundos das mais diversas origens (registros médicos, apps que monitoram atividades de pacientes, alertas em tempo real, armazenamento eletrônico de resultados de exames e dados de pacientes, prontuários eletrônicos) e o big data é o termo que representa algumas ferramentas para apoio a gestão de grande volume de dados, sejam eles estruturados ou não, e que impactam os negócios no dia a dia.

Considerando que no contexto atual, vive-se cada vez mais conectado à internet, contribuímos com uma enorme geração de dados que se dispersam rapidamente por toda a rede. Mais importante do que conceituar big data é saber o que as empresas fazem com esses dados.

No contexto de saúde o big data é um dos campos onde o impacto da pesquisa, análise e tratamento de dados é maior, isto porque engloba aspectos relacionados a prevenção, diagnóstico e investigação clínica e medicamentosa de doenças. Por isso cresce o interesse de inúmeras instituições em aderir cada vez mais às plataformas analíticas que permitem gerenciar custos operacionais, dados clínicos, exames, tratamentos e medicamentos.

Simplesmente possuir um banco de dados não significa que esses dados tenham utilidade. O principal nesse contexto é possuir inteligência para extrair informações significativas dos dados armazenados. Assim, na indústria farmacêutica, por exemplo, responsável por gerar enormes quantidades de dados a análise dessas informações representa um importante desafio e dispor de sistemas eficientes de gerenciamento torna-se indispensável.

4.1 A FUNCIONALIDADE DOS BANCOS DE DADOS E CADASTROS DE CONSUMO EM SAÚDE E O ABUSO DOS FORNECEDORES AO COMERCIALIZAR INFORMAÇÕES E DADOS SENSÍVEIS DE SAÚDE

Os dados e informações de consumo em saúde são conteúdos de grande valia para o mercado moderno e destacam-se enquanto objetos de desejo da indústria médico-farmacêutica. Esses dados enriquecem o banco de dados e cadastros de consumo trazendo informações peculiares e com utilidades que podem impactar no contexto médico futuro.

De fato, esse tipo de mercado, já tem sido alvo de preocupação do Instituto Brasileiro de Defesa do Consumidor a certo tempo, considerando que o grau de proteção dos brasileiros, em termos legais, ainda é muito baixo.

Dado é uma pré-informação, ou seja, uma informação em estado potencial. Já as informações extrapolam a representação contida no dado, chegando ao limiar da cognição pessoal (DONEDA, 2006, p. 152-153).

Os bancos de dados são um conjunto de dados armazenados em computador, de maneira estruturada e organizada, no intuito de tornar mais eficaz determinada atividade exercida por seu usuário. Importa destacar que esses bancos de dados, apresentam os mais variados objetivos, que vão desde a composição de material com finalidades estatísticas até a coleta de informações úteis a determinado segmento empresarial (GENTILI, 1999, p.70).

Nesse sentido, os bancos de dados de consumo são administrados por quem deseja coletar, armazenar processar e, se assim lhes convier, fornecer informações a terceiros sobre determinado grupo de consumidores (GENTILI, 1999, p. 71-73).

Na grande maioria das vezes, a quantidade de dados e informações que são colhidos e compartilhados, deflagra o potencial lesivo e os perigos aos quais os consumidores estão expostos, especialmente no âmbito de sua privacidade.

Posto que a grande quantidade de tráfego de dados sensíveis, é preocupante que a segurança da informação ainda não esteja estabelecida no país, enquanto política pública própria, que repercute jurídica e economicamente (MENDES, 2013, p. 253-254).

De fato, a importância de uma informação apresenta relação com o vínculo objetivo que ela possui com o indivíduo. Assim, se puder revelar suas características exclusivas, identificando a própria pessoa denominam-se dados sensíveis (DONEDA, 2006, p. 156).

Importa destacar que a coleta, armazenamento e divulgação de características como raça, religião, opção sexual ou política, compõem o rol de condutas que podem afetar os dados sensíveis, uma vez que seu uso indevido pode resultar em práticas discriminatórias e potencialmente lesivas, individual ou coletivamente (DONEDA, 2006, p. 160-163).

Assevera-se que o dado em si não é perigoso ou discriminatório, sendo que muitas vezes é essencial ao desenvolvimento, especialmente se considerarmos a área médica. O cuidado que se deve ter é quanto a finalidade com a qual esse dado

será utilizado, cabendo a legislação impor os limites de modo que efetivamente diminua a potencialidade lesiva de sua utilização (DONEDA, 2006, p. 161-162).

Reitera-se que embora o mercado de dados de saúde seja obscuro, não é secreto. As *data brokers*, por exemplo, são empresas especializadas em captar, compartilhar, analisar e comercializar grandes volumes de informações obtidas a partir do rastreamento de dados. (SAMPAIO, 2017, p. 29).

As *data brokers* são empresas que lucram através da extração de dados pessoais coletados através de interações de atividades humanas tecnicamente mediadas por máquinas criando uma rede ilimitada de conhecimento. Esse tipo de vigilância corporativa, com capacidade aparentemente infinita, atua especialmente na coleta e tratamento de dados para construir categorizações que funcionam como um modelo de predição do futuro (SAMPAIO, 2017, p. 31).

Assim, os problemas do uso de informações de risco, extrapolam a mera coleta dos dados privados que fornecemos nos diversos serviços e estabelecimentos de saúde, haja vista, que no mercado existem empresas que investem no acesso e na coleta de informações que estão públicas na internet, cruzando essas informações e estruturando um banco de dados comercializável e extremamente rentáveis, a partir de uma segmentação de perfis comportamentais e listas de clientes.

5 CONSIDERAÇÕES FINAIS

Indiscutível que a sociedade da informação reordenou a maneira de viver, interligando os continentes e criando uma cultura digital. Frente a revolução da informática e das telecomunicações, o direito à privacidade ganha destaque na sociedade digital por ser o núcleo das mídias e redes sociais, em que a vida particular das pessoas é exposta constantemente.

A realidade de descompasso entre o direito e o avanço das tecnologias de informação reside no fato de que estas tendem a transmudar-se constantemente, enquanto aquele, tem um caráter de relativa permanência. A monetização de dados pessoais é uma realidade e enquanto modelo de negócio dificilmente perderá espaço no panorama da sociedade informacional.

Essa questão requer um trabalho árduo para os operados do direito a fim de encontrarem formas de compatibilizar o respeito à presunção geral ao qual se

constitui o direito à vida privada ou privacidade com os avanços das tecnologias da informação e da comunicação.

Partindo da premissa de um mundo globalizado e sem fronteiras geográficas é de suma importância que a sociedade, conjuntamente com o poder público, possa organizar e captar os benefícios disponíveis da era tecnológica e revertê-los de modo seguro para a nossa vida.

Nesse contexto, é necessária a regulamentação a respeito dos limites em relação a coleta e armazenamento de dados pessoais a fim de tornar efetiva essa proteção.

A proteção da privacidade dos dados pessoais é garantia subjetiva dos indivíduos, enquanto faculdade do cidadão em obstar a intromissão na vida privada e intimidade e de autodeterminação de suas informações, bem como garantia objetiva, enquanto valores basilares do ordenamento jurídico, como condição a atuação dos poderes públicos constituídos.

Portanto, exige-se do Estado a organização e procedimento para tutelar a proteção de dados pessoais e instituição de uma entidade competente para a concretização deste direito fundamental.

6 REFERÊNCIAS

ANVISA. **RDC n°. 44, de 17 de agosto de 2009**. Dispõe sobre Boas Práticas Farmacêuticas para o controle sanitário do funcionamento, da dispensação e da comercialização de produtos e da prestação de serviços farmacêuticos em farmácias e drogarias e dá outras providências. Disponível em: file:///C:/Users/Fernanda/Downloads/180809_rdc_44.pdf. Acesso em: jul. 2018.

ASSEMBLÉIA GERAL DA ASSOCIAÇÃO MÉDICA MUNDIAL. **Declaração de Lisboa: sobre os direitos do paciente.** 1981. Disponível em: http://www.dhnet.org.br/. Acesso em: jul. 2018.

BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: jun. 2018.

BRASIL. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: jul. 2018a.

BRASIL. **Portaria nº. 5, de 27 de agosto de 2002.** Complementa o elenco de cláusulas abusivas constante no Art. 51 da Lei n° 8.078, de 11 de setembro de 1990. Disponível em: http://www.camara.gov.br/sileg/integras/127355.pdf. Acesso em: jul. 2018.

BRASIL. **Resolução CFM n°. 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. Disponível http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.pdf. Acesso em: jul. 2018.

BRASIL. **Lei n° 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: jul. 2018b.

BRASIL. **Lei n° 13.021, de 08 de agosto de 2014**. Dispõe sobre o exercício e a fiscalização das atividades farmacêuticas. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L13021.htm. Acesso em: jul. 2018.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: nov. 2019.

BRASIL. **Lei n° 13.853, de 08 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: nov. 2019.

BRASIL. **Decreto n° 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: jul. 2018.

BURKE, Peter. **Uma História Social do Conhecimento: de Gutenberg a Diderot.** Rio de Janeiro: Jorge Zahar, 2003, p.136.

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

_____. **A sociedade em rede**. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

_____. **Communication Power.** New York: Oxford University Press. 2009.

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

GENTILI, José Carlos. **Os bancos de dados na sociedade de consumo e o código de defesa do consumidor: a questão da responsabilidade jurídica por danos morais.** Brasília: Tecprint, 1999.

GONÇALVES, Maria Eduarda. **Direito da Informação: novos direitos e formas de regulação na sociedade da informação.** Coimbra: Almedina, 2003.

JÚNIOR, Geraldo Frazão de Aquino. **As vicissitudes do contrato no comércio eletrônico globalizado.** Revista de Direito do Consumidor, São Paulo: Revista dos Tribunais, v. 102, p. 68-70, nov.-dez./2015.

LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: 34, 1999.

_____. **As tecnologias da inteligência: o futuro do pensamento na era da informátic***a* (2ª ed.- Costa, C. I. Trad.). Rio de Janeiro: Ed. 34. 2010.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar. 2003.

MAGRANI, Bruno; SOUZA, Carlos Affonso Pereira de; DONEDA, Danilo; MAGRANI, Eduardo; CARLONI, Giovanna; KAMEDA, Koichi; MONCAU, Luiz Fernando Marrey; MACIEL, Marília; MONTEIRO, Marília; FRANCISCO, Pedro Augusto; LEMOS, Ronaldo e BRITTO Walter. **Relatório de Políticas Digitais**. 2012. Disponível em: http://www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf. Acesso em: mai. 2018.

MENDES, Laura Schertel. **Segurança da informação, proteção de dados pessoais e confiança**. Revista de Direito do Consumidor, São Paulo: Revista dos Tribunais, v. 90, p. 253, nov.-dez./2013.

MONTEIRO, Breno; OTTONI, Marcos. **A Regulamentação da LGPD e o setor de saúde.** Disponível em: http://cnsaude.org.br/artigo-a-regulamentacao-da-lgpd-e-o-setor-de-saude/. Acesso em: nov. 2019.

MORAES, Liara Hämmerli Sozzi de; VASCONCELLOS, Miguel Murat. **Política Nacional de Informação, Informática e Comunicação em Saúde: um pacto a ser construído.** Revista Saúde em Debate, v. 29, n. 69, p. 86–98, 2005.

PAESANI, Liliana Minardi. **Direito de informática**, 10ª ed., São Paulo: Atlas, 2015.

PEREZ-LUÑO. Antonio Enrique. **Los derechos humanos em la sociedade tecnológica**. Madrid: Editorial Universitas, 2012.

RAPÔSO, Cláudio Filipe Lima; LIMA, Haniel Melo de; OLIVEIRA JÚNIOR, Waldecy Ferreira de; SILVA, Paola Aragão Ferreira; BARROS, Elaine de Souza. **LGPD - Lei**

Geral de Proteção de Dados Pessoais em Tecnologia da Informação: Revisão sistemática. RACE - Revista de Administração, v.4, pg. 58-67, 2019. Disponível em: https://revistas.cesmac.edu.br/index.php/administracao/article/view/1035/802. Acesso em: nov. 2019.

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

SAMPAIO, Alice Castaldi. **Data brokers: um novo modelo de negócios baseado em vigilância de dados.** Campinas, SP: [s.n.], 2017. Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Estudos da Linguagem. Disponível em: http://repositorio.unicamp.br/handle/REPOSIP/322483. Acesso: mai. 2018.

SOLOVE, Daniel. **The Digital Person: technology and privacy in the information age.** New York: New York University Press, 2004.

THOMPSON, John B. **A mídia e a modernidade: uma teoria social da mídia**. 12ª ed. Rio de Janeiro: Vozes. 2011.

VIEIRA, Augusto Cesar Gadelha. **O projeto cartão nacional de saúde e a construção de e-saúde para o Brasil**. In: COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros – TIC Saúde 2013, coord. Coord. Alexandre F. Barbosa. São Paulo: CGI.br, 2014. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf. Acesso em: 30 mai. 2018.