DO DIREITO À PROTEÇÃO DE DADOS EM MATÉRIA DE SAÚDE NA SOCIEDADE DE INFORMAÇÃO

THE RIGHT TO THE PROTECTION OF HEALTH DATA IN THE INFORMATIONAL SOCIETY

Manuela Ithamar Lima*

Recebimento em 29 de maio de 2017.
Aprovação em 30 de junho de 2017.

Resumo: O presente artigo propõe o estudo do direito fundamental à proteção de dados em matéria de saúde na sociedade de informação, para tanto, analisa-se a definição de inovação e seu tratamento no ordenamento jurídico brasileiro, tratando a inovação tecnológica como fator determinante no surgimento da sociedade de informação. Posteriormente se perpassa pela evolução do direito à privacidade até o reconhecimento do direito fundamental autônomo à proteção de dados pessoais, definindo-se dados pessoais e concebendo os dados em matéria de saúde como uma espécie desses dados, qual seja, a categoria de dados sensíveis. Finalmente, desagua-se na análise da proteção de dados em matéria de saúde na sociedade de informação, evidenciando as possibilidades e limites das novas tecnologias inseridas no sistema de prestação de serviços de saúde, tendo como plano de fundo o cenário jurídico brasileiro.
Palavras-chave: Direito à saúde. Proteção de dados pessoais. Inovação Tecnológica. Sociedade de Informação.

Abstract: The present article proposes a study of the fundamental right to data protection on matter of health in the informational society, and for that, it analyses the definition of innovation and its treatment in Brazilian juridical ordinance, discussing the technologic innovation as a determining factor in the appearing of informational society. After, it passes by the evolution of right to privacy until the recognition of the autonomous fundamental right to personal data protection, in which it defines personal data and conceives the data on matter of health as a species of these data, whichever, a category of sensible data. Finally, it issues into the analysis of data protection on matter of health in informational society, evidencing the possibilities and limits of new technologies input at the healthcare system, as well as having as background the Brazilian juridical scenario.
Keywords: Right to Health. Personal Data Protection. Technologic Innovation. Informational Society.

INTRODUÇÃO

A sociedade de informação, também denominada de sociedade em rede, consiste em uma estrutura social baseada e operada por tecnologias de comunicação que geram, processam e distribuem informações acumuladas nas redes digitais de computadores.

* Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul PUCRS, Porto Alegre-RS, Brasil. Graduada em Direito pela Unidade de Ensino Superior Dom Bosco (UNDB). Bolsista vinculada à CAPES. Advogada. Email: manuela.ithamar@gmail.com

Essa nova forma de organização social influencia e modifica significativamente as relações sociais, de modo que se por um lado ela viabiliza a implementação mais efetiva de políticas públicas promotoras de direitos fundamentais, por outro, possibilita, também a criação e interconexão de banco de dados pessoais e a disseminação irrestrita de informações coletadas por todos os indivíduos, sendo, por isso, intitulada da sociedade do risco, por vezes ameaçadora e violadora de direitos primordiais.

Nesta senda, o presente estudo destina-se a analisar a proteção de dados pessoais em matéria de saúde na sociedade de informação, expondo que ao passo que a inserção das novas tecnologias na prestação dos serviços de saúde traz incontestavelmente benefícios na garantia e promoção do direito à saúde, propiciam, por outro lado, uma vulnerabilidade na proteção de dados pessoais.

Para tanto, inicialmente perpassa-se pela definição de inovação, partindo do pressuposto que essa é fator determinante no progresso tecnológico da sociedade, expondo-se o tratamento jurídico da inovação no cenário brasileiro, bem como a associando ao surgimento de uma nova organização social, qual seja a sociedade de informação.

Posteriormente, traça-se uma linha evolutiva no que se refere o direito à privacidade até se chegar ao direito à proteção de dados pessoais, enaltecendo que a sociedade de informação exigiu novos contornos do direito à privacidade, fazendo emergir, para além de um direito à privacidade, o direito fundamental autônomo à proteção de dados pessoais. Passa-se pela própria definição de dados pessoais, ressaltando-se a existência da categoria de dados pessoais denominada de dados sensíveis, focando-se nos dados referentes à saúde como espécie de dados sensíveis.

Destarte, com a inovação tecnológica e toda a reestruturação na organização social que ela acarretou fez-se surgir a donominada saúde eletrônica, a qual consiste na inserção das novas tecnologias na prestação dos serviços de saúde, algo que como se demonstrará não passou despercebido no ordenamento jurídico brasileiro.

Nada obstante, constata-se que a despeito dos benefícios trazidos pelas novas tecnologias em sede de promoção do direito à saúde, essas sob outra monta dificultam a concretização do direito fundamental à proteção dos dados sensíveis da saúde, sendo destacado por todo percurso discurso sobre a necessidade de se fixar mecanimos que possibilitem o não esvaziamento do direito fundamental à proteção de dados pessoais face a nova saúde eletrônica.

1 A INOVAÇÃO TECNOLÓGICA E O SURGIMENTO DA SOCIEDADE DE INFORMAÇÃO

A inovação em sentido *lato* consubstancia-se no desenvolvimento de novas formas de produzir, aplicar e distribuir o conhecimento, dito de outro modo, o conhecimento não é só fator, como também produto do processo de inovação (MACIEL, 2005, p. 34).

Destarte, observa-se que a inovação poderá ocorrer em diversos campos do conhecimento, não por outra razão, chega-se a várias tipologias de inovação, tais como inovação jurídica, inovação econômica, inovação legislativa, e especificadamente a tratada no presente artigo, a inovação tecnológica. Nesta senda, vislumbra-se que a inovação tecnológica consiste na produção, aplicação e distribuição de novas tecnologias, tendo como efeito precípuo a penetração de tais tecnologias nas diversas atividades praticadas na Sociedade, influenciando de modo demasiado os setores econômicos e sociais (RODOTÁ, 2008, p. 41-41).

A inovação tecnológica na contemporaneidade não é concebida apenas para atingir uma finalidade específica dentro do contexto social, não possuindo a tecnologia apenas um sentido utilitarista e instrumental, ao contrário, há um perfil dinâmico da tecnologia, a qual tem por escopo o progresso da Sociedade como um todo (DONEDA, 2006, p. 42). Isso porque tem-se que a inovação tecnológica é um dos principais mecanismos para o desenvolvimento social, econômico e cultural de uma população, já que essa eleva o patamar dos conhecimentos gerados e utilizados pelos indivíduos, oferecendo um constante estímulo de aprendizagem e mudança (WERTHEIN, 2000, p. 75).

No entanto, importa dispor que esse processo dinâmico de inovação acarreta um determinismo de mão dupla, visto que, se por um lado é certo que a inovação tecnológica acaba por determinar os novos moldes das relações sociais, por outro, é inconteste que a Sociedade é determinante da tecnologia, pois suas necessidades que dão azo para as inovações tecnológicas (CASTELLS, 2005, p. 17).

Nesta senda, no cenário jurídico brasileiro a importância da inovação para o progresso ganhou contornos tais que ocasionou a inserção da inovação no texto Constitucional como uma política pública a ser promovida pelo Estado. Com a Emenda Constitucional nº 85/2015 reservou-se um capítulo específico à Ciência, Tecnologia e Inovação na Constituição Federal, no qual consta que o Estado "promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação, tendo em vista o bem público e o progresso da ciência, tecnologia e inovação" (artigo 218, §1º).

Frisa-se que a inovação é primeiramente definida em termos claros na Lei nº 10.973/2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo. Na legislação, ela é considerada como sendo a "introdução de novidade ou aperfeiçoamento no ambiente produtivo ou social, que resulte em novos produtos, processos ou serviços".

No ano de 2016, ocorre, então, a promulgação da Lei nº 13.243/2016, doravante chamada de Código Nacional de Ciência, Tecnologia e Inovação (CCTI). O novo texto legal amplia o conceito de inovação contido na Lei nº 10.973/2004, deixando de prevê-la como inserção devida em ambientes produtivos, e passando a considerá-la também como um incremento a ambientes sociais. Assim, no teor do CCTI, inovação é a "introdução de novidade ou aperfeiçoamento no ambiente produtivo e social", do que decorra a. "novos produtos, serviços ou processos", ou ainda, que b. "compreenda a agregação de novas funcionalidades ou características a produto, serviço ou processo já existente que possa resultar em melhorias e em efetivo ganho de qualidade ou desempenho" (artigo 2º, inciso IV).

Assim, resta clarividente a atenção e a conotação que a inovação possui nos dias atuais. Destarte, a inovação tecnológica fez surgir a designada "sociedade de informação", uma vez que tais inovações ensejaram uma transformação na organização social. A sociedade de informação, ou também denominada de sociedade em rede, consiste em uma estrutura social que é baseada e operada por tecnologias de comunicação e de informação, as quais por sua vez, são fundadas na microtecnologia e nas redes digitais de computadores, que geram, processam e distribuem informação do conhecimento acumulado nessas redes (CASTELLS, 2005, p. 17-20).

Ocorre que o surgimento da sociedade de informação faz-se constatar que se torna cada vez maior os riscos do progresso tecnológico, o qual se torna cada vez mais acelerado e ameaça valores e direitos fundamentais primordiais (RODOTÁ, 2008, p. 41-41). Não por outra razão, reconhece-se que essa "nova sociedade" é também uma sociedade dos riscos, tem-se que a modernização avançada é acompanhada irremediavelmente da produção social de riscos. Em outros termos, os problemas e conflitos da sociedade de informação surgem da produção, definição e do compartilhamento da responsabilidade dos riscos produzidos pela inovação tecnológica (BECK, 2013, p. 25-26).

A partir disso, é possível afirmar que a despeito do processo de inovação possuir aspectos positivos incontestáveis, esse também é dotado de efeitos negativos, tal como o seu efeito de desestabilizar o plano econômico e social (FERRY, 2015, p. 17), vez que, a inovação "vestida" apenas dos aspectos positivos flexibiliza e até abole valores até então

tradicionais e primordiais para o Estado Democrático de Direito, visto que esses são considerados arcaicos e inibidores do progresso tecnológico (FERRY, 2017, p. 61).

Nessa perspectiva, atenta-se que, partindo do pressuposto que os direitos fundamentais contêm uma dimensão objetiva, não se limitando à função precípua de serem direitos subjetivos de defesa do indivíduo em face do Estado, mas que, para além dessa função, eles constituem decisões valorativas de natureza objetiva da Constituição (SARLET, 2015, p. 149), um dos valores que estão sendo mitigados e flexibilizados pelo processo de inovação tecnológica são os que compõem a dimensão objetiva do direito fundamental à privacidade e à proteção de dados.

Veja-se que conforme preleciona Rodotá, a sociedade de informação, também definida por ele como sociedade dos serviços, possui ao menos duas consequências, quais sejam, quanto mais sofisticados tecnologicamente são os serviços, mais o indivíduo deixa nas mãos do fornecedor do serviço uma parcela relevante de informações pessoais, ao passo que quanto mais a rede desses serviços se alarga, crescem as probabilidades de interconexões entre os bancos de dados e a disseminação das informações coletadas (2008, p. 100).

É partindo dessas premissas que se conclui que a sociedade de informação exigiu uma redefinição do direito à privacidade, fazendo emergir o direito autônomo à proteção de dados pessoais, na medida em que se buscaram concepções de privacidade funcionais e adaptáveis ao novo contexto (CASTELLS, 2005, p. 17). Essa redefinição, e evolução do direito à privacidade, a qual ensejou o próprio surgimento de um direito fundamental autônomo de proteção de dados.

2 DO SURGIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Inicialmente, importa considerar que o direito à proteção de dados pessoais derivou de todo um processo evolutivo do direito à privacidade, o qual se faz necessário explanar. O marco fundador do direito à privacidade é atribuído aos americanos Samuel Warren e Louis Brandeis, os quais defenderam no artigo *The right to privacy*, publicado em 1890, a existência do direito à privacidade, o qual se perfazia no direito de ser deixado só, *the right to be let alone* (BRANDEIS; WARREN, 1890, p.193).

Realça-se que o direito à privacidade surge em razão da necessidade de se proteger a vida do ser humano não tendo por base apenas a proteção do direito à propriedade, mas passando a ter como alicerce também a inviolabilidade da personalidade. Há uma alteração de paradigma, tendo em vista que até então tinha-se por premissa que o direito à vida do

indivíduo estava resguardado e protegido no caso do seu patrimônio também estar, dado que esse iria propiciar condições de uma vida digna. Conquanto, passa-se a sopesar que uma vida digna estava ligada a outros fatores que não somente os patrimoniais (MIRANDA, 2016, p. 5).

Impende dispor que, antes de se argumentar por uma defesa do direito à privacidade, na jurisprudência norte-americana vislumbrava-se de modo gradativo o reconhecimento da proteção dos direitos da personalidade, recorrendo-se à violação do direito à propriedade, da confiança ou de uma obrigação de cunho contratual. Desta maneira, o direito à privacidade, construído pela doutrina e jurisprudência americanas, reportava-se a um direito geral de personalidade, o qual era mais amplo que o direito à reserva da intimidade privada, tendência essa que se repetiu na Europa, como se pode extrair de modo exemplificativo do cenário jurídico Alemão, que por interpretação conjunta do artigo 1º da Lei Fundamental Alemã, *Grundgestz*, que consagra a dignidade humana, com o artigo 2º, o qual contempla o direito ao livre desenvolvimento da personalidade, viriam a defender um direito geral de personalidade (CASTRO, 2005, p. 17-22).

No Brasil, foi apenas com a Constituição Federal de 1988 que o direito à privacidade foi previsto expressamente, articulando-se com outros direitos fundamentais, tais como a proteção da intimidade e também a inviolabilidade do domicílio. Tem-se que a intimidade e a privacidade são, em verdade, níveis do direito à vida privada, e foram expressamente referidas separadamente na Constituição Federal (SARLET, 2016, p. 442).

Em termos claros, o direito à privacidade é dotado de maior amplitude, contendo acontecimentos atinentes aos relacionamentos pessoais de um modo geral, como relações profissionais e comerciais que os indivíduos não gostariam que fossem expostas. Ao passo que o direito à intimidade relaciona-se com episódios ainda mais íntimos, fazendo referência a relações familiares e afetivas (BRANCO; MENDES, 2016, p. 280), é o próprio direito de se afastar por vontade própria da vida ou atividades em comum (RODOTÁ, 2008, p. 26). Desse espectro o ser humano detém exclusivo domínio, não havendo, em tese, interesse público capaz de justificar a pretensão informativa sobre os aspectos da sua vida íntima (MIRANDA, 2016, p. 5).

De qualquer sorte, tal distinção é difícil de sustentar, uma vez que as diversas esferas da vida privada, englobada a intimidade, são muito fluidas, e por vezes se confundem de modo que, salvo melhor juízo, a intimidade está abarcada no âmbito de proteção do direito à privacidade (SARLET, 2016, p. 444).

Por outro lado, a própria definição do âmbito de proteção do direito à privacidade é por si só difícil de ser delineada, ressaltando-se que até o momento não se logrou êxito em definir com precisão em que consiste o direito à privacidade, refutando-se de pronto qualquer catalogação prévia e fechada de situações que se enquadrem no âmbito de proteção do referido direito (SARLET; KEINERT, 2015, p. 121).

Por derradeiro, as situações que se inserem no âmbito de proteção do direito à privacidade são delimitadas caso a caso, levando-se em consideração o que para cada indivíduo é considerado incluso na sua esfera íntima e, portanto, não passível de divulgação ou interferências de terceiros.

Ocorre que com o advento da sociedade de informação e a disseminação e inserção das novas tecnologias no organismo social surge a dificuldade de delimitar quais os contornos da privacidade nesse novo conceito de sociedade, havendo quem sustente, inclusive, que a privacidade não se trasmuda mais como um direito fundamental, constituindo-se como um obstáculo à segurança e ao progresso científico (RODOTÁ, 2008, p.17). Sob outra perspectiva, as relações intersubjetivas perdem cada vez mais seu caráter de pessoalidade e proximidade, tornando-as demasiadamente publicizadas, obstaculizando a classificação dos aspectos que estão agrupados como sendo da vida privada daqueles que não o são (RODRIGUES; RUARO, 2010, p. 17).

Nesse cenário, o direito à privacidade criado no sentido de um direito de ser deixado só, se transmuda a um direito de controle por parte do sujeito, das informações que lhe digam respeito, ou seja, o direito à privacidade faculta ao seu titular o exame, fiscalização, suspensão e até a fazer cessar a circulação de informações suas (MIRANDA, 2016, p. 5).

À par disso, constrói-se, então, no direito alemão e espanhol, o que se denominou de direito à autodeterminação informativa, ganhando seus primeiros delineamentos na influente decisão do Tribunal Constitucional Federal da Alemanha, acerca da constitucionalidade da Lei do censo populacional, julgada em 1983 (SARLET, 2016, p. 444). Tal discussão é motivada pelo temor que se propagou na população em que fosse criado um Estado ultra informado, com acesso irrestrito aos dados dos cidadãos e os utilizasse não só para fins administrativos e estatísticos, mas também como mecanismo de controle social (RODRIGUES; RUARO, 2010, p. 191).

Por derradeiro, o Tribunal Constitucional Federal Alemão julgou improcedente a citada Lei do censo, tendo por fundamento o direito à autodeterminação informativa, fixando que esse se consubstancia no direito de os indivíduos “decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2006, p. 196).

O direito à autodeterminação informativa deriva das novas possibilidades da sociedade de informação, a qual, mediante o progresso científico e tecnológico, contempla formas de reunião, armazenamento, combinação e transmissão de todo tipo de dado (CUEVA, 1999, p. 38). Ocorre que, ao passo que essas novas possibilidades apresentam pontos positivos, podendo-se citar como exemplo a facilidade e o melhoramento na prestação de serviços, elas por certo deixam a privacidade e a intimidade extremamente vulneráveis por conta do grande fluxo e armazenamento de dados pessoais, demandando-se, por consequência um direito ao controle desses dados.

Dessa forma, o direito à autodeterminação informativa faculta ao sujeito um feixe de posições juridicamente protegidas, tais como, o controle das informações que circulam ao seu respeito; o poder de negar uma informação pessoal ou até opor-se ao seu recolhimento ou difusão (CASTRO, 2005, p. 27-28). Para Rodotá, a autodeterminação informativa configura o fim da linha de todo o processo evolutivo do direito à privacidade, o qual se iniciou com o direito de ser deixado só até chegar ao direito do controle sobre a circulação de informações pessoais e de determinar os limites da sua esfera privada (RODOTÁ, 2008, p. 17).

Chama-se a atenção, contudo, que à autodeterminação informativa, possui um caráter instrumental, em outros termos, tem-se a necessidade de um direito à autodeterminação informativa para que se proteja o fluxo de dados pessoais na sociedade em rede. Isso se faz imprescindível, pois o tratamento de dados pessoais, principalmente os que se encontram automatizados é uma atividade de risco, por viabilizar a exposição e utilização indevida ou abusiva de dados pessoais, seja em razão dos dados terem sido colhidos erroneamente e não corresponderem a características do seu titular, seja por serem usados por terceiros sem o consentimento do seu titular, dentre outras hipóteses (DONEDA; MONTEIRO, 2015, p. 151).

O fato é que a proteção de dados pessoais alcançou tamanha dimensão na sociedade tecnológica, que se transformou em um verdadeiro direito fundamental autônomo (SARLET, 2016, p. 468). Assim, no plano internacional, nota-se que, no ano de 2000, a Carta de Direitos Fundamentais da União Européia reconheceu o direito à proteção de dados como um direito autônomo, abandonando a concepção de que esse seria tão somente uma extensão do direito à privacidade, tal acepção pode ser constatada, visto que os dois direitos são previstos separadamente, o direito à privacidade encontra-se previsto no artigo 7º da Carta, enquanto o direito à proteção de dados está insculpido no artigo 8º (RODOTÁ, 2008, p. 16).

No que se refere o contexto brasileiro, a despeito da Constituição Federal em seu artigo 5º, XII, consagrar o direito ao sigilo das comunicações, bem como das correspondências, das comunicações telegráficas e telefônicas, não previu expressamente o

direito fundamental à proteção e à disposição de dados (SARLET, 2016, p. 468). Tal omissão não é suficiente para se negar a existência de um direito fundamental à proteção de dados no ordenamento jurídico brasileiro, por essa razão, o reconhecimento da proteção de dados como um direito autônomo deriva dos riscos que o tratamento automatizado de dados revela para a proteção da personalidade, afetando a dignidade da pessoa humana, da intimidade, da vida privada, entre outros (DONEDA; MONTEIRO, 2015, p. 163).

A este respeito, importa enaltecer a regra insculpida no art. 5º, §2°, CF, o qual dispõe: "Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte". O citado dispositivo insere no cenário constitucional brasileiro a chamada cláusula de abertura, possibilitando que outros direitos, em virtude de seu conteúdo, tenham o *status* de fundamentais, ou seja, para além do conceito formal de Constituição, há o conceito material, o qual ampara direitos que por seu conteúdo pertencem ao corpo fundamental da Constituição do Estado, mesmo não estando previstos expressamente como tais (SARLET, 2015, p. 80).

A luz do exposto reconhece-se que os direitos fundamentais possuem uma fundamentalidade formal, essa concretizada no direito constitucional positivo, bem como uma fundamentalidade material, que por seu turno, decorre da circunstância que os direitos fundamentais trazem em seu conteúdo decisões sobre a estrutura básica do Estado e da sociedade, figurando como elemento constitutivo da Constituição material. Dessa forma, a cláusula de não taxatividade propicia a abertura da Constituição a outros direitos fundamentais não contidos expressamente em seu texto, ou ainda que previstos, situados fora do catálogo de direitos fundamentais (SARLET, 2015, p. 76).

Partindo desse entendimento, nota-se que o direito à proteção de dados pessoais configura um direito materialmente fundamental, que adere ao *status* de direito fundamental por meio da cláusula de abertura, por seu conteúdo conter decisões da estrutura básica do Estado Democrático Brasileiro, algo que se justifica, por sua ínsita relação com os direitos insculpidos no Título II da CF, como o direito à intimidade, privacidade, sigilo das comunicações, entre outros, e com princípio da dignidade da pessoa humana, norteador do Estado Brasileiro, inscrito no Título I.

Por conseguinte, resta clarividente que o direito à proteção de dados é um direito fundamental autônomo tanto no plano internacional, como no nacional. Deve-se então perquirir quais as posições juridicamente protegidas desse direito que o fazem ser autônomo em face do direito à privacidade.

O direito à privacidade faculta a pessoa o poder de impedir qualquer interferência na sua vida privada e familiar; é uma espécie de proteção estática, com uma faceta preponderantemente negativa. Ao passo que o direito à proteção de dados pessoais faculta ao indivíduo mecanismos de proteção na circulação dos seus dados, exige uma postura ativa do Estado no sentido de elaborar regras de processamento e resguardo de dados pessoais; é, por isso, um tipo de poder dinâmico, que segue os dados e seus movimentos (RODOTÁ, 2008, p. 16).

Nesta senda, a dimensão subjetiva do direito à proteção de dados contempla as seguintes posições juridicamente protegidas:

> (a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (banco de dados) públicos ou privados; (b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; (c) o direito ao conhecimento de identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização de dados; (d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados; (e) o direito à retificação, e, a depender do caso, à exclusão dos dados pessoais armazenados em banco de dados (SARLET, 2016, p. 469).

Afora isso, sob outro víeis, partindo da dimensão objetiva desse direito, incumbe ao Estado um dever de proteção a ser exercido pela feitura de normas e atos administrativos que concretizem de modo efetivo o direito à proteção de dados na esfera pública e privada (SARLET, 2016, p. 469).

Nesse ponto, importa atentar, que as prestações normativas e fáticas de efetividade do direito à proteção de dados devem guardar conformidade com os princípios que norteiam o tratamento de dados pessoais, quais sejam, princípio da correção na coleta e no tratamento de dados; princípio da exatidão e atualização dos dados coletados; princípio da finalidade na coleta de dados, a qual deve ser explicita e precedida a coleta; princípio da publicidade dos bancos de dados que tratam de informações pessoais; princípio do acesso individual, a fim de ter conhecimento de quais informações são coletadas de si próprio e o princípio da segurança física e lógica da coletânea de dados (RODOTÁ, 2008, p. 59).

Faz-se imperativo a título de compreensão do direito à proteção de dados pessoais definir o que podem ser considerados dados pessoais. Nesse ínterim, a Diretiva Europeia nº 95/1995, no seu artigo 2º, prescreve que dados pessoais são "qualquer informação relativa a uma pessoa singular identificada ou identificável", sendo "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".

À vista disto, para fins de classificação de dados pessoais, consoante disciplinado na Diretiva, é fundamental que os dados em questão permitam identificar uma pessoa direta ou indiretamente; diretamente quando pela simples leitura dos dados sabe-se de quem se trata e indiretamente quando se utiliza de instrumentos razoáveis de identificação na leitura dos dados, levando indubitavelmente a identificação do indivíduo (CASTRO, 2005, p. 71).

O contexto jurídico brasileiro direciona-se para essa mesma definição de dados pessoais, conforme se pode extrair da leitura dos Projetos de Lei que tramitam na Câmara dos Deputados e no Senado Federal. O Projeto de Lei nº 5276/2015, que tramita na Câmara dos Deputados, no artigo 5º, inciso I, assevera que dado pessoal é o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa".

O Projeto do Senado Federal nº 181/2014 foi além, detalhando ainda mais o conceito de dado pessoal, definindo-o no artigo 5º, inciso I, "como qualquer informação relativa a uma pessoa natural que permita sua identificação, direta ou indiretamente, incluindo os números de identificação ou de elemento de sua identidade física, fisiológica, psíquica, econômica, cultural ou social e o endereço de protocolo de internet".

Sucede que, dentro do espectro que se entende por dado pessoal, há uma categoria ainda mais específica, designada de dados sensíveis, que são dados dotados de uma especial sensibilidade, que envolvem aspectos de origem racial, étnica, opiniões políticas, convicções religiosas ou filosóficas, dentre outros, que de algum modo podem levar a algum tipo de discriminação do indivíduo (SARLET, 2016, p. 446).

Assim, dentro da categoria de dados sensíveis estão incluídos os dados de saúde, os quais são objeto do presente estudo, sendo esses, não apenas os que resultem de diagnóstico médico, mas todos aqueles relacionados ao paciente, desde os resultados de análises clínicas até imagens de exames radiológicos, incluindo imagens em vídeo ou fotografias que sirvam para um diagnóstico (CASTRO, 2005, p. 91).

De modo mais detalhado, os referidos dados são aqueles que revelam informações sobre a saúde física e psíquica, no passado, presente ou futuro de uma determinada pessoa, incluindo as informações prestadas durante o fornecimento de dados iniciais para a prestação de serviços de saúde, ou durante essa prestação (ARAÚJO *et al*, 2016, p. 7).

A sensibilidade dos dados de saúde é explicada em razão da viabilidade da exposição desses dados gerar uma discriminação do paciente, principalmente no tocante à discriminação

em relação a doenças que ainda são estigmatizadas, como o caso da AIDS, das patologias vinculadas à genética humana, doenças mentais, bem como dados relacionados aos idosos, crianças e adolescentes. Por conseguinte, o direito à proteção de dados em matéria de saúde faz-se primordial, tendo por base o caráter sensível dessas informações (SARLET; KEINERT, 2015, p. 127-131).

Ocorre que, conforme já enaltecido, a inovação tecnológica penetrou nas relações sociais, moldando uma nova organização social, notadamente chamada de sociedade de informação, consequentemente, em matéria de saúde isso não foi diferente. Assim, no cenário da sociedade moderna passou-se a adotar o uso de e- governo, e- comércio, e- saúde, entre outros, ou seja, ocorre a passagem das relações sociais para o ciberespaço, oportunizando o processamento de grandes volumes de dados, tornando ainda mais difícil de se estabelecer um direito fundamental à proteção de dados (MOLINARO; RUARO, 2013, p. 19).

Conquanto, por certo, o uso das novas tecnologias nos serviços de saúde traz diversos benefícios para a saúde pública e individual, seja por possibilitar a criação de registros mais robustos e confiáveis sobre o cidadão, seja pelo compartilhamento mais ágil e eficiente dessas informações entre os profissionais na saúde. Nesta senda, o compartilhamento e o banco de dados em matéria de saúde geram consequências extremamente positivas para a sociedade, como o controle de epidemias, cura de determinadas doenças, diagnósticos mais eficientes, dentre outros (DONEDA; MONTEIRO, 2015, p. 148).

Não por outra razão, que o uso de tecnologias de informação no setor de saúde cresceu de modo acelerado nas últimas três décadas, no setor público e privado, sendo inconteste que a inserção dessas tecnologias afeta de modo positivo a prestação dos serviços de saúde (VIEIRA, 2013, p.33).

Se por um lado as novas tecnologias viabilizam maior eficiência na proteção e promoção do direito fundamental à saúde, por outro, à luz do direito à proteção de dados, os sistemas automatizados de informações de saúde possuem um risco em potencial, pois facilitam o armazenamento e o compartilhamento desses dados sensíveis, o que poderá levar ao uso secundário e a exposição de tais dados sem o consentimento da pessoa, em clara violação ao direito fundamental à proteção de dados.

Dessa forma, não se defende uma supressão dos instrumentos tecnológicos em matéria de saúde, algo que seria totalmente utópico na sociedade atual e representaria um retrocesso na promoção e proteção do direito fundamental à saúde, mas argumenta-se sobre a indispensabilidade de se considerar os princípios norteadores do direito fundamental à proteção de dados na implementação desses instrumentos.

3 O TRATAMENTO DE DADOS PESSOAIS EM MATÉRIA DE SAÚDE NO BRASIL: POSSIBILIDADES E LIMITES

Consoante já enaltecido, a inovação tecnológica propiciou a incorporação de tecnologias no setor da saúde, o que vem merecendo destaque desde a década de 1970, desenvolvendo-se o que se denominou de *e-health* (Saúde Eletrônica) (ARAÚJO *et al*, 2016, p. 3). Assim, a Organização Mundial de Saúde define a *e-health* como sendo a inserção das tecnologias de informação e comunicação à saúde, ou seja, representa a prática de atenção à saúde facilitada e aperfeiçoada por tais tecnologias (VIEIRA, 2013, p. 34).

Dentre os benefícios da "saúde eletrônica" está a promoção da gestão facilitada nos processos de atendimento ao paciente, visando a maior segurança e confiabilidade nas decisões clínicas e nos diagnósticos, como também auxilia na execução de políticas públicas nessa área, na identificação dos fatores determinantes do bem-estar dos cidadãos e no controle de epidemias (VIEIRA, 2013, p. 34).

Mas não é só, tem-se ainda que esse novo modo de se promover o direito à saúde contribui para o próprio direito à informação em matéria de saúde aos cidadãos, permitindo que, pelo acesso de informações adequadas, se estimule uma melhor qualidade de vida com o incentivo de hábitos saudáveis, reduzindo, por via consequencial, os riscos de adoecimento (VENTURA, 2013, p. 636).

À par disso, o Brasil seguindo a tendência mundial, em 2009, por meio da Portaria nº 2.690, instituiu a Política Nacional de Gestão de Tecnologias em Saúde no âmbito do Sistema Nacional de Saúde, estabelecendo a gestão de tecnologias em saúde "como o conjunto de atividades gestoras relacionadas com os processos de avaliação, incorporação, difusão, gerenciamento da utilização e retirada de tecnologias do sistema de saúde" (art. 2º).

Afora isso, destaca-se que a Portaria nº 2.690 dispõe em seu artigo 3º como sendo objetivo da referida Política a maximização dos benefícios em matéria de saúde, a qual será alcançada por meio dos recursos tecnológicos efetivos e seguros ofertados à população. Frisando-se que a Portaria, ainda que indiretamente, faz menção a alguns aspectos do direito à proteção de dados pessoais, ao ressaltar, por exemplo, a imprescindibilidade de "sensibilizar os profissionais de saúde e a sociedade em geral para a importância das consequências econômicas e sociais do uso inapropriado de tecnologias nos sistemas e serviços de saúde" (art. 3º, IV).

No entanto, expressamente a Portaria nada trouxe em relação à proteção de dados pessoais no processo de inserção de tecnologia no sistema de saúde, o que de certo modo, conjugado com a ausência de regulação acerca da proteção de dados no cenário jurídico brasileiro contribui para a vulnerabilidade dos instrumentos implementados com base nessa Política no tocante ao tratamento de dados pessoais, como se passará a se tratar.

Dentre esses instrumentos, o primeiro que se chama atenção é o Telessaúde. O Telessaúde Brasil Redes é um sistema de suporte tecnológico que possibilita a interconexão de profissionais de saúde de vários lugares do Brasil, o compartilhamento rápido e eficiente de dados, imagens e registros em geral, por qualquer computador (SARLET; KEINERT, 2015, p. 134).

Ou seja, o Telessaúde tem por objetivo a prestação de serviços à distância, o intercâmbio de informações entre os profissionais de saúde de todo o Brasil, quebrando as barreiras geográficas, temporais, sociais e culturais, de modo a contribuir na qualidade, rapidez e eficiência na prestação de serviço à saúde (MINISTÉRIO DA SAÚDE, 2016, p.38).

A Portaria nº 2.546/2011 redefine e amplia o Programa Telessaúde Brasil, concebendo que esse programa fornecerá aos trabalhadores e profissionais na área da saúde, os serviços de: (a) teleconsultoria, que consiste na consulta registrada e realizada entre trabalhadores, profissionais e gestores na área da saúde, a qual poderá ocorrer em tempo real, por chat, web ou videoconferência, como também poderá ser realizada por meio de mensagens off-line; (b) telediagnóstico, que consiste em serviço de apoio ao diagnóstico, através de trocas de conhecimento entre os profissionais de saúde; (c) segunda- opinião formativa, que é a resposta sistematizada a perguntas originadas nas teleconsultorias, orientadas por evidencias científicas e clínicas e a (d) tele-educação, que se transmuda em aulas e cursos ministrados por meio das tecnologias de informação (art.2º, I, II,III,IV).

Os benefícios do Telessaúde são incontestes, contribuem para a capacitação dos profissionais da saúde através da tele- educação, na solução de diagnósticos e tratamentos de difícil resolução, com base na troca de informações de profissionais especializados nas mais variadas áreas, além de, através do intercâmbio de informações de locais distintos do Brasil, propiciar a descoberta primitiva de determinadas doenças, facilitando o desenvolvimento de uma possível cura, ou ainda no controle de epidemias, dentre outras possibilidades.

Entretanto, não se deve silenciar acerca dos riscos à proteção de dados pessoais que possam advir do referido Programa, tais como, a perda da confidencialidade das informações prestadas pelos pacientes que são atendidos por meio do Telessaúde. Isso porque, por vezes, o indivíduo é atendido por um médico específico, o qual pessoalmente colhe seus dados

pessoais, mas posteriormente, compartilha-os através da teleconsultoria ou do telediagnóstico, com outros profissionais de saúde. Esses dados, então, são repassados, armazenados e compartilhados por computadores, sendo criado um verdadeiro banco de dados pessoais, o qual pode ser facilmente violado e do qual, geralmente, sequer os pacientes têm conhecimento (SARLET; KEINERT, 2015, p. 124).

Destaca-se que por vezes o ambiente que ocorre a teleconsultoria ou o telediagnóstico, envolve a participação não só de profissionais da saúde, como também de outros profissionais, a exemplo de técnicos de informática, os quais poderão facilmente ter acesso às informações confidenciais dos pacientes. Para, além disso, o armazenamento e a transmissão de dados pelo Telessaúde propiciam um ambiente de fácil alteração, podendo ser essa intencional ou não, das mensagens trocadas entre os profissionais, o que leva a violação do princípio da exatidão dos dados pessoais (REZENDE *et al*, 2013, p. 369).

Ademais, apesar do Ministério da Saúde, ser enfático no sentido de que as Unidades de Saúde que participam do Programa Telessaúde devam contar com computadores que sejam de uso exclusivo ou extremamente preferencial para o Telessáude, ressaltando que o ambiente no qual ocorre as teleconsultorias e os telediagnósticos deverá ser restrito e isolado, permitindo a troca confidencial entre os profissionais de saúde (MINISTÉRIO DA SAÚDE, 2012, p. 31-31), sabe-se que a falta de fiscalização na execução das políticas públicas torna na maior parte dos casos inaplicável tal orientação, ensejando a exposição irregular de dados sensíveis dos pacientes.

Outro instrumento que merece atenção é o prontuário eletrônico. O prontuário consoante a Resolução nº 1638/2002 do Conselho Federal de Medicina, consiste:

> No 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 (art.1º).

Percebe-se, pois, que o prontuário figura como um documento que contém inúmeros dados sensíveis do paciente, os quais são de extrema relevância médica, além de primordiais para um efetivo tratamento, ao passo que demandam também sigilo e proteção. Ocorre que com o desenvolvimento das novas tecnologias, nasce a forma eletrônica do prontuário médico, de modo que o prontuário médico eletrônico traz consigo diversos benefícios, como a atualização, legibilidade e exatidão das informações, as quais são disponíveis qualquer

momento e em qualquer lugar para o médico, trazendo maior segurança ao paciente e maior efetividade no tratamento (CONSELHO FEDERAL DE MEDICINA, 2012, p. 6).

Em contrapartida, o prontuário eletrônico possibilita o compartilhamento dos dados do paciente de maneira facilitada com terceiros, bem como seu armazenamento em banco de dados, o que viabiliza um ambiente favorável ao uso inadequado e a quebra na proteção dos dados pessoais (SARLET; KEINERT, 2015, p. 124).

O uso inadequado dos dados do prontuário eletrônico pode ser de dois modos, o primeiro consiste no compartilhamento desses dados com outros profissionais ou outras instituições sem o consentimento e o conhecimento do paciente. O segundo, que poderá ocorrer o uso secundário desses dados, também destituído do conhecimento e do consentimento do indivíduo, havendo um desvirtuamento da finalidade da coleta de dados.

Nesse último, salienta-se que o próprio Conselho Federal de Medicina na sua Cartilha sobre prontuário eletrônico, trata expressamente sobre o uso secundário dos dados, sem sequer ressaltar a imprescindibilidade do consentimento do indivíduo para tanto. O Conselho enaltece que o prontuário eletrônico, tem como um de seus benefícios à contribuição para a pesquisa clínica, sendo utilizados de modo secundário para fins de pesquisa, estatísticos e epidemiológicos (CONSELHO FEDERAL DE MEDICINA, 2012, p.06).

Ora, o uso secundário irrestrito dos dados contidos no prontuário médico, sem qualquer cuidado com o consentimento do paciente, viola diretamente o direito fundamental à proteção de dados pessoais. Clarifica-se que os dados contidos no prontuário são de propriedade do paciente, sendo os profissionais de saúde responsáveis direta e indiretamente por sua custódia e confidência, assim, as Instituições e os esses profissionais são compelidos a não revelar as informações fornecidas em confidência pelo paciente sem sua autorização, excetuando-se apenas o caso de tais informações poderem ser utilizadas em função da necessidade de cuidado ao paciente, por estrito dever legal (MOTTA, 2005, p. 5).

Há que se falar também em termos de tecnologia aplicável ao sistema de saúde, sobre o Portal de Saúde do Cidadão criado pelo Ministério da Saúde. Lançado em 2012, o Portal registra as informações individualizadas de produção do atendimento e exames realizados pelo cidadão no Sistema Único de Saúde, de modo que esse poderá ter acesso aos procedimentos médicos realizados, aos atendimentos por quais passou, bem como os exames realizados, além de ter acesso às informações gerais de interesse à saúde (VIEIRA, 2013, p. 39).

Trata-se de verdadeiro instrumento de um Governo Digital, o que se comumente denomina de *e- government*, destarte, através de ferramentas tecnológicas o Estado cria novos canais de interlocução com a sociedade, especificadamente o ambiente virtual, promovendo um contato mais rápido com o cidadão, concretizando o direito à informação, bem como executando políticas públicas em diversas áreas. Em matéria de saúde, ferramentas como essas ganham relevância, visto que se trata de um setor carente de cuidados e reformas para conferir maior eficácia aos serviços prestados, prescindindo de políticas públicas que realmente apresentem resultados (CERQUINHO; TAVARES; VITORINO, 2015, p. 350).

Sucede que, o Portal da Saúde passa pela mesma problemática das outras ferramentas tecnológicas do sistema de saúde, qual seja, a proliferação na formação de banco de dados, que são naturalmente transferidos, manipulados e até reinventados, levando a riscos que afrontam a dignidade da pessoa humana, como por exemplo, no tocante aos dados sensíveis de saúde, a discriminação da pessoa por ser portador de uma dada doença ainda estigmatizada pela sociedade (RUARO; LIMBERGER, 2012, p. 87).

Enaltece-se que não se esgota no presente artigo os diversos mecanismos da saúde eletrônica no Brasil, esses foram apenas alguns exemplos que se procurou trazer para ilustrar que a despeito dos seus benefícios, esses em razão da ausência de legislação robusta sobre o tema, são extremamente frágeis no que se refere à proteção de dados.

Salienta-se que há dois grandes desafios na proteção de dados na sociedade de informação, o primeiro é a facilidade no acesso e compartilhamento desses dados, os quais podem recair na mão de terceiros e serem facilmente publicizados. O segundo é que as inovações tecnológicas colocaram também em funcionamento instrumentos de comunicação de mão dupla, ou seja, coletam-se dados para o fornecimento de serviços, criam-se verdadeiros bancos de dados e os utilizam, posteriormente e sem o consentimento da pessoa, para finalidades secundárias (RODOTÁ, 2008, p. 47).

Em matéria de saúde não é diferente, a saúde eletrônica exige do cidadão que, para ter acesso à prestação do serviço à saúde, forneça dados pessoais, os quais são armazenados; e o perigo ocorre exatamente no uso secundário desses dados. Isso porque por vezes o uso secundário acontece não só para a utilização de aperfeiçoamento dos serviços saúde pública, ou para pesquisas, estatística e controle epidemiológico, conforme já ressaltado. Mas pode calhar, que em razão da facilidade do acesso a esses dados, eles recaiam no domínio de terceiros não envolvidos na prestação dos serviços de saúde, como entidades privadas, prestadoras de serviços e produtos no mercado de consumo (DONEDA; MONTEIRO, 2015, p. 148).

Nessa hipótese, ter-se-á o uso secundário desses dados no sentido de que, eles conjugados com demais dados pessoais que o indivíduo possui na rede, tais como os de consumo, oportunizam a criação de perfis individuais, com a identificação precisa de hábitos, inclinações, interesses e preferências, (RODOTÁ, 2008, p.62), o que poderá ocasionar uma discriminação do indivíduo por parte das empresas creditícias e das seguradoras de saúde (MOLINARO; RUARO, 2013, p. 20).

Não por outra razão, reconhecendo-se a vulnerabilidade da proteção de dados em matéria de saúde, o próprio Ministério da Saúde, está em um processo de estímulo e consolidação de uma Política de Informação e Informática em Saúde (PNIIS), tendo por um de seus fundamentos a ausência de padronização nos procedimentos de coleta e tratamento de dados em saúde (MINISTÉRIO DA SAÚDE, 2016, p. 7), algo que contribui por certo com a vulnerabilidade na proteção de dados pessoais, por não se ter um efetivo controle, confiabilidade e segurança no tratamento de tais dados.

Realça-se que a PNIIS contempla como um de seus princípios "a confidencialidade, sigilo e privacidade da informação de saúde pessoal como direito de todo indivíduo", o qual está diretamente conectado com a proteção de dados pessoais.

Com base no exposto, tem-se que a inserção das novas tecnologias em matéria de saúde traz inúmeros benefícios para a promoção e proteção desse direito fundamental, no entanto, não sendo ele absoluto, há urgentemente que se fixar instrumentos de conciliação da saúde eletrônica com a proteção de dados sensíveis de saúde, de modo que esse não reste esvaziado na sociedade de informação.

De qualquer sorte, o primeiro passo é estabelecer uma legislação acerca da matéria, a qual vincule todos os envolvidos, formando um sistema de responsabilidade solidária no caso de violação à proteção de dados pessoais. Uma legislação que estabeleça critérios de máxima transparência nas atividades desenvolvidas na saúde eletrônica e que evidencie a imprescindibilidade do consentimento do indivíduo para o uso e compartilhamento de seus dados (VENTURA, 2013, p. 626).

Necessário também, definir padrões mínimos de segurança dos bancos de dados, que impossibilite o acesso a terceiros não participantes da prestação dos serviços de saúde a esses dados, bem como, estabelecer formas de controle de quem pode ter acesso a essas informações (SARLET; KEINERT, 2015, p. 135).

Nesse ponto, enfatiza-se que o principal instrumento para se elaborar uma legislação eficaz no que toca a proteção de dados pessoais é partir da análise de todas as potencialidades do uso das tecnologias e não somente avaliar formas de conter o poder das redes tecnológicas,

para tanto é importante principalmente estabelecer meios de controle e conhecimento por parte do indivíduo acerca da circulação, do uso e armazenamento dos seus dados (RODOTÁ, 2008, p. 33).

No entanto, em nada se prestará uma legislação eficaz sem o monitoramento da sua efetiva aplicação na execução da política pública de saúde eletrônica. Por fim, tais soluções serão totalmente inócuas se não se promover a capacitação e conscientização dos profissionais de saúde no que se refere a utilização das tecnologias em matéria de saúde, a fim de que eles tenham total conhecimento e domínio das suas potencialidade e limites.

CONSIDERAÇÕES FINAIS

A inovação tecnológica consiste em um verdadeiro mecanismo de progresso social, dessa forma, a sociedade não só molda o processo de inovação, como é ela própria definida por ele, por derradeiro, a partir do desenvolvimento das novas formas de produzir e aplicar o conhecimento na seara tecnológica fez-se emergir a sociedade de informação.

Essa, por sua vez, é denominada sociedade de rede, na qual se possibilita cada vez mais a circulação acelerada de informações e o armazenamento e associação de dados. É nesse cenário que o direito à privacidade ganha novos contornos, e passa por todo o processo evolutivo, partindo do marco inicial de um direito a ser deixado só, até ao direito do indivíduo do controle das informações que lhe digam respeito, podendo inclusive fazer cessar a circulação dessas informações.

Nesse cenário que surge o direito à proteção de dados pessoais como um direito autônomo, sendo reconhecido como tal por meio da sua fundamentalidade material, e adentrando-se no catálogo de direitos fundamentais na ordem Constitucional Brasileira por meio da cláusula de abertura insculpida no §2º do artigo 5º da CF/88.

Tem-se, que os dados em matéria de saúde consubstanciam uma categoria de dados pessoais, comumente denominada de dados sensíveis, que fazem menção a aspectos mais íntimos da vida do indivíduo, os quais merecem proteção, tendo em vista que por vezes a exposição de tais dados levará a uma discriminação do sujeito por parte de terceiros.

Afora isso, vislumbra-se que a inovação tecnológica influenciou na prestação de serviços de saúde, criando a saúde eletrônica, essa promove benefícios de extrema relevância na proteção do direito à saúde, contudo, as novas tecnologias precisam ser implementadas de modo a não esvaziar à proteção de dados pessoais em matéria de saúde, a qual está cada vez mais deficitária nesse novo formato de prestação de serviços de saúde.

Posto isso, conclui-se pela imprescindibilidade da feitura de uma legislação robusta sobre o tema, que viabilize a implementação adequada da saúde eletrônica, fixando mecanismos de segurança dos bancos de dados, tratando-se expressamente sobre o consentimento do indivíduo no tocante ao tratamento de seus dados pessoais por terceiros, bem como atribua atenção à capacitação dos profissionais da saúde sobre os limites e as possibilidades das novas tecnologias na prestação de serviços de saúde.

REFERÊNCIAS

ARAÚJO, Alexandra Rodrigues *et al*. Saúde Móvel: desafios globais à proteção de dados pessoais sob a perspectiva do direito da União Europeia. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, Rio de Janeiro, v. 10, n. 4, out./dez. 2016. Disponível em: <http://www.arca.fiocruz.br/handle/icict/17000> Acesso em: 10. mai. 2017.

BECK, Ulrich. **La sociedad del riesgo:** hacia una nueva modernidad. Barcelona: Paidós, 1998.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1980. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: 10 mai. 2017.

CASTELLS, Manuel. A Sociedade em rede: do conhecimento à política. *In:* CASTELLS, Manuel; CARDOSO, Gustavo. **A Sociedade em Rede** - Do conhecimento à acção política. Lisboa: Imprensa Nacional, 2005, p. 17- 30.

CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CERQUINHO, Kleomara Gomes; TAVARES, Wellington; VITORINO, Irineu Amaro. O cidadão e o acesso à saúde por meio digital: uma análise da gestão do Portal da Saúde nos limites entre *e-government* e *e-participation. In:* KEINERT, Tania Margarete Mezzomo *et al* (Org.). **Proteção à privacidade e acesso às informações em saúde**: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

CONSELHO FEDERAL DE MEDICINA. **Cartilha sobre prontuário eletrônico: a certificação de sistemas de registro eletrônico de saúde**¸ fev. 2012. Disponível em: <http://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf>. Acesso em: 15 mai. 2017.

DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. **Revista de Estudios Políticos** (Nueva Época), n. 104, p. 35-60, abr./jun. 1999.

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

DONEDA, Danilo; MONTEIRO, Marilia de Aguiar. Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde – privacidade e e-Health. *In:* KEINERT, Tania Margarete Mezzomo *et al* (Org.). **Proteção à privacidade e acesso às informações em saúde**: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

FERRY, Luc. **A Inovação Destruidora** - ensaio sobre a lógica das sociedades modernas. Rio de Janeiro: Objetiva, 2015

MENDES, Gilmar Ferreira; COELHO, Inocêncio Martires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 4. ed. rev. e atual. São Paulo: Saraiva, 2009.

MINISTÉRIO DA SAÚDE. **Manual de Telessaúde**: para Atenção Básica/Atenção Primária à Saúde. Brasília: Ministério da Saúde, 2012. Disponível em: <http://dab.saude.gov.br/portaldab/biblioteca.php?conteudo=publicacoes/manual_telessaude> Acesso em: 10 mai. 2017.

MINISTÉRIO DA SAÚDE. **Política Nacional de Informação e Informática em Saúde**. Brasília: Ministério da Saúde, 2016. Disponível em: <http://bvsms.saude.gov.br/bvs/publicacoes/politica_nacional_infor_informatica_saude_2016.pdf>. Acesso em: 15 mai. 2017.

MIRANDA, Victor Vasconcelos. O direito à privacidade na era digital e as tutelas assecuratórias. **Fórum de Direito Civil**, Rio de Janeiro, n. 12, p. 97-121, mai./ago. 2016.

MOLINARO, Carlos Alberto; RUARO, Regina Linden. Internet y estado de Vigilancia: El Desafio de la Protección de Datos (Internet and the Surveillance State: The Challenge of Data Protection). **SSRN Eletronic Journal**, Londres, ago. 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2310267>. Acesso em: 10 mai. 2017.

MOTTA, Gustavo Henrique Matos Bezerra. **Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos**. 2003. Tese (Doutorado em Sistemas Eletrônicos) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2004.

REZENDE, Edson José Carpintero *et al*. Telessaúde: confidencialidade e consentimento informado. **Revista Médica de Minas Gerais**, Belo Horizonte, v. 23.3, p. 367-373, Jul./Set. 2013. Disponível em: http://www.rmmg.org/artigo/detalhes/223. Acesso. 10 mai. 2017.

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

RUARO, Regina Linden; LIMBERGER, Têmis. Banco de dados de informações genéticas e administração pública como concretizadora da proteção dos dados pessoais e da dignidade humana. **Revista NEJ – Eletrônica,** Itajaí, v. 18, n. 1, p. 85-99, jan./abr. 2013.

RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Revista Direito, Estado e Sociedade**, Rio de Janeiro, n. 36, p. 178-199, jan./jun. 2010.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2015.

SARLET, Ingo Wolfgang. Direitos Fundamentais em Espécie. *In:* SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 5. ed. rev. e atual. São Paulo: Saraiva, p. 400-735.

SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In:* KEINERT, Tania Margarete Mezzomo *et al* (Org.). **Proteção à privacidade e acesso às informações em saúde**: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

VENTURA, Miriam. Lei de acesso à informação, privacidade e a pesquisa em saúde. **Caderno de Saúde Pública**, Rio de Janeiro, n. 29, p. 636-638, abr. 2013.

VIEIRA, Augusto Cesar Gadelha. O projeto cartão nacional de saúde e a construção de e-saúde para o Brasil. *In:* BARBOSA, Alexandre F. (Org.). **TIC SAÚDE 2013** - pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2015, p. 33-46.

WERTHEIN, J. A sociedade da informação e seus desafios. **Ciência da Informação**, v. 29, n. 2, p. 71-77, 2000. Disponível em: <http://basessibi.c3sl.ufpr.br/brapci/v/a/967>. Acesso em: 20 mai. 2017.