E-Saúde e desafios à proteção da privacidade no Brasil

Koichi Kameda[1]
Magaly Pazello[2]

Ementa: 1. Introdução. 2. Iniciativas de e-Saúde no Brasil. 3. Desafios à proteção da privacidade no âmbito dos sistemas de e-Saúde e a necessidade de um marco regulatório do tratamento de dados pessoais. 4. Conclusão.

1. Introdução

O uso de tecnologias de informação e comunicação (TICs) em saúde para o oferecimento e entrega de serviços de saúde é hoje visto como estratégico em todo mundo, incluindo o Brasil. Grandes promessas (algumas antigas e custosas) alimentam a introdução de prontuários eletrônicos nas unidades de saúde e a criação de registro eletrônico de saúde dos usuários do Sistema Único de Saúde (SUS), assim como o uso de redes colaborativas para auxiliar a prestação de serviços, entre os quais o telediagnóstico, a teleconsultoria etc.

Esses sistemas envolvem a intensa manipulação de informações pessoais de saúde, consideradas informações sensíveis em razão do potencial discriminatório que guardam caso sejam reveladas em determinadas situações e sem o consentimento de seu titular. Assim, preocupações com a proteção da privacidade dos pacientes nesses ambientes inevitavelmente emergem.

Este artigo tem o propósito de apresentar um breve panorama da eSaúde no Brasil, identificando as principais iniciativas já implementadas ou em vias de implementação, e a presença (ou ausência) de salvaguardas legais e normativas para a proteção da privacidade dos usuários dos sistemas de saúde.

2. Iniciativas de e-saúde no Brasil

O uso de tecnologias de informação e comunicação para mediar a atenção à saúde é denominado de eSaúde (*eHealth*). A terminologia[3], adotada pela Organização Mundial da Saúde para abarcar o campo, inclui a assistência a paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde.[4] De mais específico, processos de e-Saúde incluem: teleconsultorias, telediagnóstico, segunda opinião formativa, telecirurgia, telemonitoramento (televigilância), educação permanente, teleducação e prontuário eletrônico.[5]

Alguns exemplos de iniciativas de eSaúde são a rede RUTE, considerada bem-sucedida; o Cartão Nacional de Saúde; e a adoção de prontuário eletrônico.

---

1 Pesquisador do Instituto Nupef, bacharel em Direito pela UERJ e doutorando em Saúde Coletiva no Instituto de Medicina Social da UERJ

2 Pesquisadora do Instituto Nupef

3 Outros termos comumente utilizados como sinônimos de eSaúde são telessaúde e telemedicina, embora tenham sido utilizados em momentos mais iniciais (Rezende et al., 2010). Hoje a preferência é pela terminologia "eSaúde". (PNIIS, 2012).

4 http://www.who.int/topics/ehealth/en/ .

5 REZENDE, E. J. C. et al. Ética e telessaúde: reflexões para uma prática segura. Rev Panam Salud Publica, v. 28, n. 1, p. 58–65, 2010.

A RUTE - Rede Universitária de Telemedicina (www.rute.rnp.br) -, é um projeto do Ministério da Ciência, Tecnologia e Inovação, criado em 2005 com o propósito de conectar hospitais universitários e instituições de ensino via infraestrutura de comunicação nacional da Rede Nacional de Ensino e Pesquisa, possibilitando, de modo colaborativo, a realização de videoconferências para o intercâmbio de informação, discussões, estudo de casos, educação continuada, segunda opinião formativa, teleconsultoria, entre outros usos.[6]. Outra rede é a Telessaúde Brasil Redes, capitaneada pelo Ministério da Saúde, e inicialmente instituída sob o nome Programa Nacional de Telessaúde em 2007.[7]

O Cartão Nacional de Saúde, também conhecido como Cartão SUS, é um documento de identificação do usuário do SUS. Instituído em 1996, possui mais de 144 milhões de usuários cadastrados. Entre os objetivos do Cartão, que passa por reformulação, estão facilitar a marcação de consultas e exames pelos pacientes e permitir a consulta ao histórico clínico dos usuários a partir de uma base de dados.[8]. O projeto é alvo de críticas, tendo a falta de transparência sido apontada como uma das explicações para a sua não finalização. Com a promessa da integração digital do SUS com interoperabilidade, mais de duzentos milhões de dólares foram gastos pelos governos entre 2000 e 2011, sem o acompanhamento do controle social.[9]

Recentemente a Secretaria de Estado da Saúde de São Paulo lançou um modelo de prontuário eletrônico unificado com o histórico de atendimentos dos pacientes nas unidades estaduais de saúde. O programa "S4SP" (Saúde para São Paulo), com investimentos de R$ 56 milhões do governo do Estado, foi desenvolvido no Instituto do Coração (InCor) do Hospital das Clínicas da Faculdade de Medicina da USP, numa parceria com a Companhia de Processamento de Dados de São Paulo (Prodesp). O sistema permitirá o armazenamento padronizado e o compartilhamento dos registros de saúde do paciente coletados em hospitais, ambulatórios, laboratórios ou farmácias da Secretaria. Segundo notícia da página eletrônica oficial da Secretaria da Saúde do Governo do Estado de São Paulo, "o grande diferencial do novo sistema é operar em 'nuvem', o que resultou em custo zero em hardwares, softwares e equipamentos, como microcomputadores, ou mesmo a montagem de uma rede física de servidores e sistema de segurança e manutenção."[10]. A Prodesp ficará responsável pela garantia do sigilo das informações dos cerca de vinte milhões de pacientes do SUS no Estado. [11].

---

6 A nível operacional, cada membro da rede formaliza o seu Núcleo de Telemedicina e Telessaúde, com espaço físico e equipe dedicada; são organizados workshops para compreensão do trabalho colaborativo visando à integração nacional em ensino, pesquisa e melhoria do atendimento de saúde da população; e grupos de interesse especial formados pelas instituições são criados para o desenvolvimento de atividades colaborativas de pesquisa, ensino e assistência em temas específicos da Telemedicina e Telessaúde. (Coury et al, 2010). Para mais informações sobre a RUTE ver Coury et al, 2010; Silva e Moraes, 2012.

7 SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

8 "Ceensp debate novos rumos para o Cartão SUS". Disponível em Disponível em http://www.ensp.fiocruz.br/portal-ensp/informe/site/materia/detalhe/24947

9 SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

10 "Paciente ganha prontuário unificado na rede do SUS paulista". Disponível em http://www.saude.sp.gov.br/ses/noticias/2013/agosto/paciente-ganha-prontuario-unificado-na-rede-do-sus-paulista

É preciso observar que o campo da eSaúde está diretamente relacionado às políticas de informação, informática e comunicação em saúde no Brasil. Essa afirmação é importante num contexto em que se constata a inseparabilidade cada vez maior entre informação e as tecnologias que lhe dão suporte, o que tem contribuído para a progressiva substituição da denominação "informação, informática e comunicação" por "tecnologia da informação e comunicação".[12].

O uso de informação para gestão do sistema de saúde não é de hoje entendida como relevante, tendo a lei 8.080/1990 incluído entre as atribuições das unidades federativas a organização e coordenação do sistema de informação em saúde (art. 15, inciso IV, CF). A despeito dos diversos sistemas de informação em saúde existentes, Vasconcellos e Moraes (2005, p. 97) identificam o potencial, ainda pouco explorado, do uso da informação no processo decisório de saúde, incluindo a formulação de políticas, gestão, vigilâncias, clínica e também no controle social a fim de enfrentar a desigualdade de acesso aos benefícios do avanço tecnológico.

A necessidade de se estabelecer o propósito e as diretrizes de um Sistema Nacional de Informação em Saúde levou à elaboração de uma Política Nacional de Informação e Informática em Saúde, finalizada em 2004. Embora a PNIIS não tenha tido seu conteúdo regulamentado nem institucionalizado, acredita-se que tenha servido de inspiração para ações e normatizações no âmbito do SUS e do MS, bem como fundamento para o processo de construção da PNIIS 2012, em fase final de elaboração.[13]

O documento de 2012, que ainda resta ser aprovado, reconhece "eSaúde" como a terminologia mais utilizada no mundo para descrever as políticas nacionais na área de TI em saúde e propõe a mudança da nomenclatura para "Política Nacional de eSaúde".[14] Nesse contexto, o documento afirma que a nova PNIIS deve ter como foco o usuário e registro eletrônico de saúde (RES), defendendo para isso o estabelecimento de padrões para representação e compartilhamento da informação em saúde, de infraestrutura de conectividade, a capacitação de recursos humanos na área de informação e informação em saúde, e, principalmente, a garantia da privacidade e confidencialidade da informação de saúde pessoal.[15].

Em paralelo aos debates para revisão da PNIIS, a constatação da necessidade de uma política estratégica de eSaúde levou à elaboração de uma proposta de "Visão Estratégica de eSaúde para o Brasil", conduzida pela Secretaria de Gestão Estratégica e Participativa (SGEP) do Ministério da Saúde, por meio do Departamento de Informática do SUS (DATASUS). A construção desse documento se deu em oficinas

---

11 "Entidades médicas de SP temem quebra de sigilo em novo modelo de prontuário digital". Disponível em http://veja.abril.com.br/noticia/saude/entidades-medicas-de-sp-temem-quebra-de-sigilo-em-novo-modelo-de-prontuario-digital

12 MORAES, I. H. S. DE; VASCONCELLOS, M. M. 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.

13 BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em:http://www.isc.ufba.br/arquivos/2012/Politica_Nacional_de_Informacao_e_Informatica_em_Saude.pdf

14 Para mais detalhes sobre o documento da PNIIS 2012, consultar: http://www.isc.ufba.br/arquivos/2012/Politica_Nacional_de_Informacao_e_Informatica_em_Saude.pdf

15 BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em:http://www.isc.ufba.br/arquivos/2012/Politica_Nacional_de_Informacao_e_Informatica_em_Saude.pdf

com a participação de profissionais representativos do Ministério da Saúde e de outros órgãos do governo federal, estadual e municipal, bem como do setor privado e de organizações não governamentais. Essas oficinas de eSaúde, realizadas desde maio de 2012, tiveram como foco a construção do RES, que integrado ao Sistema de Informação de Saúde (E-SUS), compõe o Sistema Cartão Nacional de Saúde. O grupo de trabalho é composto por especialistas e técnicos do Poder Executivo Federal, de conselhos de classe, das operadoras de planos de saúde e profissionais de saúde dos Estados e Municípios.[16]

3. Desafios à proteção da privacidade no âmbito dos sistemas de eSaúde e a necessidade de um marco regulatório do tratamento de dados pessoais

Os sistemas de e-Saúde, por envolverem o processamento de informações, que varia da simples comunicação entre pacientes e funcionários ao compartilhamento mais complexo de dados entre instituições de atenção à saúde[17], exigem cautela quanto ao seu emprego e ambiente tecnológico e, ao mesmo tempo, garantias com relação a proteção da privacidade e dos dados pessoais dos pacientes e usuários dos serviços de saúde. Ademais, esses sistemas, em razão de sua diversidade, envolvem o tratamento de diferentes tipos de informação pessoal para propósitos distintos.[18].

Antes de avançar, é preciso fazer alguns esclarecimentos.

Ainda que corriqueiramente utilizados como sinônimos, existe distinção entre "dado" e "informação". "Dado" possui uma conotação mais primitiva, estando ligado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração da informação. "Informação", por sua vez, pressupõe a depuração de seu conteúdo.[19].

Quando se fala em dados ou informações pessoais, refere-se a qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, como o seu nome, número de identidade, etc.

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. [20.]

Os dados de saúde são considerados dados sensíveis, assim como aqueles dados que revelem a origem racial ou étnica de uma pessoa, sua convicção religiosa, filosófica ou moral, sua opinião política, sua filiação partidária, sindical ou a organizações de caráter religioso, filosófico ou político. Também são incluídos entre os dados sensíveis os dados referentes à vida sexual e os dados genéticos e biométricos de uma pessoa. [21] [22]

---

16 "Especialistas se reúnem em Brasília para a VI Oficina da E-Saúde". Disponível em http://portal.saude.gov.br/portal/saude/profissional/visualizar_texto.cfm?idtxt=42509

17 Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

18 Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

19 DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006.

20 DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006.

Considerados esses esclarecimentos, num contexto atual em que as novas tecnologias possibilitam o registro e o tratamento de informações em grande volume, incluindo informações sensíveis, surgem alguns desafios à proteção da privacidade dos usuários do sistema de saúde, como aqueles relacionados ao "vazamento" e ao acesso indevido de dados pessoais. A ausência de uma política de administração dessas informações permite que a sua manipulação ocorra de modo descuidado e em quantidades excessivas, facilitando a sua difusão pública, acidental ou intencional.[23]

Os casos de vazamento de dados pessoais, ao se tornarem públicos, acabam provocando uma sensação de desconfiança por parte dos cidadãos e dos consumidores em relação à instituição que permitiu a difusão das informações. E ainda que não se torne pública, a difusão indevida dos dados é capaz de provocar danos concretos em diversas situações, com potencial de discriminação no caso de dados sensíveis. [24].

Outro risco envolve a transferência de dados pessoais sem consentimento do seu titular ou utilização dos dados para fins distintos dos que legitimaram a sua coleta. Denúncia recente causou grande polêmica ao revelar convênio firmado pelo Tribunal Superior Eleitoral para entrega de dados pessoais de eleitores para o Serasa, empresa privada que se ocupa da comercialização de informações.[25]

Essas preocupações fazem total sentido no âmbito das iniciativas de eSaúde, que têm o potencial de identificar o usuário dos serviços de saúde a partir da expansão e do aprimoramento de bases nominais e da integração entre os bancos de dados. Exemplos são os já citados Cartão Nacional de Saúde, que promove o cadastramento da população, e as aplicações da telemedicina e da telessaúde, que poderão fornecer informações de percurso do paciente pelos serviços de saúde e seu atendimento sem a necessidade de presença física do médico.[26]

É, portanto, importante que existam regras claras sobre o tratamento dos dados pessoais por essas iniciativas, sobretudo num contexto de tensão entre interesses públicos, coletivos e da indústria privada no âmbito do uso das TICs no SUS.[27] Moraes[28] adverte sobre a importância de se adotar um processo democrático emancipador em relação à implantação das tecnologias de informação para a saúde, o que inclui o estabelecimento de limites ao tratamento de informações pessoais dos pacientes, sob pena de os pobres terem os seus corpos esquadrinhados, de os indivíduos serem regulados e controlados em nome da garantia das suas qualidades de vida.[29].

---

21 DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006.

22 Ministério da Justiça. Anteprojeto de proteção a dados pessoais. Disponível em http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf

23 MAGRANI, Bruno et al. Relatório de Políticas Digitais http://www.cgi.br/publicacoes/livros/pdf/relatorio-politicas-internet-pt.pdf

24 MAGRANI, Bruno et al. Relatório de Políticas Digitais http://www.cgi.br/publicacoes/livros/pdf/relatorio-politicas-internet-pt.pdf

25 "Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais". Disponível em http://www.rets.org.br/?q=node/2313

26 MORAES, I. H. S. DE; VASCONCELLOS, M. M. 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.

27 SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

28 (Moraes, 2002)

Por tais razões, o tratamento de dados pessoais vêm sendo alvo de crescente regulação no exterior. Contudo, o Brasil ainda não possui uma lei de proteção de dados pessoais, a exemplo dos demais integrantes do G20[30].

A proteção da privacidade no país tem como base a Constituição Federal, que a inclui entre os direitos fundamentais, nos dispositivos que tratam da tutela da intimidade e da vida privada (art. 5o, inciso X) e da inviolabilidade da correspondência, do domicílio e das comunicações (art. 5o, incisos XI e XII).[31].

No âmbito infraconstitucional, o Código Civil (lei 10.406/2002) garante a proteção da vida privada do indivíduo (art. 21) e o Código de Defesa do Consumidor (lei 8.078/1990) regula a manutenção de bancos de dados e cadastros de consumidores, estabelecendo uma série de garantias a estes últimos.

O sigilo profissional também é tratado pela legislação. O Código Penal trata da divulgação de informações obtidas no exercício de atividade profissional, incluindo entre os tipos penais a revelação, sem justa causa, de segredo do qual se teve conhecimento em razão de função, ministério, ofício ou profissão, e cuja revelação possa causar dano a alguém (art. 154). Também é proibida ou desobrigada de depor a pessoa a respeito de fato que deva guardar sigilo profissional (Código de Processo Penal, Código de Processo Civil e Código Civil).

Na área da saúde, a privacidade e o sigilo de informações em saúde são abordadas por algumas normas setoriais e éticas.

O Código de Ética Médica (CEM) elenca, entre os seus princípios, o dever de sigilo profissional, salvo por motivo justo, dever legal ou consentimento do paciente; veda ao médico permitir o manuseio dos prontuários sob sua responsabilidade por pessoas não obrigadas ao sigilo profissional (art. 85); e proíbe também, durante o exercício da docência, a prática da medicina sem o consentimento do paciente e sem zelar por privacidade (art. 110).

A Agência Nacional de Saúde Suplementar (ANS) estabeleceu um padrão obrigatório para a troca de informações em saúde entre operadoras de planos privados de assistência à saúde e prestadores de serviço, que foi denominado Padrão TISS (Troca de Informações na Saúde Suplementar), atualmente estabelecido pela Resolução Normativa 305 (RN 305), de outubro de 2012. Um dos componentes desse padrão é o da segurança e privacidade, que prevê os requisitos para proteção dos dados de atenção à saúde, devendo seguir a legislação vigente.

Cabe mencionar que as normas existentes relacionadas a e-Saúde demonstram preocupação com a segurança e a privacidade das informações, como a portaria 2.073/2011, sobre o uso de padrões de informação em saúde e de interoperabilidade entre os sistemas de informação do SUS e para os sistemas privados e de saúde suplementar, e a Portaria 940/2011, que regulamenta o Sistema Cartão Nacional de

---

29 SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

30 "Lei de dados pessoais: Justiça promete reenvio de anteprojeto à Casa Civil.". Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32911&sid=97#.UbCQ1qU8hzo

31 A CF também assegura o direito de acesso do indivíduo às informações que lhe digam respeito e constem de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como a possibilidade de retificação desses dados (inciso LXXII). Esse remédio constitucional, chamado de habeas data, é disciplinado pela lei 9.507, de 12 de novembro de 1997. Vale mencionar que também se assegura o sigilo das informações obtidas no exercício da atividade profissional (inciso XIV).

Saúde, ambas do Ministério da Saúde. Enquanto a Portaria 2.073/2011 apenas coloca entre seus objetivos a promoção da utilização de uma arquitetura da informação em saúde de modo a permitir o compartilhamento de informações em saúde num meio seguro e com respeito ao direito à privacidade (art 2º, II), a Portaria 940/2011 especifica as regras para garantia do sigilo dos dados e das informações dos usuários SUS coletados pelo Sistema.

Também a PNIIS 2012, como mencionado, entende a importância da garantia da confidencialidade, sigilo e privacidade do que chama de "informação de saúde pessoal", identificando a necessidade do estabelecimento de um marco legal, normativo e organizacional relacionado à segurança e confidencialidade da informação.[32]

Tendo em vista a legislação existente sobre privacidade no país, percebe-se a importância de um marco regulatório que estabeleça de modo mais geral os limites para o tratamento de dados pessoais, sobretudo para as informações pessoais sensíveis e de saúde, e os direitos do titular desses dados. Esse seria um primeiro passo para se garantir a proteção da privacidade num momento em que se descobre o potencial das tecnologias da informação para a prestação de serviços, como em iniciativas de eSaúde.

Uma iniciativa que merece menção é o anteprojeto de lei (APL) de proteção aos dados pessoais, concebido pelo Ministério da Justiça e levado a discussão pública entre novembro de 2010 e abril de 2011. O anteprojeto regula o tratamento[33] de dados pessoais realizado em território nacional por pessoa física ou jurídica de direito público ou privado, estabelecendo os princípios gerais e requisitos para utilização desses dados.

O APL estabelece que, em regra, o tratamento de dados pessoais somente pode ocorrer mediante prévio consentimento livre e expresso do titular, o qual deve ser informado, entre outras questões, da finalidade da coleta e tratamento de seus dados, da difusão desses dados e de seus direitos como, por exemplo, o de se negar a fornecer tais dados.

O anteprojeto elenca alguns princípios gerais de proteção aos dados pessoais, entre eles:

- Princípio da finalidade: os dados pessoais somente podem ser alvo de tratamento compatível com as finalidades que fundamentaram a sua coleta e foram informadas ao titular.

- Princípio da necessidade: o tratamento dos dados pessoais deve ser limitada ao mínimo necessário, sobretudo quando a finalidade possa ser atingida com a utilização de dados anônimos ou com uso de meios que permitam a identificação do titular somente em caso de necessidade.

---

32 BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em: http://www.isc.ufba.br/arquivos/2012/Politica_Nacional_de_Informacao_e_Informatica_em_Saude.pdf.

33 O anteprojeto entende como tratamento "toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita a coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio e cancelamento de dados pessoais, bem como o seu fornecimento a terceiros por meio de transferência. comunicação ou interconexão".

- Princípio do livre acesso: o titular deve poder consultar gratuitamente os seus dados pessoais e as modalidades de tratamento dos mesmos.

- Princípio da proporcionalidade: o tratamento de dados pessoais deve ocorrer apenas quando houver relevância e pertinência em relação à finalidade para a qual foram coletados.

- Princípio da qualidade dos dados: exatidão dos dados pessoais alvo de tratamento.

- Princípio da transparência: o titular deve ser informado sobre os tratamentos de seus dados, como finalidade, quais dados foram tratados e tempo de conservação dos mesmos; o anteprojeto também exige o respeito da lealdade e da boa fé objetiva no tratamento das informações (princípio da boa fé objetiva).

- Princípios da segurança e da prevenção: utilização das medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados pessoais e às características específicas do tratamento a fim de proteger os dados de destruição, perda, alteração e difusão, tanto acidentais quanto ilícitas, bem como do acesso não autorizado. Ademais, tais medidas, sempre que possível, devem ser capazes de prevenir a ocorrência desses danos.

- Princípio da responsabilidade: deverão ser reparados os danos patrimoniais, morais, individuais ou coletivos causados aos titulares dos dados pessoais.

O anteprojeto possui normas específicas sobre dados sensíveis, categoria que inclui os dados de saúde. Por se tratarem de dados pessoais com potencial de gerar discriminação de seus titulares, os dados sensíveis encontram restrições para a sua inclusão em bancos de dados. O tratamento seria permitido em alguns casos, mediante prévio consentimento livre, informado e por escrito do titular, quando indispensável para o exercício legítimo das atribuições legais ou estatutárias do responsável pela utilização dos dados; quando for destinado a pesquisa histórica, científica ou estatística; quando for realizado por profissionais da área da saúde e for indispensável para a tutela da saúde do interessado; e quando for necessário para o exercício de funções próprias dos poderes de Estado.

Para a estrita observância das normas do anteprojeto é criada uma autoridade de garantia da proteção de dados pessoais. A autoridade é responsável por propor ações da política nacional de proteção de dados pessoais; receber e analisar consultas, denúncias e sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado referentes à proteção de dados pessoais; e aplicar sanções, medidas corretivas e preventivas para garantir a observância das normas e princípios do anteprojeto, entre outras medidas.

Os princípios e regras previstos no APL se coadunam com os requisitos legais e regulatórios estabelecidos em legislações dos Estados Unidos, Canadá e Europa a respeito da privacidade em ambientes de alta tecnologia. Segundo estudo da *Policy Engagement Initiative*, da *London School of Economics*, tais requisitos podem, inclusive, auxiliar na própria prestação dos serviços de saúde e na incorporação de

iniciativas de eSaúde, ajudando a garantir a integridade e acurácia informação médica presente nesses bancos de dados.[34]

4. Conclusão

Este artigo procurou apresentar brevemente um panorama das iniciativas de e-Saúde no Brasil, apontando as lacunas da legislação sobre privacidade em termos de proteção aos dados pessoais no âmbito da saúde. Os sistemas de eSaúde, um campo marcado pela diversidade de tecnologias e aplicações, envolve o tratamento de diferentes tipos de dados pessoais e para finalidades distintas.

Num momento em que se discute a implementação de iniciativas como o Cartão Nacional de Saúde, que inclui o registro eletrônico de saúde dos usuários dos sistemas de saúde, e a adoção de prontuários eletrônicos pelas unidades de saúde, é preciso que sejam acompanhadas de regras claras sobre o tratamento dos dados e informações de saúde. A portaria 940/2011 do MS possui dispositivos específicos sobre o sigilo das informações dos usuários vinculadas ao Cartão Nacional de Saúde, mas outras legislações são exigidas para regular o tratamento de informações pessoais de saúde em outras iniciativas.

É importante que as iniciativas e políticas de e-Saúde, como a PNIIS 2012, que já identificam a importância de um marco legal relacionado à segurança e à confidencialidade da informação, estejam integradas a outras iniciativas do próprio governo envolvendo a regulação das tecnologias de informação e comunicação e o tratamento de dados pessoais. Um marco normativo para proteção dos dados pessoais beneficiaria sem dúvida o setor da saúde ao prever princípios e regras que assegurem, por exemplo, que apenas as informações relevantes sejam coletadas e sejam armazenadas com o devido cuidado.

É claro, além das medidas legais, outras são igualmente primordiais para se garantir a privacidade dos pacientes no âmbito dos sistemas de eSaúde. Assim, a adoção de tecnologias baseadas em conceitos como *privacy-enhancing*, *privacy assessment impact* e *privacy-by-design,* e normas que regulem a nível profissional a confidencialidade e a privacidade das informações dos pacientes e usuários dos sistemas de saúde, inclusive com medidas de educação dos profissionais envolvidos no tratamento dos dados pessoais, podem ser úteis.[35]

5. Referências bibliográficas

BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em:http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_de_Informacao_e_Informatica_em_Saude.pdf

34 Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

35 Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010. http://www.cgi.br/publicacoes/ livros/pdf/relatorio-politicas-internet-pt.pdf

MAGRANI, Bruno et al. Relatório de Políticas Digitais. Disponível em http://www.cgi.br/publicacoes/livros/pdf/relatorio-politicas-internet-pt.pdf

Ministério da Justiça. Anteprojeto de proteção a dados pessoais. Disponível em http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf

MORAES, I. H. S. DE; VASCONCELLOS, M. M. 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.

REZENDE, E. J. C. et al. Ética e telessaúde: reflexões para uma prática segura. Rev Panam Salud Publica, v. 28, n. 1, p. 58–65, 2010.

SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

WHO. eHealth. http://www.who.int/topics/ehealth/en/

“Ceensp debate novos rumos para o Cartão SUS”. Disponível em http://www.ensp.fiocruz.br/portal-ensp/informe/site/materia/detalhe/24947

“Entidades médicas de SP temem quebra de sigilo em novo modelo de prontuário digital”. Disponível em http://veja.abril.com.br/noticia/saude/entidades-medicas-de-sp-temem-quebra-de-sigilo-em-novo-modelo-de-prontuario-digital

“Especialistas se reúnem em Brasília para a VI Oficina da E-Saúde”. Disponível em http://portal.saude.gov.br/portal/saude/profissional/visualizar_texto.cfm?idtxt=42509

“Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais”. Disponível em http://www.rets.org.br/?q=node/2313

“Lei de dados pessoais: Justiça promete reenvio de anteprojeto à Casa Civil.” Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32911&sid=97#.UbCQ1qU8hzo

“Paciente ganha prontuário unificado na rede do SUS paulista”. Disponível em http://www.saude.sp.gov.br/ses/noticias/2013/agosto/paciente-ganha-prontuario-unificado-na-rede-do-sus-paulista