Temas em Saúde Coletiva
18

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética

Instituto de Saúde
2015
São Paulo

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética

Instituto de Saúde
Rua Santo Antonio, 590 – Bela Vista
São Paulo-SP – CEP: 01314-000
Tel.: (11) 3116-8500
Fax: (11) 3105-2772
www.isaude.sp.gov.br

Secretaria de Estado da Saúde de São Paulo

Secretário de Estado da Saúde de São Paulo
David Everson Uip

Instituto de Saúde

Diretora do Instituto de Saúde
Luiza Sterman Heimann

Vice-diretora do Instituto de Saúde
Sônia I. Venancio

Diretora do Centro de Pesquisa e Desenvolvimento para o SUS-SP
Silvia Regina Dias Médici Saldiva

Diretor do Centro de Apoio Técnico-Científico
Márcio Derbli

Diretora do Centro de Gerenciamento Administrativo
Bianca de Mattos Santos

Coleção Temas em Saúde Coletiva
Volume 18 – Proteção à privacidade e acesso às informações em saúde:
tecnologias, direitos e ética
ISBN 85-88169-01-0 Coleção Temas em Saúde Coletiva
ISBN 978-85-88169-27-2

Tiragem: 2000 exemplares

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética

Organização: Tania Margarete Mezzomo Keinert, Flávia Mori Sarti, Carlos Tato Cortizo, Silvia Helena Bastos de Paula.

Edição: Márcio Derbli

Imagens da capa e contracapa: Marianne Nassuno (mnassuno@gmail.com)
Pinturas (sem nome), original acrílica sobre papel, tamanho 42 cm x 29 cm, 2012, fotografadas por Kell Motta.
Revisão, capa e tratamento de imagens: Imprensa Oficial do Estado de São Paulo

Projeto gráfico, editoração e impressão: Imprensa Oficial do Estado de São Paulo

Núcleo de Comunicação Técnico-Científica
Camila Garcia Tosetti Pejão

Administração
Bianca de Mattos Santos

Biblioteca
Carmen Campos Arias Paulenas

Dados Internacionais de Catalogação na Publicação – CIP
Biblioteca. Centro de Apoio Técnico-Científico. Instituto de Saúde

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética/organizado por Tânia Margarete Mezzomo Keinert... [et al]. São Paulo: Instituto de Saúde, 2015.
464 p. (Temas em saúde coletiva, 18)

ISBN: 978-85-88169-27-2

1. Privacidade 2. Confidencialidade 3. Direitos do Paciente 3. Ética 4. Tecnologia da informação/legis I. Keinert, Tânia Margarete Mezzomo, org. II. Série.

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética

Tania Margarete Mezzomo Keinert
Flávia Mori Sarti
Carlos Tato Cortizo
Silvia Helena Bastos de Paula
Organizadores

Instituto de Saúde
São Paulo - 2015

Sumário

Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética

Organização: Tania Margarete Mezzomo Keinert, Flávia Mori Sarti, Carlos Tato Cortizo, Silvia Helena Bastos de Paula

V Acesso às informações em saúde: transparência e participação social

VI Privacidade e Confidencialidade das Informações em Saúde: voluntariado, Documentação e Ética

Prefácio

Ilara Hämmerli Sozzi de Moraes[1]

> *"Eu, sentado na minha mesa, conseguia grampear qualquer pessoa. Você, seu contador, seu médico, um juiz federal, até o presidente se eu tiver o e-mail pessoal dele."*
>
> Edward Snowden (2014)

Relevância. Esta é a primeira ideia que surge ao conhecer a iniciativa de elaboração deste livro. O tema da privacidade constitui um dos grandes desafios do mundo contemporâneo. Impacta diretamente no projeto de democracia e de cidadania de um povo. A relevância da defesa da privacidade se agudiza no contexto de uma determinada forma de globalização que aprofunda desigualdades marcadas pela iniquidade entre pessoas, cidades e nações.

Ao longo do século passado, a ciência e a técnica ganham expressão e passam a ser cada vez mais utilizadas pelo mercado que se beneficia da conexão Ciência & Tecnologia (C & T). Nos últimos 30 anos, agrega-se o exuberante desenvolvimento das tecnologias de informação compondo as condições materiais necessárias ao 'coroamento' do processo histórico do atual modelo da globalização capitalista. Este se sustenta, por um lado, por disseminar a retórica de uma globalização que acolhe a diversidade, mas de fato se fortalece através de sutis e eficazes formas unitárias de pensar o mundo a partir do *modus operandi* dos países ricos do hemisfério norte.

O debate sobre a defesa da privacidade está imerso no contexto de uma globalização de agravamento das desigualdades, de desrespeito à vida digna e ao conceito pleno de cidadania. No entanto, ao mesmo tempo, eclodem forças, movimentos sociais, vozes, ideias, pensamentos que tencionam o *status quo* que se pretende permanente. A resultante dessa

1 Ilara Hämmerli Sozzi de Moraes (ilara@ensp.fiocruz.br) é Doutora em Saúde Pública pela Fundação Oswaldo Cruz e Pesquisadora Titular da Escola Nacional de Saúde Pública da Fundação Oswaldo Cruz, onde exerce, atualmente, a coordenação do Fórum de Informação, Comunicação e Tecnologia de Informação.

correlação de forças (manutenção ou mudança) orienta também os regimes informacionais atuais e o significado político, ético, social e econômico da privacidade em cada formação social das nações.

Em relação à Saúde, o tema da privacidade se reveste de especificidades, principalmente no Brasil, onde se constitui um direito universal e dever do Estado. Para além dos desafios técnicos, organizacionais e tecnológicos, suscita questões novas e ressuscita antigas, relacionadas às relações de poder e saber em disputa pela direcionalidade da política nacional de saúde, na qual se inclui a política de informação e tecnologia de informação em saúde.

Ameaças à privacidade no âmbito dos serviços de saúde não são novidades, apesar de sua problematização ter ingressado na agenda política a partir da segunda metade do século XX. Refletir sobre privacidade no âmbito da saúde revela o outro lado da moeda: o debate em torno dos limites entre a esfera pública e a esfera privada da vida em sociedade. Esta constatação tem como uma de suas principais fundamentações a análise da gênese da atual *práxis* informacional em saúde.

A lógica contemporânea de produção da informação em saúde surge no contexto histórico em que as questões relativas à vida e à morte de uma população adquirem relevância política e social: tornam-se eventos que justificam seu monitoramento, sua visibilidade, sua vigilância através de dispositivos de Estado, conforme descritos por Foucault (1980, 1982), no exercício de um biopoder (1988). Esse processo vincula-se às transformações políticas, sociais, econômicas, científicas e tecnológicas decorrentes da formação do Estado Moderno, em um crescente processo de urbanização e de organização da sociedade capitalista. Como parte constitutiva desse momento histórico (final do século XVIII e início do século XIX), o Estado Moderno estabelece dispositivos de atuação voltados para a gestão da vida, que permitem o exercício de um poder disciplinar que se expressa capilarmente em todo o campo social, de um biopoder, que nasce imerso na constituição de uma sociedade panóptica (MORAES, 2002).

No mesmo período, observa-se a ruptura da medicina clássica para a medicina moderna, com o pensamento anátomo-clínico e patológico: é o nascimento da Clínica (FOUCAULT, 1980). A Doença adquire um novo significado e passa a ser corporificada no indivíduo. As informações em saúde,

nos moldes como se expressam até os dias atuais, consolidam-se como um dos instrumentos estratégicos dessa transformação, "*ao amplificar, paulatinamente, o 'olhar do médico' sobre os sinais e sintomas do corpo do paciente para o 'olhar dos aparelhos de Estado' sobre os 'corpos das populações, constituindo-se em espaço de disputas de relações de poder e produção de saber. Neste esforço, firma-se, enquanto analítica central, o poder. Não qualquer poder, mas o poder vigilante que institucionaliza as informações em saúde como parte integrante dos dispositivos políticos de atuação do Estado Moderno de controle/monitoramento da população* (MORAES e GOMEZ, 2007)."

A análise da construção histórica da 'informação e informática em saúde' evidencia a miríade de interesses em disputas ao longo desse processo. Observam-se as diferentes concepções de Saúde, de Política de Saúde e de Privacidade em busca de hegemonia em cada conjuntura histórica específica, o que inclui as opções em torno das tecnologias de informação adotadas, resultantes da pressão do mercado da computação e das telecomunicações (MORAES e GÓMEZ, 2007).

A depender das relações de poder e saber, as 'soluções' para ameaças à privacidade são desenvolvidas e implementadas com variações sobre a prioridade na alocação de recursos, ora com maior ênfase no *apparatus* tecnológico, ora nas telecomunicações, ora em padrões de segurança, mas dificilmente na formação de uma cultura ética institucional e profissional de respeito à privacidade do outro, no caso aqui, o cidadão no gozo de seu direito à Saúde.

A racionalidade de um Estado vigilante, no âmago de uma sociedade panóptica, *vis a vis* a defesa intransigente da privacidade do indivíduo definem os limites entre interesses da esfera pública e da esfera privada. Na dimensão pública, deve prevalecer os interesses da coletividade, do dever do Estado em garantir saúde universal, o que demanda mecanismos de gestão e o desenvolvimento de C & T em Saúde cada vez mais complexos. Na dimensão privada, deve prevalecer o direito do indivíduo de ter preservada sua privacidade e a confidencialidade dos dados sobre sua Saúde, cabendo ao Estado a obrigação de garanti-las, através de Políticas competentes não só de segurança da informação, como também do respeito à cidadania de cada ser humano.

Ao longo do tempo, as nações precisam responder: Até onde vai o direito do Estado, da Ciência e da Tecnologia da Informação (TI) em conhecer e usar aspectos da vida íntima das pessoas em nome da coletividade e da defesa da segurança pública? Até onde vai o direito do cidadão em preservar a privacidade? As fronteiras não são claras, ainda há imensas zonas de nebulosidade. E vislumbra-se o acirramento das tensões e ameaças à privacidade na medida em que os mecanismos de vigilância se tornam cada vez mais complexos, decorrentes em grande medida do avanço das TI, no contexto de expansão (eficaz e perversa!) da cultura política, social e ética do medo, produzindo lucros astronômicos para as empresas de segurança, onde se destacam as de tecnologia de informação.

O marco histórico de radicalização da racionalidade panóptica, surgida no final do século XVIII na formação do Estado Moderno capitalista, encontra-se no atentado terrorista de 11 de setembro de 2001 em Nova York/EUA. A partir daí, expande-se pelo planeta a busca por legitimidade da retórica e das ações que definitivamente violam a privacidade, desrespeitam a autonomia do indivíduo e da coletividade e ameaçam à liberdade e à democracia das nações. Consolida-se, como política do governo americano e de "seus aliados", a Guerra ao Terror.

No bojo da tensão entre ameaça *versus* defesa da privacidade, surgem reações, já inscritas no panteão dos marcos da história contemporânea, como o WikiLeaks[2] e as denúncias de Edward Snowden[3], dentre as quais as revelações acerca da violação da autonomia das pessoas e dos países praticada pela Aliança dos Cinco Olhos (The Five Eyes Alliance: EUA, Canadá, Inglaterra, Austrália e Nova Zelândia).[4]

2 WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página (site), postagens (posts) de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. Lançado em dez/2006, seu principal editor e porta-voz é o australiano Julian Assange, jornalista e ciberativista. (Wikipédia, 20/04/2015)

3 Edward Snowden (1983) é analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana. Forneceu detalhes da Vigilância Global de comunicações e tráfego de informações executada através de vários Programas, entre eles o programa de vigilância PRISM dos Estados Unidos. (Wikipédia, 20/04/2015).

4 The Five Eyes Alliance refere-se à aliança entre cinco países (USA, Austrália, Canadá, Nova Zelândia e Reino Unido) voltada para ações e cooperação em inteligência. Suas origens conhecidas datam da 2ª. Guerra Mundial, mantendo-se no decorrer da guerra fria, com o desenvolvimento de sistema de vigilância de monitoramento das comunicações privadas e de países em todo o mundo. A partir de 2001, expande sua capacidade de vigilância com ênfase sobre a Internet. Para Snowden, os 'cinco olhos' são uma "*organização supranacional de inteligência que não responde às leis conhecidas de seus próprios países*". (Wikipédia, 20/04/2015)

Ao ser eleito Reitor da Universidade de Glasgow (2014), Snowden emitiu um comunicado em que afirma: "*Se não contestar a violação do direito fundamental de pessoas livres de não serem molestadas em seus pensamentos, associações e comunicações – de serem livres de suspeita, sem causa – teremos perdido a base da nossa sociedade pensante. A defesa dessa liberdade fundamental é o desafio de nossa geração, um trabalho que exige a criação de novos controles e proteções para limitar os poderes extraordinários de Estados sobre o domínio da comunicação humana*" (Wikipédia, 20/04/2015).

O contexto atual do debate em torno da privacidade de indivíduos é o da vigilância global no âmbito do g*lobalitarismo*, na formulação de Milton Santos (2000). Não se trata mais de uma ameaça à privacidade, mas sim da sua violação efetiva, sem o livre e esclarecido consentimento do cidadão. O limite ao direito do Estado, da Ciência e da Tecnologia da Informação (TI) em conhecer e usar informações das pessoas vem se diluindo paulatinamente pela quase onipresença planetária da racionalidade panóptica *pari passu* à difusão de um discurso único, em uma perigosa aproximação ao que aparece no romance de Ray Bradbury de 1953: *Fahrenheit 451*. Neste livro, Bradbury apresenta um futuro onde o pensamento crítico é suprimido.

Aliás, cabe lembrar como a arte já denunciava o risco da sociedade panóptica ainda em 1932, quando Aldous Huxley publicou *Admirável mundo novo*; ou ainda em 1949, com a publicação do livro *1984* de George Orwell. Neste, o autor cria o personagem fictício Big Brother, o 'Grande Irmão' que expressa a vigilância onipresente para zelar pela paz de todos! Na sociedade descrita por Orwell, todas as pessoas estão sob constante vigilância. A obra *1984* transforma-se em um arauto dos tempos da vigilância global, que se expressa capilarmente nas sociedades através do GPS dos carros e dos celulares, nas câmaras de segurança dos elevadores e shopping, no rastreamento do uso dos cartões de crédito... no uso do cartão nacional de saúde (?).

No Brasil, como dimensões agravantes dessa realidade, cabe destacar que permanece incipiente o debate político na sociedade sobre o tema da privacidade, mesmo após o profícuo processo de elaboração do Marco Civil da Internet, que culminou com sua aprovação

através da Lei Nº 12.965, sancionada pela presidente Dilma Rousseff em abril de 2014.

Outro agravante expressa-se no SUS (Sistema Único de Saúde), conforme descrito pela pesquisadora da FGV, Sonia Fleury: *"As articulações entre público e privado [*aqui utilizado para referir-se ao setor econômico empresarial*] já não representam enfrentamentos de interesses, representam a canalização dos interesses privados para o interior de um sistema público que se fragiliza, por isso mesmo, cada vez mais. Hoje, ninguém quer acabar com o SUS, todos querem fortalecê-lo para tirar dele o maior proveito, sejam eles grupos empresariais, industriais, seguros, corporações, políticos, ..."* (p.5) (FLEURY, 2011). Dentre os quais observa-se a confluência de interesses entre o complexo econômico industrial da saúde e o complexo econômico industrial de TI e Telecom na Saúde diante do avanço das ações denominadas pela OMS como *e-health*.

O complexo painel aqui delineado da contemporaneidade determina a urgência por ampliar a participação da sociedade na produção de respostas a questões como: Qual o papel do Estado na relação público – privado? Qual o significado da Democracia no Estado Panóptico e do *Big Data*? Qual o papel do indivíduo na Sociedade Panóptica e do Big Data? Será que os movimentos sociais só atuam ao perderem a "confiança" no *establishment* ao serem diretamente afetados, com prejuízos pessoais ou aos familiares? Afinal, quais são os limites entre os interesses da esfera pública e os da esfera privada da vida? Quem e como se definem os limites entre estes interesses?

As respostas atuais a estas questões, resultantes da correlação de forças dos interesses políticos, econômicos, sociais, científicos, tecnológicos, culturais e simbólicos, tecem a contextura da Governança da informação e das tecnologias de informação em saúde, nas três esferas de governo, com reflexos sobre a privacidade e o uso de dados pessoais e corporais.

Os avanços tecnológicos e a interoperabilidade entre grandes bancos de dados (*big data*) na Saúde, compostos por bases nominais (identificação do cidadão), ampliam o potencial de novas ameaças à privacidade e à confidencialidade das informações fornecidas, em confiança, pelos cidadãos aos profissionais e estabelecimentos de saúde. No SUS, essas ameaças se intensificam a depender dos desdobramentos de algu-

mas iniciativas, tais como: Cartão Nacional de Saúde, e-Saúde, Prontuário Eletrônico do Paciente, Centrais de Regulação e Telessaúde.

Configuram-se como ações que abrem um leque de possibilidades há muito almejado por seu potencial para a melhoria da qualidade na atenção à saúde. No entanto, permitem o rastreamento do percurso do cidadão pelos serviços de saúde (públicos ou privados), potencializando riscos de invasão à privacidade e violação da confidencialidade, princípios éticos fundamentais na relação do cidadão com os profissionais e serviços de saúde.

Ocorrem inúmeras ações que tornam vulneráveis a privacidade de pacientes. A título de exemplo, cita-se o caso, noticiado pelo New York Times, ocorrido no New York-Presbyterian Hospital. Em 2010, dados clínicos de 6,8 mil pacientes tornaram-se acessíveis por mecanismos de buscas na internet. Informações como nome, idade, situação clínica, cirúrgica, pulso e temperatura estavam disponíveis no ciberespaço. Segundo o New York Times, o erro foi descoberto no início de julho/2010, somente após a denúncia de parentes de um paciente que encontraram informações sobre ele na internet. Cabe destacar que o problema só foi tornado público por causa da investigação do caso.

Enfim, para o bem ou para o mal, constata-se que não existe mecanismo de segurança 100% garantido! Isso vale tanto para os dispositivos de vigilância (vide WikiLeaks e Snowden), quanto para a garantia constitucional da inviolabilidade da intimidade de um cidadão. Requer reflexões críticas e propositivas permanentemente diante da vigilância exercida por autoridades e/ou por empresas de TI/segurança, uma vez que na grande maioria dos casos em que foram detectadas violações de privacidade, os sistemas de informação utilizados incluíam as tecnologias de segurança preconizadas. Ou seja, as violações ocorreram não por falta de dispositivos de segurança!

Levantamento bibliográfico, realizado nas bases de dados MEDLINE via PubMed, Scielo e Web of Science, no período de 2000 a 2014, sobre violação de privacidade em ambientes hospitalares, evidenciou que, não apenas no Brasil como também em outros países, as normas, os regulamentos e os mecanismos de segurança são fundamentais, mas por si só têm se mostrado insuficientes para a preservação do direito à privacidade. Então, o que fazer?

Para superar este desafio, além do contínuo aprimoramento do que já se utiliza, estão em construção diferentes alternativas, não necessariamente excludentes. No entanto, ainda persiste a pouca ênfase em ações dedicadas ao componente humano presente na relação profissional/estabelecimento de saúde e o cidadão/paciente.

Nesta direção, cabe refletir sobre possíveis estratégias de fomento a processos de comprometimento político-ético da equipe (tanto de saúde quanto de tecnologia da informação) em torno da vontade e da compreensão sobre a importância da privacidade para a qualidade da vida em sociedade.

Óbvio que ações voltadas para o estabelecimento de compromissos da equipe de saúde com a privacidade não produz lucro ao complexo econômico industrial de TI e Telecom, focado na venda de seus produtos e serviços de segurança. Talvez esse fato se configure como uma das principais hipóteses explicativas para que a defesa da privacidade ocorra majoritariamente vinculada a mecanismos associados à hardware e software de segurança, barreiras físicas, treinamentos pontuais.

Por outro lado, observam-se avanços referidos ao arcabouço jurídico, normativo, institucional e deontológico das profissões de saúde. Entretanto, a matriz gnosiológica baseia-se na punição através de penalidades, caso a violação da privacidade seja denunciada. Ou seja, impera a lógica de um agir *post factum* ou, no dito popular, depois que o leite foi derramado. Certamente, não está sendo proposta a impunidade ou mesmo a desvalorização de avanços normativos. Pretende-se, tão somente, destacar que mecanismos de segurança e arcabouço jurídico-institucional são necessários, mas estes sozinhos têm se mostrado insuficientes.

Talvez se deva problematizar a racionalidade que perpassa historicamente as 'respostas' de defesa da privacidade: Há um princípio comum subjacente de dúvida sobre a prática do Outro, de que não há como 'confiar' no outro, visto como potencial violador de normas e padrões. Por conseguinte, resta apenas criar obstáculos, dificuldades de acesso, controlar e punir o infrator. Este caminho parece não contribuir para um projeto civilizatório calcado na ética da responsabilidade, proposta por Hans Jonas ainda em 1974 (JONAS, 1974). Neste sentido, pode se afirmar que a

ação humana continua a demandar novas vias sobre como construir seu futuro global e local.

A ética põe em relevo a questão da conduta a seguir num mundo complexo. Destaca a importância de se refletir sobre o impacto das mudanças tecnológicas, em especial as decorrentes das tecnologias de informação, para saber se contribuem para a emancipação e o respeito à dignidade do ser humano de forma universal e equânime. Esta agenda política-ética pressupõe o estabelecimento de novos pactos em torno de compromissos éticos para com a defesa da privacidade, da confidencialidade da informação, do controle dos aparelhos de Estado sobre o cidadão, novos pactos de governança sobre as relações entre a esfera pública e a esfera privada da vida. Compromissos éticos que se expressem em mudanças na gestão informacional e, por conseguinte, em 'soluções' novas no *modus faciendi* de respeito à privacidade.

A tecnologia pode ser temida tanto pelos seus sucessos e avanços quanto pelos seus fracassos. Quando Jonas (1974) propõe uma ética baseada no conceito da responsabilidade, parte da ideia de que o poder da tecnologia cria problemas éticos desconhecidos até então. Portanto, os preceitos antigos não podem mais dar conta. Enfrentar os desafios que emergem da intervenção tecnológica contemporânea requer mudanças em racionalidades que, até então, orientam a ação humana. Mudanças que ampliem as condições materiais de participação consciente, livre e esclarecida da população acerca dos limites que as pessoas consideram como aderidos a um projeto civilizatório calcado no respeito à vida digna (AGAMBEN, 2002), universal e equânime, respondendo: Até onde, como e quando o Estado deve "saber e controlar" a vida do cidadão e da sociedade e estes devem "saber e controlar socialmente " o aparato estatal?

O desafio é trabalhar, por exemplo, cada local de trabalho (um centro de saúde, um hospital, uma secretaria municipal ou estadual de saúde) como espaço de possibilidades criativas de mudanças que culminem no estabelecimento de um Pacto Ético e Político que expresse o VALOR atribuído, pela equipe de saúde, à Vida, ao outro (seu paciente), em um mundo globalizado. A formulação desse desafio adota o entendimento de que o local onde se vive e trabalha é expressão do contraponto glo-

bal/local, no mundo globalizado (MORAES, 2002; IANNI, 1996 a, 1996 b; SANTOS, 1996).

A matriz de pensamento que fundamenta essa proposição tem por princípio que a construção de um projeto civilizatório emancipador se trava no cotidiano, na ação local, que se expande para o global, difundindo novas possibilidades de vida. Considera que o respeito à privacidade é requisito para a existência de uma sociedade mais respeitosa para com o outro e para si próprio enquanto nação justa, fraterna e digna (MORAES, 2002).

Por isso, cada ação local se constitui em locus fecundo no qual sujeitos singulares e coletivos problematizem suas insatisfações, dúvidas e necessidades de mudanças que passam a ter um significado estrutural, dinâmico e estratégico se marcadas pela responsabilidade com as consequências das ações de cada um sobre o outro e o coletivo. No exercício dessa construção político-ética, os cidadãos compreendem que são produtos e agentes de uma situação histórica, da sua atualidade, cuja característica central é ser mutável. Afinal, as contradições nunca se resolvem, desenvolvem-se, lançam-se em outros níveis, abrem outras perspectivas, pois, quanto mais global for o problema, mais locais e mais multiplamente locais devem ser as 'soluções'.

Em síntese, afirma-se que nenhuma ação isoladamente garantirá, com efetividade, o respeito a limites entre a dimensão pública e privada. Estes limites são historicamente definidos a partir de pactos políticos e éticos orientadores da governança dos Estados em sua relação com a sociedade. Lembrando que ainda é preciso ser incorporado, à cultura institucional do SUS, o princípio de que as informações fornecidas pelo cidadão em seu contato com o sistema de saúde são dele e não da instituição, da equipe ou do médico, independentemente do suporte tecnológico utilizado.

Considerar os dados pessoais e corporais fornecidos pelo indivíduo como DELE alarga o papel e a função do cidadão na sociedade. Ele decide, conscientemente, sobre a destinação das informações que lhe dizem respeito. Um dos possíveis mecanismos de operacionalização desse princípio é a institucionalização, nos serviços de saúde, do consentimento li-

vre e esclarecido em relação ao acesso e uso dos dados nominais e corporais fornecidos na relação com a equipe de saúde: o cidadão passa a deter o controle sobre os termos da autorização (MORAES, 2014).

A conclusão a que se chega é que sem um conjunto de iniciativas políticas, éticas e tecnológicas voltadas para o respeito à privacidade do cidadão, ampliam-se as condições de um "ambiente de risco" para o projeto de uma nação que preserve o valor da vida. Trata-se de um projeto civilizatório para uma nova globalização.

Nada parece mais difícil que a construção da solidariedade, em tempos de globalização, massificação, individualismo, competitividade ... Mas, sempre há os que não se acomodam. São sujeitos sociais, heterogêneos entre si, que de diferentes modos e em suas múltiplas trincheiras vêm conferindo espessura política ao enfrentamento dos problemas, às reivindicações, promovendo ligações entre as suas manifestações locais em diferentes partes do mundo. Eles estão tecendo uma rede de solidariedade e esperança envolvendo o planeta Terra, fincando as bases materiais, as interlocuções, as relações de poder e produção de saberes em torno de interesses que, sem negar a importância das lutas pelo bem-estar pessoal, defendem pactos transnacionais e transgeracionais, procurando (re)elaborar coletivamente nossas realidades, apesar da existência de forças centrífugas na economia globalizada.

> *"Daí a relevância da política, isto é, da arte de pensar mudanças e de criar as condições para torná-las efetivas. Aliás, as transformações que a história ultimamente vem mostrando permitem entrever a emergência de situações mais promissoras. Podem objetar-nos que a nossa crença na mudança do homem é injustificada.*
>
> *E se o que estiver mudando for o mundo?*
>
> *Estamos convencidos de que a mudança histórica em perspectiva provirá de um movimento de baixo para cima, tendo como atores principais os países subdesenvolvidos e não os ricos; os deserdados e os pobres e não os opulentos e classes obesas; o indivíduo liberado partícipe das novas massas e não o homem acorrentado; o pensamento livre e não o discurso único".*
>
> *(Santos, 2000).*

Referências

AGAMBEN, G. **Homo Sacer: o poder soberano e a vida nua**. Belo Horizonte: UFMG, 2002

FLEURY, S. Defesa intransigente do interesse público na saúde. In: SIMPÓSIO DE POLÍTICA E SAÚDE, 2., 2011, Brasília. p. 4-6. Disponível em: <http://cebes.org.br/site/wp-content/uploads/2011/07/CEBES_Teses.pdf>. Acesso em: 18 dez.2013.

FOUCAULT, M. **História da sexualidade I: a vontade de saber**. Rio de Janeiro: Graal, 1988.

FOUCAULT, M. **Microfísica do poder**. Rio de Janeiro: Graal, 1982.

FOUCAULT, M. **O nascimento da clínica**. Rio de Janeiro: Forense-Universitária, 1980.

IANNI, O. **A sociedade global**. Rio de Janeiro: Civilização Brasileira, 1996a.

IANNI, O. **Teorias da globalização**. Rio de Janeiro: Civilização Brasileira, 1996b.

JONAS, H. **Philosophical essays. From ancient creed to technological man**. Chicago: The University of Chicago, 1974.

MORAES, I.H.S. **Política, tecnologia e informação em saúde:** a utopia da emancipação. Salvador: UFBA/ Casa da Qualidade, 2002.

MORAES, I.H.S. Sistema de Informações em Saúde: patrimônio da sociedade brasileira. In: PAIM, Jairnilsom S; ALMEIDA-FILHO, Naomar (Org). **Saúde Coletiva**: teoria e prática. Rio de Janeiro: MedBook, 2014. p. 649-665.

MORAES, I.H.S.; GÓMEZ, M.N.G. Informação e informática em saúde: caleidoscópio contemporâneo da saúde. **Ciência & Saúde Coletiva**, v.12, p.553-565, 2007. Disponível em: <http://www.scielo.br/pdf/csc/v12n3/02.pdf ou http://www.scielo.br/pdf/csc/v12n3/08.pdf >. Acesso em: 19 set. 2013.

SANTOS, B.S. **Pela mão de Alice. O social e o político na pós-modernidade**. São Paulo: Cortez, 1996.

SANTOS, M. **Por uma outra globalização:** do pensamento único à consciência universal. São Paulo: Record, 2000.

Introdução

Tania Margarete Mezzomo Keinert[1]
Flávia Mori Sarti[2]
Carlos Tato Cortizo[3]

O contexto atual de célere desenvolvimento tecnológico traz a necessidade de aprofundamento do debate sobre **Proteção à Privacidade e Acesso às Informações em Saúde**, considerando múltiplos aspectos que tangenciam difusão de tecnologias e garantias de direitos com uma abordagem ética na interface entre áreas de conhecimento aparentemente distantes entre si. A intensificação do uso de redes digitais na intermediação da troca de informações pessoais representa um conjunto de novos desafios para proteção à privacidade. Simultaneamente, há ampliação do acesso à informação por meio da busca de transparência nos dados relativos ao setor público. Isso resume alguns dos principais aspectos que justificam um esforço para reunir especialistas e estudiosos de diferentes campos de pesquisa na produção de uma reflexão abrangente sobre proteção à privacidade, sistematizada no presente livro.

A obra também busca discutir outras dimensões da privacidade como uma questão que permeia a totalidade da sociedade, ressaltando relações entre individual e coletivo dentro do quadro da organização do poder político, desde o contexto de governos até grandes corporações, onde infraestrutura de troca de informação representa um dos componentes fundamentais hoje.[4]

---

1 Tania Margarete Mezzomo Keinert (taniak@isaude.sp.gov.br) é administradora pública e bacharel em Direito, Mestre e Doutora em Administração Pública pela FGV/SP com pós-doutorado em Gestão de Qualidade de Vida na Universidade do Texas/Austin (EUA) e Pesquisadora Científica IV do Instituto de Saúde.

2 Flávia Mori Sarti (flamori@usp.br) é Bacharel em Economia pela Faculdade de Economia, Administração e Contabilidade (FEA-USP) e Nutrição pela Faculdade de Saúde Pública (FSP-USP). Doutora em Nutrição Humana Aplicada (PRONUT-USP), Pesquisadora do Núcleo de Pesquisas em Estudos Interdisciplinares de Sistemas Complexos da Universidade de São Paulo (NISC-USP) e Docente da Universidade de São Paulo.

3 Carlos Tato Cortizo (tato@isaude.sp.gov.br) é graduado em Processamento de Dados pela Faculdade de Tecnologia de São Paulo do Centro Estadual de Educação Tecnológica Paula Souza, Mestre em Saúde Pública pela Faculdade de Saúde Pública da Universidade de São Paulo e Assistente Técnico de Pesquisa Científica e Tecnológica do Instituto de Saúde.

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

A privacidade, a confidencialidade e o sigilo das informações dos cidadãos tornam-se temas relevantes, também, para as organizações internacionais. A Organização das Nações Unidas vem, neste momento, mais especificamente em sua 28ª. Sessão Ordinária Conselho dos Direitos do Homem, realizada neste ano de 2015, discutir a adoção de um relator especial para o Direito à Privacidade.[5]

A importância do presente livro no setor de saúde (em geral) e no Sistema Único de Saúde (em particular) reside na apresentação de um conjunto de reflexões e conhecimentos para subsidiar debates nos Conselhos de Saúde sobre proteção à privacidade de informações dos pacientes que trafegam na Internet, nos meios digitais e em bases de dados organizacionais. A questão tornou-se progressivamente relevante aos profissionais de saúde, pois envolve questões de natureza política e ética, além de aspectos técnicos e jurídicos. Tendo em vista que equipes de saúde multidisciplinares lidam cotidianamente com dados pessoais dos pacientes, bem como sistemas de informações em nível populacional, a preocupação com privacidade deve envolver profissionais de níveis administrativos e técnicos, indistintamente.

A privacidade, o sigilo e a confidencialidade das informações em saúde constituem temas de vital importância igualmente aos pacientes usuários dos sistemas de saúde, uma vez que são proprietários dos dados disponibilizados às instituições de saúde, ao contrário do que é imposto por noções equivocadas sobre direitos à informação e benefícios dos sistemas de saúde, especialmente no setor público. Note-se que dados dos indivíduos, além de serem informações pessoais, via de regra são também dados sensíveis.[6]

---

5 Vide projeto de resolução **O direito à privacidade na era digital**, apresentado por Brasil e Alemanha, que teve copatrocínio de 64 países, disponível em: http://www.brasil.gov.br/governo/2014/11/onu-adota-proposta-feita-por-brasil-e-alemanha-para-garantir-privacidade-na-internet Também é interessante a **Resolução do Parlamento Europeu**, na qual CDHONU é exortado a prosseguir o debate sobre direito à privacidade e, consequentemente, designar um relator especial (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-2015-0232+0+DOC+XML+V0//PT). Ainda no mesmo tema, foi realizada declaração oral por 92 entidades civis de vários países que apoiam a **Chamada para estabelecer um Relator Especial da ONU sobre o direito à privacidade** (http://www.nupef.org.br/?q=node/119).

6 O anteprojeto de lei de proteção de dados pessoais (atualmente sob consulta pública em plataforma digital no site do Ministério da Justiça) classifica dados pessoais e dados sensíveis em seu artigo 4º da seguinte forma: **Dados Pessoais:** "qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores" (Inciso I); e **Dados Sensíveis:** "dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos e biométricos" (Inciso IV). Disponível em: <http://www.acessoainformacao.gov.br/menu-de-apoio/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf> Acesso em: 11.03.2015.

Destaque-se, ainda, a importância da correta adoção e utilização do Termo de Consentimento Livre e Esclarecido (TCLE) dentro do contexto de pesquisas na área da saúde, como instrumento de proteção da privacidade e promoção da autonomia decisória dos cidadãos participantes de estudos envolvendo seres humanos. A coleta e o uso da informação para fins de avanços na ciência não têm precedência em relação à necessidade de esclarecer sujeitos de pesquisa quanto a riscos e benefícios de intervenções em saúde, assim como no que tange ao direito de escolha em participar (ou desistir de participar a qualquer momento) da pesquisa.

A informatização afeta sobremaneira diversas atividades de processamento das informações em saúde; como, por exemplo, registro de dados nos prontuários dos pacientes, que incluem conjuntos de informações sobre determinada pessoa. O fato de registros em prontuários de pacientes em papel serem abandonados em favor de uma coleta e processamento eletrônico resulta em mudanças substanciais no acesso e no tratamento das informações digitalizadas, podendo gerar fragilidade na proteção da privacidade.

A premissa fundamental de regulamentação da interface entre comportamento ético e prontuário do paciente postula manutenção dos deveres dos profissionais de saúde em qualquer meio de registro dos dados, vale dizer, permanecem inalteradas normas de conduta previstas para prontuário médico registrado em papel após migração dos sistemas de informação em saúde para prontuário eletrônico.

Dentro do contexto das informações em saúde, há aspectos sensíveis ao paciente que devem ser considerados no processo de conversão de prontuários médicos em prontuários eletrônicos. Se, por um lado, sistemas de informação em saúde permitem avanços históricos no acesso à saúde para indivíduos em regiões de difícil acesso, incluindo possibilidades de colaboração à distância entre equipes de saúde para elaboração de diagnósticos mais precisos; por outro lado, há também riscos relativos à invasão dos sistemas de informação para obtenção de dados pessoais e disseminação indiscriminada de informações em saúde com potenciais prejuízos sociais e econômicos ao paciente e às organizações de saúde envolvidas.

O prontuário eletrônico do paciente (PEP), como qualquer inovação tecnológica, apresenta aspectos positivos (como promoção de eficiência no atendimento ambulatorial ou hospitalar e transferência interinstitu-

cional de dados importantes à gestão e operacionalização dos serviços de saúde) e aspectos negativos (como resistência dos profissionais de saúde à adoção do PEP ou possibilidade de infrações éticas no uso de informações pessoais). Entretanto, trata-se de uma nova fronteira para avanços na gestão da assistência em saúde para promoção da equidade no acesso e uso dos serviços de saúde, dada a atual velocidade de disseminação das tecnologias de informação e comunicação.

Tendo em vista a complexidade e a atualidade da temática, não há pretensão de esgotar o debate em torno do assunto no contexto do presente livro. Tampouco há anseio de trabalhar conceitos unívocos e lineares. Pelo contrário, as perspectivas de análise são pluralistas e interdisciplinares, constituindo-se em uma contribuição inicial à abordagem do objeto em estudo. Alguns conceitos são retomados em diferentes capítulos, de forma a permitir tanto uma leitura pontual quanto uma fonte de consulta contínua, quando necessário.

A organização do sumário por eixos temáticos, por outro lado, buscou aglutinar temas dos capítulos para servir como um guia ao leitor. Ainda assim, procurou-se utilizar uma abordagem dedutiva, partindo de aspectos mais gerais para temas específicos; no entanto, é importante destacar que isto foi realizado de forma parcial, uma vez que cada capítulo tem, em seu início, uma abordagem geral e introdutória do tema tratado.

A presente obra é destinada a quaisquer cidadãos interessados no tema da Proteção à Privacidade e Acesso às Informações em Saúde, não sendo dedicada exclusivamente para técnicos e especialistas, tendo em vista que fornece uma primeira aproximação à discussão da garantia dos direitos individuais de preservação das informações pessoais em saúde, face à contínua difusão de tecnologias de acesso e comunicação de dados.

No intuito de auxiliar a leitura, os capítulos foram elencados em seis partes:

I Privacidade e Confidencialidade das Informações em Saúde: Dimensões e Perspectivas
II Proteção à Privacidade das Informações em Saúde e Direitos
III Segurança das Informações, Privacidade e Informática em Saúde

IV Prontuário Eletrônico do Paciente: Ponderações Técnicas e Éticas
V Acesso às Informações em Saúde: Transparência e Participação Social
VI Privacidade e Confidencialidade das Informações em Saúde: Voluntariado, Documentação e Ética

Toda a complexidade desta temática exige que nos debruçamos sobre as questões informacionais, políticas e sociais suscitadas pela necessidade de dar a devida atenção à importância dos temas da proteção à privacidade, da garantia do sigilo e da manutenção da confidencialidade das informações em saúde, sempre entendidas em seus aspectos de segurança e de tecnologia, jurídicos e de sua defesa como direito, e, especialmente éticos, tanto numa perspectiva individual, profissional, corporativa ou social.

Esperamos que tenham todos uma excelente leitura e estamos à disposição para realizar parcerias, debates, encontros e cursos de formação sobre a temática.

I

Privacidade e confidencialidade das informações em saúde: dimensões e perspectivas

1

Privacidade das informações em saúde e privacy concerns: uma temática multifacetada e interdisciplinar

Edimara Mezzomo Luciano[1]
Rodrigo Hickmann Klein[2]
Vergilio Ricardo Britto-da-Silva[3]

Luiza trabalhava na administração de uma grande empresa e estava tomando café em uma cafeteria de um shopping center. Na mesa ao lado um homem desconhecido faz uma ligação pelo celular, pedindo para chamar uma mulher, com nome e sobrenome repetido algumas vezes. Tratava-se de um nome incomum, porém Luiza sabia quem era, pois era o nome de uma das suas funcionárias. A ligação destinava-se à marcação de uma consulta médica para o dia seguinte, pois o resultado de um exame tinha chegado e a situação não estava nada boa, e as piores expectativas tinham se materializado. Alguns minutos depois chega uma antiga amiga deste desconhecido, menciona o nome dele e dentre outros assuntos pergunta sobre as cirurgias que ele tem realizado. Agora Luiza já tinha as informações necessárias para deduzir que a sua funcionária estava com câncer, pois o homem desconhecido era um médico oncologista.

(Situação hipotética ilustrativa, baseada em fatos reais).

1 Edimara Mezzomo Luciano (eluciano@pucrs.br) é Bacharel em Ciência da Computação, Doutora em Administração e Professora Titular da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

2 Rodrigo Hickmann Klein é Bacharel em Ciência da Computação, Mestre em Administração e Doutorando em Administração do Programa de Pós-Graduação em Administração da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

3 Vergilio Ricardo Britto-da-Silva é Bacharel em Administração, Mestre em Administração pelo Programa de Pós-Graduação em Administração da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e Pesquisador do Grupo de Pesquisas em Gestão e Tecnologia da Informação, no tema Privacidade.

Introdução

O assunto privacidade tem sido mais conhecido e comentado no Brasil na medida em que aumenta a utilização de redes sociais. Vazamentos de fotos de brasileiros famosos, as notícias de espionagem por parte do Governo Americano em relação à Presidente da República, à Petrobras e outras personalidades e organizações contribuíram para trazer à tona para uma parcela maior da população os perigos de vazamento de informações sem consentimento ou de espionagem eletrônica. No Brasil esta discussão iniciou tardiamente em comparação com países desenvolvidos e até em relação a alguns países em desenvolvimento. A título de exemplo, em um estudo sobre a adoção de Telemedicina no Brasil e EUA, Luciano, Mahmood e Mansouri-Rad (2014) identificaram situações opostas em relação à *privacy concerns*, ou seja, em relação ao nível de preocupação com a privacidade: enquanto nos EUA este assunto é o item de maior importância na tomada de decisão sobre a adoção da Telemedicina, para os respondentes brasileiros é o item com menor importância.

As questões relacionadas à privacidade não são recentes, porém se tornaram mais importantes na medida em que há um crescimento exponencial de informações sobre cada indivíduo sendo gerada, armazenada, transmitida e utilizada. O crescente volume de informação é inerente ao maior uso de Tecnologia da Informação e dispositivos cada vez mais onipresentes. A Figura 1 mostra algumas maneiras ao longo do tempo – desde a pré-história até o século 21 – de observar ou se intrometer na vida de outras pessoas e de acompanhar o que estas estavam fazendo. De fato, é possível que um vizinho nos acompanhe pela janela a cada movimento de saída e chegada em casa, a que horas isso ocorreu e com quem estávamos acompanhados. Entretanto, o crescimento da utilização de dispositivos tecnológicos — como, por exemplo, *smartphones* — possibilita o monitoramento, permitindo que os dados sobre os percursos percorridos e interesses sejam analisados para a formação de padrões de comportamento, chegando a conclusões sobre o usuário destes dispositivos que nem o próprio usuário perceberia. Apesar da discussão sobre proteção de informações ter recebido grande atenção nos meios de comunicação ao longo dos últimos 10 anos, as ameaças de divulgação indevida de informações continuam a crescer.

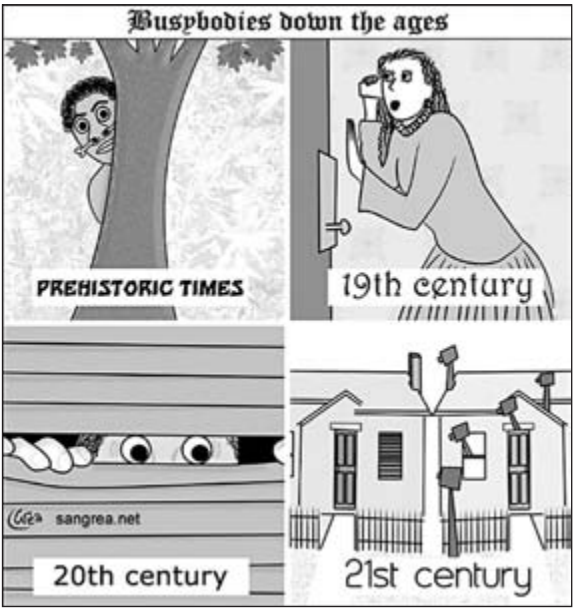


Figura 1 - Intromissões ao longo do tempo

Fonte: SANGREA (2015)

Dentro deste contexto, as ameaças à privacidade dos indivíduos se potencializa na medida em que mais dados são coletados, armazenados, analisados, trocados e por vezes vendidos. Estas etapas de coleta e utilização da informação deveriam ser sempre autorizadas pelo indivíduo, porém respeitar este aspecto tem sido cada vez mais difícil, se não impossível. Com a evolução das tecnologias de redes móveis e dos *smartphones*, as questões de privacidade tornaram-se extremamente importantes: mais conexão em mais lugares possibilita o acesso a um grande volume de informações pessoais (XUE et. al, 2012). Um interessante exemplo neste sentido é mostrado na Figura 2, ambas na Praça São Pedro, no Vaticano e envolvendo Papas. A foto de 2005 mostra o momento em que o corpo do falecido Papa João Paulo II cruzava a praça em direção à Basílica, para o velório. A segunda foto, de 2013, mostra o momento de aparição do Papa Francisco logo após ter sido escolhido como Papa. Embora os eventos sejam diferentes, é visível a diferença do uso de tecnologias ocorrida em oito anos.

Figura 2 - Eleição do Papa

Fonte: NBC News (2015)

No entanto, há um equívoco frequente em relação às ameaças à privacidade terem apenas fonte tecnológica. Toda vez que lidamos com uma informação que pertence a outras pessoas podemos gerar vulnerabilidade em relação à violação da privacidade deste indivíduo, assim como ocorreu no caso que abre este capítulo. Preocupar-se apenas com a tecnologia envolvida na garantia da privacidade, equivale a se preocupar apenas com o dinheiro no banco, sem se preocupar com o dinheiro na carteira, numa situação possivelmente mais vulnerável.

Os comentários a respeito de dados de pacientes, conversas informais em ambientes públicos, mesmo que sejam dentro da própria instituição, podem resultar em rupturas no processo de segurança desses dados. Corroborando essa preocupação, Goldin e Francisconi (2009) citam que as informações que os pacientes fornecem, quando de seu atendimento em um estabelecimento de saúde, assim como os resultados de exames e procedimentos realizados, com finalidade diagnóstica ou terapêutica, são de propriedade do paciente. Como exemplo, eles

afirmam que durante uma internação, em um hospital de grande porte, até 75 pessoas diferentes chegam a lidar com o prontuário de um paciente.

As preocupações com privacidade aumentam quando se trata de dados relacionados à saúde: Gaertner e Silva (2005) afirmam que o histórico médico de um indivíduo está entre os tipos de informação que mais se deseja preservar. O vazamento de informações desse tipo pode ser catastrófico para os usuários dos serviços de saúde e seus familiares, uma vez que os danos causados pelo vazamento acidental ou voluntário de dados e informações sigilosas podem ser irreversíveis (LUCIANO, BRAGANÇA e TESTA, 2011). Acquisti e Grossklags (2008) ressaltam que nem sempre sabemos quando, onde e como o todo ou parte de informações pessoais que deveriam ser privadas estão sendo utilizadas.

Acquisti e Grossklags (2003) investigaram as causas da dicotomia existente entre a intenção e a ação no sentido do trato adequado da informação e concluíram que, mesmo existindo atualmente diversas tecnologias que visam a garantir a privacidade das informações, muitas delas, aparentemente, não têm obtido êxito nesse sentido, podendo ser a divulgação por meio de profissionais (e não por meios eletrônicos) a explicação dessa divergência. Nesse contexto, a privacidade das informações médicas de um paciente é um direito deste da mesma forma em que é igualmente uma obrigação do profissional de saúde que o atende. E esse direito não se extingue com a morte da pessoa. A Declaração de Genebra, de 1924, diz que os segredos confiados ao profissional de saúde deverão ser respeitados mesmo após a morte do paciente, e assim o dever de confidencialidade que todos os profissionais de saúde devem observar mantém-se mesmo após a morte do paciente (GOLDIN e FRANCISCONI, 2009).

A informação deve ser protegida e processos de segurança devem ser criados e gerenciados, independentemente da forma como essa informação é armazenada, transmitida ou acessada (MOREIRA, 2001), e acessível para as pessoas certas, na devida quantidade: nunca a mais do que cada indivíduo necessita para sua tomada de decisão.

Um breve histórico e o conceito de privacidade

A discussão sobre privacidade remonta a tempos antigos. Em seus ensaios sobre ética e política, Aristóteles diz que um dos papéis da política liberal é o de garantir uma zona de liberdade dos cidadãos, na qual eles possam viver sua vida de acordo com sua vontade, independentemente do julgamento alheio, desde que não causando mal a outros (SWANSON, 1992, p. 36), o que remonta ao conceito de privacidade. Em 1873, um estudo do juiz americano Thomas Colley, chamado de *The Elements of Torts*, deu uma definição clássica para a palavra privacidade, de que esta é a limitação do acesso às informações de uma dada pessoa, ao acesso à própria pessoa, à sua intimidade, envolvendo as questões de anonimato. É a liberdade que uma pessoa tem de não ser observada sem autorização. Já Warren e Brandeis, em 1890, incluíram na privacidade o direito à solitude, ao afastamento ou solidão voluntária, definindo a privacidade como um direito, o direito de ficar sozinho.

Derivada do latim *privatus*, que significa aquilo que está fora da alçada do Estado, sendo pertencente à própria pessoa, ao próprio indivíduo, a privacidade pode também ser definida como um conceito que se caracteriza pela capacidade que cada indivíduo tem de proteger e gerenciar o acesso às suas informações pessoais.

Mais contemporaneamente, a partir dos anos 1950, os estudos de Westin contribuíram para a noção de privacidade como uma reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida suas informações são comunicadas a outros. O livro *Privacy and Freedon*, publicado por Westin em 1967, ainda é uma referência fundamental sobre o assunto. Westin, advogado e cientista político americano, estudou o tema por mais de 40 anos, trazendo a preocupação em relação ao que as empresas faziam com os dados de seus clientes ainda antes da utilização de Sistemas de Informação e da Internet, preocupando-se também com o tratamento das escutas telefônicas ilegais, dados financeiros, médicos e outros dados pessoais.

Em um sentido geral, Westin (1967) diz que a privacidade pode ser entendida como o conjunto de informações acerca do indivíduo o qual

ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições, sem a isso ser legalmente sujeito. A privacidade de um indivíduo e de suas informações é um direito de cada cidadão e a ele pertence. Dessa forma, nenhuma organização deve negligenciar essa responsabilidade nem descuidar de nenhuma informação que lhe for confiada (MOREIRA, 2001; FONTES, 2006). Westin transformou o debate sobre privacidade, trazendo a noção de privacidade como direito, mas também a responsabilidade de cada indivíduo em zelar sobre a sua privacidade.

Há duas questões intrigantes neste breve histórico. A primeira delas é que um dos países que foi precursor em estudos sobre privacidade, com legislação específica sobre o assunto e que tem debates ferrenhos da comunidade sobre o assunto, é o mesmo país que detém diversas das grandes companhias que utilizam dados de clientes como parte de seu negócio e cujo governo faz significativo uso de dados de cidadãos, porém nestes dois últimos casos, nem sempre com a autorização dos indivíduos. Desta forma, os Estados Unidos da América são ao mesmo tempo um dos países onde a privacidade é mais discutida, mais legislada e potencialmente mais violada.

Os EUA promulgaram em 2006 a *Health Insurance Portability and Accountability Ac*t (HIPAA), que visa a proteger toda informação pessoal disponibilizada e utilizada na prestação de serviços de saúde. De acordo com Baumer, Earp e Payton (2000), esse ato pode ser visto como a resposta oficial para preocupações éticas e morais de proteção da informação do indivíduo na forma da Lei nos Estados Unidos, definindo diretivas dos direitos à privacidade e ao manuseio dos registros de saúde.

Enquanto a HIPAA trabalha no sentido de proteção da privacidade, o *Patriot Act* permite que órgãos de segurança e de inteligência dos EUA interceptem ligações telefônicas e e-mails de organizações e pessoas estrangeiras ou americanas supostamente envolvidas com o terrorismo, sem necessidade de qualquer autorização da Justiça. No entanto, não são conhecidas as variáveis que permitem que o governo Americano caracterize uma ameaça terrorista, gerando uma brecha para que isso seja usado como pretexto para a violação da privacidade. Mais um aspecto da contradição entre a proteção e ao uso (indevido) de informações.

A segunda questão intrigante é o uso de vigilância e de coleta, armazenamento e uso de informação pelo próprio governo. Mesmo nos EUA, que detêm legislação sobre privacidade desde a década de 1950, impera o silêncio acerca de eventuais violações de privacidade pelo governo.

No Brasil, o Ministério da Saúde do Brasil (MS) definiu alguns padrões para o RES (Registro Eletrônico de Saúde), através da Portaria no 2.073, de 31 de agosto de 2011. O RES é um conjunto de informações de saúde e assistência a um paciente durante a sua vida, contendo informações que orientarão sobre procedimentos, exames e consultas deste paciente. Além disso, pode ser utilizado como fonte de informações sobre epidemias e dados demográficos de grupos ou regiões (ARAUJO, PIRES e BANDEIRA-PAIVA, 2014).

Segundo o Ministério da Saúde, no RES devem ser utilizados padrões para os dados, que permitam a interoperabilidade entre os diferentes sistemas e a integração entre fontes de informações de diferentes instituições e hospitais. Como o RES aborda informações complexas e tem grande necessidade de confidencialidade, a implementação de seu uso deve considerar padrões da área de saúde, como o Digital Imaging Communication in Medicine (DICOM) para imagens médicas, desenvolvido pela Radiology Society of North America (RSNA) e pela National Electrical Manufacturers Association (NEMA), o padrão Clinical Document Architecture (CDA) da organização Health Level Seven (HL7), além de utilizar o padrão TISS (Troca de Informação de Saúde Suplementar) (ARAUJO, PIRES e BANDEIRA-PAIVA, 2014).

A TISS foi criado pela Agência Nacional de Saúde Suplementar (ANS) e visa à interoperabilidade de sistemas de informação de saúde suplementar recomendados pela ANS, com o objetivo de estabelecer um padrão obrigatório para a troca de informações eletrônicas de saúde suplementar (MENDES, 2009). A TISS (Troca de Informação de Saúde Suplementar) padroniza ações administrativas, além de oferecer suporte ao acompanhamento e avaliação não somente financeira e econômica, mas também assistencial das operadoras de planos de saúde privados. A organização do padrão TISS se divide em: organizacional, conteúdo e estrutura, representação de conceitos em saúde, segurança e privacidade, nesta última são descritos os requisitos para proteção dos dados, para a

comunicação e para os meios e métodos que garantam a segurança da informação (ARAUJO, PIRES e BANDEIRA-PAIVA, 2014).

A vida imita a arte? Algumas reflexões

Há filmes e livros que permitem ilustrar os aspectos e contextos da privacidade, pois alguns relatos que outrora eram ficcionais se tornaram reais atualmente. Muitas tecnologias apresentadas como ficção podem não estar disponíveis exatamente como apresentadas nos filmes ou livros, mas o serviço e a funcionalidade que proporcionam no enredo já estão disponibilizados no nosso dia a dia. Desta forma, muitas destas obras de ficção permitem exemplificar alguns casos e consequências da perda da privacidade, facilitando o entendimento da severidade das ameaças e como podemos estar vulneráveis a elas. Como, por exemplo, no livro de George Orwell, intitulado *1984*, cuja primeira edição é de 1949. Nesta obra o autor elabora uma ficção que projeta um hipotético cotidiano de 1984, em um regime totalitário e repressivo, no qual a chamada "polícia do pensamento" acompanha todas as ações, manifestações e pensamentos dos cidadãos em um país fictício denominado Oceânia, punindo duramente quem agir ou pensar em discordância com as regras vigentes. Os aspectos abordados no livro e relacionados à Segurança da Informação vão além da perda da privacidade, abrangendo a questão da integridade dos dados, pois um dos personagens principais adultera documentos que servem de referência ao passado, beneficiando ao interesse do Partido que domina o país. O livro permite demonstrar as consequências psicológicas quando a privacidade não é respeitada, abrangendo aspectos como a falta de individualidade e livre-arbítrio, a humilhação e o desânimo.

Não obstante, o filme *Minority Report* exemplifica o que ocorre quando há confiança desacerbada em um sistema de detecção prévia de crimes, que invade a privacidade do cidadão. Segundo o enredo deste filme, no ano 2054 o crime estará praticamente eliminado na cidade de Washington DC, graças a uma unidade de elite, que possui três videntes com poderes especiais para ver o futuro e prever crimes; estas previsões estão interligadas a um sistema que digitaliza e armazena as visões dos viden-

tes. O personagem John Anderton lidera esta unidade e acredita na perfeição do sistema. No entanto, um dia os videntes preveem que o próprio Anderton cometerá um assassinato. Anderton inicia uma corrida contra o tempo para tentar provar sua inocência, durante a busca encontra diversas falhas no sistema e descobre que as pessoas têm o poder de mudar seu próprio destino. Neste contexto a privacidade é totalmente desconsiderada e a credibilidade no sistema de detecção prévia de crimes é tão grande que sobrepuja questões legais e éticas.

Por outro lado, o filme *A vida dos outros* provoca reflexões sobre a questão ética entre o limite do que pode ser feito em prol da segurança da sociedade versus a privacidade e liberdade do cidadão. O enredo deste filme decorre em uma sociedade oprimida pela vigilância constante, na qual um agente do governo encontra-se em um dilema ético entre os interesses pessoais dos governantes e a garantia dos direitos dos vigiados. O filme demonstra que os dados coletados dos cidadãos fornecem poder a quem os possui e este poder pode corromper e servir como barganha para obter vantagens, ilustrando quão importante são os dados privados para quem os perde e os riscos aos quais estão submetidos.

Na ficção *Controle Absoluto*, um sistema onipresente de inteligência artificial começa a tomar as suas próprias decisões, controlando cada passo por meio de câmeras, semáforos, ligações telefônicas, drones, etc. O sistema tem acesso a todas as informações de todos os cidadãos, em prol do combate ao terrorismo, porém começa a manipular as pessoas com ameaças e decide eliminar seus oponentes. Este filme demonstra o que pode ocorrer com os cidadãos, ao aceitarem perder sua privacidade a favor de uma alegada segurança nacional. Além disso, demonstra que a confiança apenas em automatismos, como hardware e software, para gerenciar a segurança da informação pode incorrer em erros, pois as pessoas e o seu comportamento perante a segurança são tão ou mais importantes quanto o hardware e o software. O grau de responsabilização das pessoas em relação às falhas é tão grande que há uma norma ISO dedicada a esse tema, a ISO/IEC 27002 (ABNT, 2005), que considera as pessoas o principal fator de falhas da Segurança da Informação. Conforme esta norma internacional, a Segurança da Informação é obtida a partir da

implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e, por fim, funções de software e hardware.

Outro filme que aborta o comportamento humano em relação à Segurança da Informação é filme *Violação de Privacidade*. A trama desta ficção ocorre em um mundo onde há microchips implantados nas pessoas, que podem gravar todos os momentos das suas vidas. Os chips são removidos após a morte, para que as imagens possam ser editadas e fornecidas aos entes queridos. Conforme o enredo deste filme, o personagem de Robin Williams é o melhor editor da empresa, capaz de assistir a situações mais adversas das vidas alheias e a quem é atribuído os casos mais difíceis. O ponto ético principal abordado pelo filme não é a perda da privacidade consentida, mas a manipulação dos dados por quem tem acesso a eles, retirando todos os pontos negativos das pessoas falecidas, e ocultando crimes quando isso é conveniente aos envolvidos. Neste aspecto ocorre a perda da integridade da informação, que está relacionada à proteção da exatidão e da completude da informação.

No filme *Inimigo do Estado*, um segredo de estado cai em mãos erradas e o governo tenta eliminar as provas e os envolvidos que as detêm. O filme demonstra que o cidadão sem proteção a sua privacidade fica à mercê das falhas do governo ou de quem detém as suas informações. Por exemplo, um erro governamental pode provocar a perda da confidencialidade dos dados de um cidadão, através da publicação em portais de Dados Abertos Governamentais, quando o responsável pela publicação não se preocupa com as possíveis combinações entre os dados publicados e demais fontes de dados na Internet, deixando de ofuscar as informações que permitam essas combinações.

Porque é importante nos preocuparmos com a nossa privacidade?

Quando nos preocupamos com alguma coisa, prestamos mais atenção aos aspectos relacionados ao objeto da preocupação, nos torna-

mos mais observadores e vigilantes aos detalhes relacionados. Em uma pesquisa sobre as intenções dos usuários de computadores de seguirem as regras explicitas nas políticas de Segurança da Informação, Pahnila, Siponen e Mahmood (2007) identificaram a importância dos usuários conhecerem a severidade das ameaças. Os autores perceberam – em estudos na área da saúde – que pessoas com câncer passaram a se cuidar mais e a seguir mais os procedimentos médicos quando tomavam conhecimento da severidade das ameaças.

No mesmo sentido, a privacidade é mantida com o nosso comportamento responsável a respeito de que tipo de informação divulgamos sobre nós mesmos. Por exemplo, uma rede social divulga em sua política de privacidade quais dados de um perfil de usuário vai utilizar, em que tipo de situação e como vai utilizar – cabe a nós ler a política de privacidade, refletir sobre o seu conteúdo e somente se acharmos razoável, aceitar o serviço. Mesmo assim, é aconselhável verificar se a cada postagem não estamos nos expondo demais.

Uma possível explicação para o comportamento ambíguo de preocupação com privacidade, mas mantendo, por exemplo, o uso intensivo de redes sociais, pode ser proveniente da Teoria da Prevenção da Ameaça Tecnológica (*Technology Threat Avoidance* Th*eory*, TTAT). Segundo esta teoria, criada por Liang e Xue em 2009, os usuários, ao decidirem como lidar com ameaças resultantes do uso de dispositivos de Tecnologia da Informação passam por dois processos cognitivos: a avaliação da ameaça e a avaliação das formas de enfrentamento da ameaça. Na avaliação da ameaça, os usuários percebem a ameaça à qual estão suscetíveis e avaliam se as consequências negativas serão severas. Segundo Klein (2014), a percepção de ameaça leva à avaliação de enfrentamento, na qual os usuários avaliam o grau em que a ameaça pode ser evitada, tomando medidas de salvaguarda baseadas na eficácia percebida, nos custos da medida de salvaguarda e na autoeficácia da adoção da medida de salvaguarda. A TTAT propõe que os usuários são motivados a evitar prejuízos quando percebem uma ameaça e acreditam que a ameaça é evitável através de medidas de salvaguarda. Por outro lado, se os usuários acreditam que a ameaça não pode ser totalmente evitada tomando as medidas de salvaguarda, optam pelo enfren-

tamento focado na emoção (LIANG e XUE, 2009). A emoção explicaria o comportamento dos usuários no pouco zelo em preservar informações sobre si mesmo.

Um exemplo da exposição indevida é a utilização de serviços em aparelhos celulares que registram os itinerários percorridos em um mapa, contendo todo o trajeto de um determinado usuário em determinado período, indicando em detalhes as ruas, a ordem em que se deslocou e os locais onde parou (Figura 3). Muitas pessoas divulgam essa imagem nas redes sociais apresentando grande satisfação, sem desconfiar que estão expondo informações em demasia, que podem ser usadas, por exemplo, para um sequestro-relâmpago. No entanto, mesmo que elas não façam isso, a informação possivelmente já foi coletada e armazenada em bases de dados.

Figura 3 - Histórico de localização do usuário do Android

Fonte: Techmundo (2015)

Quanto menos se tem privacidade, menos controle se tem sobre a vida, sobre o destino ou ainda a respeito da utilização lícita ou ilícita de nossas informações pessoais. Dyson (2008) cita que "a privacidade real – que é o respeito pelas pessoas e não mera ausência de dados – depende do discernimento humano e do bom senso". Ela está ligada à vigilância e à segurança. Necessário se faz, então, que o equilíbrio entre privacidade, segurança e controle seja alcançado, de forma a garantir a preservação dos direitos tanto coletivos quanto individuais.

Segundo Klein (2014), a popularização de artefatos de TI que visam mitigar as ameaças à Segurança da Informação acabou produzindo uma noção incorreta que esses artefatos – como, por exemplo, antivírus e firewall e sistemas de detecção de intrusos – podem proteger os usuários de ataques e suplantar qualquer ameaça. Essa noção equivocada pode ser originada pela obtenção de informações parciais sobre o assunto ou pela falta da conscientização adequada (LIANG e XUE, 2009) e é um fator humano que pode provocar acréscimo de vulnerabilidade, pois ocasiona um comportamento imprudente dos usuários em relação aos Sistemas de Informação (LIGINLAL et al., 2009). Entretanto, somente esse equívoco em relação à percepção da ameaça e a sua severidade não explica as brechas na Segurança da Informação provocadas por fatores humanos. Outra percepção importante é o esforço percebido no cumprimento de ações que conduzem a um comportamento responsável em relação à Segurança da Informação, que somados aos aspectos como a indiferença às regras da Segurança da Informação e o erro humano, também podem ser fatores indutores de vulnerabilidade e brechas na Segurança da Informação.

Outro motivo para a preocupação com a manutenção da privacidade é que esta assegura um certo equilíbrio social. Observe a Figura 4, abaixo.

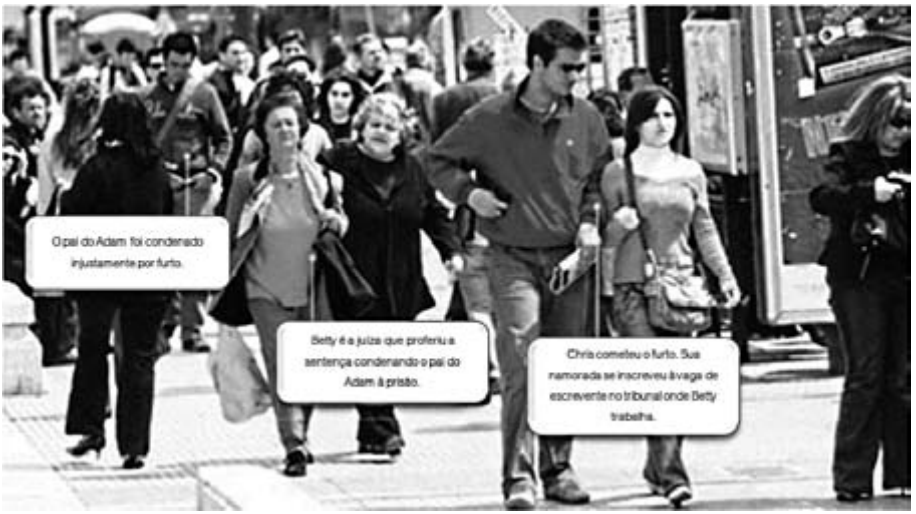


FIGURA 4 - Reflexões sobre privacidade.

Fonte: Adaptado de Dyson (2008) – MARK CLEMENS (foto-ilustração); RICHARD NOWITZ National Geographic Collection (cena de público)

Não seria possível a convivência em grupo se detalhes da vida de cada um e em especial da intersecção de fatos envolvendo diferentes pessoas fossem sempre públicas. As questões envolvendo Adam, Betty e Chris precisam ser resolvidas, mas não expostas a uma situação pública em um dia qualquer, sem preparação dos indivíduos para com esta situação. Isto é o que Westin (1967) chama de valor social da privacidade, que provê a indivíduos e grupos a preservação da autonomia, a liberação da interpretação de papéis, um tempo para autoavaliação e uma comunicação protegida.

Um assunto com muitas facetas

Privacidade é um assunto complexo, com muitas questões envolvidas. Uma destas questões é paradoxal, em relação ao não fornecimento de informações ou à conveniência gerada pelo compartilhamento dessa informação: no entendimento da privacidade como um direito, ela não é passível de troca por nenhum tipo de benefício; por outro lado, a privacidade tem sido usada como moeda de troca em serviços 'gratuitos'. Para utilizar serviços disponíveis na Internet, o usuário fornece uma quantidade considerável de informações pessoais, que podem colocar em risco a sua privacidade. Se ele o faz deliberadamente, tanto melhor é do que se não se der conta de que um grande número de dados a seu respeito está sendo coletado em redes sociais, aplicativos gratuitos e outros dispositivos de hardware e software.

Há uma série de desafios relacionados à geração de menor vulnerabilidade à privacidade. Estes desafios não são tanto de cunho tecnológico, mas sim de cunho comportamental. Em pesquisa com profissionais da assistência multidisciplinar na região Sul, Luciano, Bragança e Testa (2011) identificaram com os respondentes os principais desafios na construção de um ambiente nas instituições de saúde de zelo com a privacidade dos pacientes. Dos oito desafios identificados, cinco se referiam a

aspectos comportamentais, um a aspectos tecnológicos e um a mecanismos de proteção, conforme o Quadro 1, abaixo.

Quadro 1 – Desafios relacionados à privacidade

Categoria	Principais itens (na visão dos entrevistados)	Citações
Tecnológicos	▪ Impedir o acesso não autorizado às informações de pacientes.	1
Comportamentais	▪ Formação da compreensão do significado de sigilo e privacidade. ▪ Entendimento da motivação do acesso não autorizado. ▪ Capacitações que permitam uma mudança da cultura de acesso onipotente e não punição. ▪ Os comentários dos profissionais em áreas comuns podem ser a maior fonte de quebra de sigilo.	5
	▪ A percepção do que é lícito é difícil no dia a dia em cada contato com o paciente ou com os colegas.	2
Mecanismos de proteção	▪ Definição mais clara de regras de acesso às informações (inclusive para documentos em papel).	3

Fonte: Luciano, Bragança e Testa (2011)

Observa-se que, na visão dos respondentes, não se trata de um problema relacionado à tecnologia, mas sim a aspectos comportamentais dos indivíduos envolvidos. Nesse sentido, faz-se necessário analisar de maneira mais aprofundada quais são as possíveis formas de modificar esse comportamento e introduzir, paulatinamente, uma mudança cultural. A definição de mecanismos de proteção igualmente só funcionará com uma cultura que valoriza e respeita a privacidade de informações de pacientes.

No mesmo sentido, os autores perguntaram aos respondentes a respeito da responsabilidade dos profissionais envolvidos. Segundo os respondentes, há um entendimento equivocado de que os comentários com colegas da área da saúde não envolvidos no caso não constituem quebra de sigilo, mostrando a necessidade de deixar mais claros os conceitos, a importância, abrangência e amplitude do conceito e da prática da preservação da confidencialidade de dados e da privacidade de indivíduos.

Ao longo de 40 anos pesquisando sobre privacidade, o advogado Westin percebeu que os problemas de proteção da privacidade são agora tão assustadores que eles não podem ser tratados apenas pelo ponto de visto jurídico, mas exigem um mix de soluções jurídicas, sociais e tecno-

lógicas (FOX, 2013). Há questões legais, sociológicas, filosóficas, antropológicas, de comportamento humano, computacionais e de gestão envolvidas. No nosso entendimento, planejamento do uso de Tecnologia da Informação nas organizações, conscientização das ameaças e um detalhado programa de governança da informação complementam este mix.

Referências

A VIDA dos outros (Das Leben der Anderen). Direção: Florian Henckel von Donnersmarck. Alemanha: Europa Filmes, 2006. 137 min.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação.** Rio de Janeiro, 2005.

ACQUISTI, A.; GROSSKLAGS, J. Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. In: ANNUAL WORKSHOP ON ECONOMICS AND INFORMATION SECURITY-WEIS, 2., 2003.

ACQUISTI, Al.; GROSSKLAGS, J. What can behavioral economics teach us about privacy. In: ____. **Digital privacy: theory, technologies and practices**. New York: Auerbach, 2008. p. 363-377.

ARAUJO T.V.; PIRES S.R.; BANDIERA-PAIVA P. Adoção de padrões para Registro Eletrônico em Saúde no Brasil. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 8, n. 4, p. 554-566, 2014.

BAUMER D.; EARP J.B.; PAYTON F.C. Privacy of medical records: IT implications of HIPAA. **ACM SIGCAS Computers and Society**, v. 30, n. 4, p. 40-47, 2000.

CONTROLE Absoluto (Eagle Eye). Direção: D.J. Caruso. EUA: Paramount Pictures, 2008. 118min.

DYSON, E. Reflexões sobre privacidade. **Scientific America Brasil**, out. 2008. Disponível em: <http://www2.uol.com.br/sciam/reportagens/reflexoes_sobre_privacidade_imprimir.html>. Acesso em: 8 de jan. de 2015.

FONTES, E. **Segurança da Informação:** o usuário faz a diferença, Rio de Janeiro: Saraiva, 2006.

FOX M., Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83, **New York Times**, 22 fev. 2013, p. D7. Disponível em: <http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who--defined-right-to-privacy-dies-at-83.html?pagewanted=all&_r=0>. Acesso em: 3 fev. 2015.

GAERTNER, A.; SILVA, H. P. Privacidade da Informação na Internet: ausência de normalização. In: ENCONTRO NACIONAL DE CIÊNCIA DA INFORMAÇÃO, 6., Bahia, 2005. Proceedings CINFORM. Bahia, 2005.

GOLDIN, J.R.; FRANCISCONI, X. Bioética. Disponível em: <http://www.ufrgs.br/bioetica/provac.ppt#9>. Acesso em: 1 jul. 2009.

INIMIGO do estado (Enemy of the state). Direção: Tony Scott. EUA: Jerry Buckheimer, 1998. 132 min.

KLEIN, R. H. **Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à segurança da informação**. 2014. Dissertação (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia. Pontificia Universitade Católica do Rio Grande do Sul, Porto Alegre, 2014. Disponível em: <http://repositorio.pucrs.br:8080/dspace/handle/10923/577>. Acesso em: 3 fev. 2015.

LIANG, H.; XUE, Y. Avoidance of information technology threats: a theoretical perspective. **MIS Quaterly,** v. 33, n. 1, p. 71-90, 2009.

LIGINLAL, D.; SIM, I.; KHANSA, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. **Computers & Security,**v.28, p.215-228, 2009.

LUCIANO, E. M.; BRAGANÇA, C. E. B.; TESTA, M. G. Privacidade de informações de pacientes de instituiçoes de saúde: a percepção de profissionais da área de saúde. **REUNA**, v. 16, n. 2, 2011.

LUCIANO, E. M.; MAHMOOD, M. A.; MANSOURI-RAD, P. Telemedicine adoption issues in the U.S.A. and Brazil: perception of health-care professionals. In: ANNUAL MEETING OF THE DECISION SCIENCES INSTITUTE, 45., Tampa, Florida, 2014. Annals... Houston: Decision Sciences Institute, 2014.

MENDES, S. F. et al. Uma análise da implantação do padrão de troca de informação em saúde suplementar no Brasil. **Journal of Health Informatics**, v. 1, n. 2, 2009.

MINORITY Report . A Nova Lei. (Minority Report, EUA, 2002). Direção: Steven Spielberg. EUA: 20th Century Fox, 200. 146 min.

MOREIRA, N. S. **Segurança mínima**: uma visão corporativa da Segurança da Informação. Rio de Janeiro: Axcel Books, 2001.

NBC News. Pope Election. Disponível em: <http://instagram.com/p/W2FCksR9-e/>. Acesso em: 8 jan. 2015.

PAHNILA, S.; SIPONEN, M.; MAHMOOD, A. Employees' behavior towards IS security policy compliance. In: ANNUAL HAWAII INTERNATIONAL CONFERENCE ON IEEE, 40., 2007. p. 156b-156b.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

SANGREA. Busybodies down the ages. Disponível em: <http://www.sangrea.net/free-cartoons/privacy_busybodies.jpg>. Acesso em: 7 jan. 2015.

SWANSON, J. A. **The public and the private in Aristotle's political philosophy.** New York: Cornell University, 1992.

TECHMUNDO. Histórico de Localização do Google Maps mostra por onde você já passou. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/12/historico-de-localizacao-do-google-maps-mostra-por-voce-ja-passou-veja.html>. Acesso em: 7 jan. 2015.

VIOLAÇÃO de Privacidade *(The final cut)*. Direção: Omar Naim. EUA: PlayArte. 2005.

WESTIN, Alan D. **Privacy and Freedon**. New York: Athenum, 1967.

XU, H. et al. Measuring mobile users' concerns for information privacy. Thirty Third International Conference on Information Systems (ICIS). Orlando: [s.n.] 2012.

2

E-Saúde e desafios à proteção da privacidade no Brasil[1]

Koichi Kameda[2]
Magaly Pazello[3]

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 o 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 e a teleconsultoria.

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.

1 Versão atualizada do artigo originalmente publicado na Revista PoliTICs, número 16, Novembro de 2013.

2 Koichi Kameda (kkameda@nupef.org.br) é bacharel em Direito e mestre em Bioética, Ética Aplicada e Saúde Coletiva, ambos pela Universidade do Estado do Rio de Janeiro (UERJ) e pesquisador colaborador do Núcleo de Estudos, Pesquisas e Formação (Instituto Nupef), Rio de Janeiro.

3 Magaly Pazello é graduada em Letras pela Universidade Federal Fluminense, mestre em Letras Neolatinas pela Universidade Federal do Rio de Janeiro (UFRJ) e Pesquisadora do Instituto Nupef.

Este artigo tem o propósito de apresentar um breve panorama da e-Saúde 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 do sistema de saúde.

Iniciativas de e-Saúde no Brasil

O uso de tecnologias de informação e comunicação para mediar a atenção à saúde é denominado de e-Saúde (*e-Health*). A terminologia[4], adotada pela Organização Mundial da Saúde, inclui a assistência a paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde (WHO, 2005). De modo mais específico, processos de e-Saúde incluem: teleconsultorias, telediagnóstico, segunda opinião formativa, telecirurgia, telemonitoramento (televigilância), educação permanente, teleducação e prontuário eletrônico (REZENDE, 2010).

Alguns exemplos de iniciativas de e-Saúde no Brasil são a rede RUTE e o Cartão Nacional.

A Rede Universitária de Telemedicina (RUTE) 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.[5]. Outra rede é a Telessaúde Brasil Redes, capitaneada pelo Ministério da Saúde, e inicialmente instituída sob o nome Programa Nacional de Telessaúde em 2007 (SILVA; MORAES, 2012).

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

5 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.

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 (FIOCRUZ, 2011). O projeto foi 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 (SILVA; MORAES, 2012).

É preciso observar que o campo da e-Saúde 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" (MORAES; VASCONCELLOS, 2005).

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, vigilância, 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 (BRASIL, 2015).

O documento de 2012 reconhece "e-Saúde" 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 e-Saúde".[6] 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 (BRASIL, 2015).

Em paralelo aos debates para a revisão da PNIIS, a constatação da necessidade de uma política estratégica de e-Saúde levou à elaboração de uma proposta de "Visão Estratégica de e-Saúde 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 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 e-Saúde, realizadas a partir de maio de 2012, tiveram como foco a construção do RES que, integrado ao Sistema de Informação de Saúde (E-SUS), compõem o Sistema Cartão Nacional de Saúde. O grupo de trabalho foi 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.

Desafios à proteção da privacidade no âmbito dos sistemas de e-Saúde 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

6 Para mais detalhes sobre o documento da PDTI 2014-2015, consultar: http://datasus.saude.gov.br/images/PDTI_2014-2015_Vs_Atualizada_jul2015.pdf

atenção à saúde (IDRC, 2010), exigem cautela quanto ao seu emprego e ambiente tecnológico e, ao mesmo tempo, garantias com relação à 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 (IDRC, 2010).

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 (DONEDA, 2006).

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 (DONEDA, 2006).

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 (DONEDA, 2006).

Considerados esses esclarecimentos, no 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 (MAGRANI, 2012).

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 (MAGRANI, 2012).

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. Em 2013, causou grande polêmica a divulgação de um 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.[7]

Essas preocupações fazem total sentido no âmbito das iniciativas de e-Saúde, 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 (MORAES; VASCONCELLOS, 2005).

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 (SILVA; MORAES, 2012). Moraes (2002) 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 mais vulneráveis terem os seus corpos esquadrinhados, de os indivíduos serem regulados e controlados em nome da garantia das suas qualidades de vida (SILVA; MORAES, 2012).

7 "Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais". Disponível em < http://www.rets.org.br/?q=node/2313 > Acesso em: 08 Março 2015.

Por tais razões, o tratamento de dados pessoais vem 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[8]

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).[9]

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).

8 "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#.VTgcQfAYHUR > Acesso em: 08 Março 2015

9 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).

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 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 (BRASIL, 2015).

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 e-Saúde.

Uma iniciativa que merece menção é o anteprojeto de lei (APL) de proteção aos dados pessoais, concebido e levado a consulta públi-

ca pelo Ministério da Justiça.[10]. O anteprojeto regula o tratamento[11] de dados pessoais ocorrido em território nacional, seja por pessoa natural ou pessoa jurídica de direito público ou privado, estabelecendo os princípios gerais e os requisitos para utilização desses dados, bem como os direitos do titular e a responsabilidade dos agentes envolvidos na operação.

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 específica do e de seus direitos como, por exemplo, o de se negar a fornecer tais dados.

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

- Princípio da finalidade: o tratamento deve ser fundamentado em finalidades legítimas, específicas, explícitas e conhecidas pelo titular;
- Princípio da adequação: o tratamento precisa ser compatível tanto com o fim almejado quanto com as expectativas do titular;
- Princípio da necessidade: o tratamento dos dados pessoais deve ser limitado ao mínimo necessário, abarcando apenas dados que sejam pertinentes, proporcionais e não excessivos;
- Princípio do livre acesso: o titular deve poder consultar gratuitamente e com facilidade as modalidades de tratamento e a integralidade de seus dados pessoais;
- Princípio da qualidade dos dados: exatidão, clareza e atualização dos dados pessoais alvo de tratamento;
- Princípio da transparência: o titular deve ter acesso a informações claras e adequadas sobre os tratamentos de seus dados;

10 Uma primeira versão foi levada a discussão pública entre novembro de 2010 e abril de 2011. Em janeiro de 2015, uma nova versão foi apresentada para consulta pública. Este artigo se baseia na versão mais recente.

11 O anteprojeto entende como tratamento o "conjunto de ações referentes à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração".

- Princípios da segurança: utilização das medidas técnicas e administrativas proporcionais ao atual estado da tecnologia e à natureza dos dados pessoais a fim de protegê-los de destruição, perda, alteração, comunicação ou difusão, tanto acidentais quanto ilícitas, bem como do acesso não autorizado;
- Princípio da prevenção: devem ser adotadas medidas capazes de prevenir a ocorrência de danos decorrentes do tratamento de dados;
- Princípio da não discriminação: veda o tratamento de dados pessoais para fins discriminatórios.

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. Em princípio, o tratamento é vedado pelo anteprojeto, salvo em caso de consentimento do titular especificamente em relação ao tratamento desses dados e com informação sobre a sua natureza sensível e os riscos envolvendo sua utilização. Por outro lado, o tratamento seria autorizado quando os dados forem de acesso público irrestrito ou em casos previstos no próprio anteprojeto, como, por exemplo, para a proteção da vida ou da incolumidade física do titular ou de outra pessoa.

Outro ponto colocado em debate pelo anteprojeto é a criação de um orgão administrativo responsável pela proteção de dados pessoais. O orgão teria como atribuições a proposição de ações, o estabelecimento de normas complementares e a tomada de decisão em casos envolvendo o tratamento desses dados. Também caberia ao orgão o recebimento de reclamações e aplicação de sanções administrativas e medidas corretivas. Assim, o orgão teria como objetivo não somente a garantia das normas previstas no anteprojeto, mas também um caráter propositivo, contribuindo para a formulação de políticas publicas e para a busca de soluções mais rápidas e adequadas para um tema amplamente marcado pelo avanço tecnologico como o tratamento de dados pessoais.

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 e-Saúde, ajudando a garantir a integridade e acurácia informação médica presente nesses bancos de dados (IDRC, 2010).

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 e-Saúde, 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 atividades 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 e-Saúde. 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 do sistema de saúde, inclusive com medidas de educação dos profissionais envolvidos no tratamento dos dados pessoais, podem ser úteis (IDRC, 2010).

Referências

BRASIL. Ministério da Justiça. **Anteprojeto de proteção a dados pessoais**. Disponível em: < http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf >. Acesso em: 8 Março 2015.

BRASIL. **Plano Diretor de Tecnologia da Informação do Ministério da Saúde**. Brasília, DF, 2015. Disponível em: <http://datasus.saude.gov.br/images/PDTI_2014-2015_Vs_Atualizada_jul2015.pdf>. Acesso em: 8 março 2015.

ESCOLA NACIONAL DE SAUDE PÚBLICA. Ceensp debate novos rumos para o Cartão SUS. **Informe ENSP**, 16 jul. 2015. Disponível em: < http://www.ensp.fiocruz.br/portal-ensp/informe/site/materia/detalhe/24947 > Acesso em: 8 março 2015.

INTERNATIONAL DEVELOPMENT RESEARCH CENTRE. **Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations.** London: The London School of Economics and Political Science**, 2010.**

MAGRANI, B. et al. **Relatório de Políticas Digitais**. 2012. Disponível em: < http://www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf >. Acesso em: 8 março 2015.

MORAES, I.H.S. **Política, tecnologia e informação em saúde**: a utopia da emancipação. Salvador: Casa da Qualidade, 2002.

MORAES, I.H.S.; 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.

REDE LATINO-AMERICANA DE ESTUDOS SOBRE VIGILÂNCIA, TECNOLOGIA E SOCIEDADE. **Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais.** Disponível em: < http://www.rets.org.br/?q=node/2313 >. Acesso em: 8 março 2015.

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. . O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira. **Physis** (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

WORLD HEALTH ORGANIZATION. eHealth. Disponivel em: < http://www.who.int/topics/ehealth/en/ > Acesso em: 8 Março 2015.

3

Infraestrutura e disponibilidade de tecnologias da informação e comunicação nos estabelecimentos de saúde no Brasil: preocupações com privacidade e confidencialidade entre gestores, médicos e enfermeiros[1]

Alexandre Fernandes Barbosa2
Alisson Bittencourt[3]
Manuella Maia Ribeiro[4]
Fábio Senne[5]

Introdução

As tecnologias da informação e comunicação (TIC) vêm sendo amplamente adotadas por diversos setores da sociedade. O setor de saúde é uma das áreas que avalia a utilização intensiva das tecnologias como pro-

1 Esse capítulo foi baseado na análise de resultados da pesquisa TIC Saúde 2013. O trabalho completo pode ser encontrado no seguinte endereço: http://cetic.br/pesquisa/saude/.

2 Alexandre Fernandes Barbosa (alexandre@nic.br) é Doutor em Administração de Empresas pela Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (EAESP-FGV) e Gerente do Centro de Estudos sobre as Tecnologias da Informação e Comunicação (Cetic.br).

3 Alisson Bittencourt é Analista de Informações do Centro de Estudos sobre as Tecnologias da Informação e Comunicação (Cetic.br).

4 Manuella Maia Ribeiro é Doutoranda em Administração Pública e Governo pela Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (EAESP-FGV) e Analista de Informações do Centro de Estudos sobre as Tecnologias da Informação e Comunicação (Cetic.br).

5 Fábio Senne é bacharel em Ciências Sociais pela universidade de São Paulo (USP), Mestre em Comunicação pela Universidade de Brasília (UnB) e Coordenador de pesquisas no Centro de Estudos sobre as Tecnologias de Informação e Comunicação (Cetic.br).

motora de uma série de benefícios. Por exemplo, são citados frequentemente como vantagens do uso das TIC: o aumento da qualidade dos tratamentos e eficiência dos serviços de saúde; a redução dos custos de operação de serviços clínicos; a redução de custos administrativos; e a abertura de possibilidades para novas formas de tratamento (CGI.br, 2014).

Compreender a adoção e uso das TIC pelos estabelecimentos de saúde é fundamental para identificar e analisar o estágio de adoção dessas tecnologias na área, bem como para auxiliar na tomada de decisão das organizações públicas e privadas quanto à utilização das tecnologias nas suas atividades. Também é importante conhecer as barreiras para que os profissionais do setor, como médicos e enfermeiros utilizem adequadamente essas ferramentas. Dentre as possíveis barreiras para a adoção das TIC em estabelecimentos de saúde, este capítulo destacará a percepção dos profissionais do setor no Brasil sobre as preocupações com a privacidade e a confidencialidade das informações.

Cabe ressaltar que a adoção de sistemas eletrônicos, especialmente on-line, bem como a ampliação do relacionamento dos atores da área de saúde com os pacientes por meio das TIC, devem levar em consideração as discussões sobre a confidencialidade e privacidade das informações. A garantia do sigilo das informações deve ser um dos princípios que guiam os estabelecimentos de saúde na adoção das TIC. Portanto, identificar o estágio de uso dessas tecnologias se torna basilar para compreender o seu alcance e implicações na confidencialidade e segurança de informação nos dados mantidos pelos estabelecimentos de saúde no país.

Nesse sentido, a Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação em Estabelecimentos de Saúde no Brasil (TIC Saúde) – realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) - traz importantes insumos para compreender o cenário de adoção das TIC em estabelecimentos de saúde no Brasil. A pesquisa é conduzida anualmente desde 2013 e apresenta indicadores relativos ao uso de TIC entre gestores, médicos e enfermeiros de estabelecimentos de saúde públicos e privados. Entre esses indicadores, foram medidas as barreiras para adoção de sistemas eletrônicos por profissionais de saúde. Entre essas dificuldades, um dos temas abordados foi a questão da privacidade e confidencialidade das informações.

O objetivo deste capítulo, portanto, é apresentar os principais resultados da pesquisa TIC Saúde 2013, detalhando indicadores referentes à percepção do papel das preocupações com segurança e confidencialidade das informações na adoção de sistemas eletrônicos em estabelecimentos de saúde brasileiros, por gestores, médicos e enfermeiros.

Para compreender este cenário, este capítulo foi dividido nas seguintes seções:

- Descrição do Cetic.br e das suas atividades;
- A agenda de e-saúde e a pesquisa TIC Saúde;
- Os principais resultados da pesquisa TIC Saúde 2013; e
- A percepção dos gestores, médicos e enfermeiros em relação às preocupações com a segurança e confidencialidade das informações na utilização de sistemas eletrônicos em estabelecimentos de saúde.

Por fim, são apresentadas as considerações finais do trabalho que resumem os desafios para a adoção de TIC no âmbito dos estabelecimentos de saúde no Brasil.

As pesquisas do Cetic.Br

Criado em 2005 para monitorar a adoção das TIC no Brasil, o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação[6] (Cetic.br) é um departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil (CGI.br).

O Cetic.br é responsável por realizar a atribuição do CGI.br de produzir conhecimento capaz de contribuir para o desenvolvimento da Internet no Brasil, através da condução de estudos relacionados ao acesso e uso das TIC no país em diferentes âmbitos da sociedade.

São realizadas periodicamente pesquisas que adotam metodologias baseadas em orientações e parâmetros definidos internacionalmente, por

6 Mais informações em: http://cetic.br.

meio de organismos multilaterais, como a União Internacional de Telecomunicações (UIT), a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), o Instituto de Estatísticas da Comissão Europeia (EUROSTAT) e a Comissão Econômica para a América Latina e Caribe (CEPAL). Além das referências internacionais, o processo de produção de pesquisas e indicadores conta com a contribuição voluntária de especialistas, vinculados a instituições acadêmicas e organizações sem fins lucrativos e de governo. Estes especialistas auxiliam principalmente nas etapas de definições metodológicas e no processo de análise dos resultados.

A partir de 2012, o Cetic.br se tornou um centro regional sob os auspícios da UNESCO, quando assumiu também funções relacionadas à capacitação em metodologias de pesquisa TIC e ao compartilhamento de conhecimentos sobre o desenvolvimento da sociedade da informação, especialmente entre países da América Latina e países de língua portuguesa na África.

Entre os temas investigados pelo Cetic.br está a adoção das TIC no setor de saúde. Tendo como referência indicadores internacionalmente comparáveis, o Cetic.br realizou a Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação em Estabelecimentos de Saúde no Brasil (TIC Saúde) com o objetivo de compreender o estágio de adoção das TIC nos estabelecimentos de saúde brasileiros e sua apropriação pelos profissionais do setor.

A agenda de E-Saúde e a pesquisa TIC Saúde

A e-saúde pode ser definida como a aplicação das TIC no setor de saúde:

> (...) e-Saúde representa o contexto da prática de atenção à saúde facilitada e aperfeiçoada pelo uso das TIC 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 acom-

> panhamento 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. 31).

Assim, a agenda de e-saúde está relacionada à análise sobre o impacto das TIC nos sistemas de saúde. Portanto, tal qual em outros setores da economia, a área de saúde também vem adotando a visão que as TIC podem ser um elemento fundamental para aprimorar seus processos de gestão, como a redução dos custos de operação de serviços clínicos e administrativos (OECD, 2010, p. 12).

Além dos benefícios no âmbito dos processos gerenciais dos estabelecimentos de saúde, outras áreas que vêm recebendo investimentos na adoção das TIC são aquelas ligadas à assistência, garantindo o suporte à decisão clínica, contribuindo para a redução de erros médicos, desenvolvendo formas inovadoras de tratamento e viabilizando a realização de pesquisa e construção de evidências para o fortalecimento do corpo do conhecimento em saúde (OECD, 2010, p. 12).

Desta maneira as TIC podem ser aplicadas na área de saúde em diversas atividades como (OECD, 2010; ITU, 2010; WHO, 2006):

- Coordenação e organização dos processos e gestão da informação internamente aos estabelecimentos de saúde;
- Uso de registros e prontuários eletrônicos e melhor intercâmbio de informações entre profissionais, estabelecimentos e com os pacientes;
- Sistemas que permitem a marcação de consultas on-line e comunicação segura com médicos;
- Campanhas educativas e preventivas a distância;
- Práticas de medicina e saúde pública por meio de suportes móveis.

Nesse contexto, obter dados confiáveis, comparáveis internacionalmente e de forma sistemática para conhecer a infraestrutura tecnológica existente, os serviços e aplicações disponíveis e o uso efetivo que os profissionais fazem das TIC na saúde é fundamental para a geração de

informações que possam contribuir para o subsídio de políticas públicas no setor. Esse é o objetivo da TIC Saúde 2013, que busca compreender o estágio de adoção das TIC nos estabelecimentos de saúde brasileiros e sua apropriação pelos profissionais do setor.

Cabe destacar que a pesquisa possui como objetivos mapear:

- A penetração das TIC nos estabelecimentos de saúde brasileiros, especialmente:
  - A infraestrutura de TIC disponível e a gestão de TI;
  - A disponibilidade de sistemas e aplicações baseados em TIC destinados a apoiar serviços assistenciais e a gestão dos estabelecimentos de saúde.
- A apropriação das TIC por profissionais de saúde, tendo como objetivos específicos avaliar:
  - Atividades realizadas com o uso de TIC e as capacidades/habilidades dos profissionais que as realizam;
  - Motivações e barreiras para a adoção das TIC pelos profissionais de saúde.

A população-alvo do estudo é composta por estabelecimentos de saúde brasileiros. Para efeitos da investigação e do levantamento da população de referência, foram considerados os estabelecimentos presentes no Cadastro Nacional de Estabelecimentos de Saúde (CNES). Assim, a pesquisa tem como escopo os estabelecimentos de saúde públicos e privados cadastrados no CNES, que possuam Cadastro Nacional da Pessoa Jurídica (CNPJ) próprio ou de uma entidade mantenedora, além de instalações físicas destinadas exclusivamente a ações na área de saúde e que possuam ao menos um médico ou um enfermeiro. Além dos gestores (responsáveis por prestar informações sobre os estabelecimentos de saúde), médicos e enfermeiros também fazem parte da população-alvo da pesquisa.

Na pesquisa TIC Saúde 2013 foram entrevistados 1.685 gestores de estabelecimentos de saúde públicos e privados em todo o território nacional, além de 4.180 médicos e enfermeiros vinculados a estes estabelecimentos.

Principais resultados da pesquisa TIC Saúde 2013

A pesquisa mediu diversos indicadores sobre uso e apropriação de TIC em estabelecimentos de saúde no Brasil. Apesar do estudo não focar na privacidade e confidencialidade dos pacientes, uma série de indicadores auxiliam na compreensão do papel da tecnologia na área de saúde e, consequentemente, os desafios para garantir o sigilo das informações. Neste tópico são destacadas as dimensões de infraestrutura e disponibilidade de TIC e os serviços oferecidos ao paciente e formas de troca de informação nos estabelecimentos.

Infraestrutura de TIC nos estabelecimentos de saúde brasileiros

A pesquisa TIC Saúde 2013 revelou que a infraestrutura tecnológica básica está presente na maioria dos estabelecimentos de saúde do Brasil: 83% utilizaram computador e 77% utilizaram internet nos 12 meses anteriores à pesquisa.

O acesso a estas tecnologias é elemento fundamental para a adoção de TIC no setor. A importância do acesso foi ressaltada nos documentos da Cúpula Mundial sobre a Sociedade da Informação (WSIS – *World Summit on the Information Society*), que estabeleceu em seu plano de ação, dentre os seus objetivos e metas, a necessidade de conectar os centros de saúde e hospitais à internet banda larga e utilizar as TIC para aprimorar o atendimento médico, o treinamento, a educação e a pesquisa em saúde.[7]

Há, no entanto, um déficit localizado de infraestrutura, concentrado nos estabelecimentos responsáveis pela atenção básica e ambulatorial (aqueles em que não há internação): 22% não utilizaram computadores nos últimos 12 meses e 29% não utilizaram internet. A pesquisa também revelou que os estabelecimentos públicos de saúde possuem menos infraestrutura de TIC que os privados. Enquanto é praticamente universalizado o acesso a computador e internet nos estabelecimentos privados (100% dos privados utilizaram computadores e 99% acessaram a internet

7 O Plano de Ação da Cúpula Mundial sobre a Sociedade da Informação (WSIS), definido na primeira fase do evento (que ocorreu em 2003, na cidade de Genebra), pode ser acessado no seguinte endereço: http://www.itu.int/wsis/docs/geneva/official/poa.html.

nos 12 meses anteriores à pesquisa), 68% dos estabelecimentos públicos utilizaram computador e pouco mais da metade a internet (57%).

Outros indicadores importantes para avaliar o potencial de adoção de tecnologia nos estabelecimentos são o tipo e a velocidade de conexão à internet. Quanto ao primeiro, nos estabelecimentos que têm acesso à internet, a quase totalidade tem banda larga fixa (92%), sendo que 48% utilizavam conexão via linha telefônica (DSL) e 46% conexão via cabo ou fibra ótica. É importante esclarecer que mais de um tipo de conexão pode ter sido mencionada pelo mesmo estabelecimento. A penetração da banda larga móvel (tecnologia 3G) é de 23% do total dos estabelecimentos com internet, o que indica o uso desta tecnologia como forma de conexão complementar à banda larga fixa pelos estabelecimentos de saúde.

Com relação à velocidade, a pesquisa mostrou que aproximadamente metade dos estabelecimentos tem velocidade acima de 1 Mbps (48%), sendo que entre os privados, de maior complexidade (com internação e mais de 50 leitos) e voltados a Serviço de Apoio à Diagnose e Terapia as proporções estão acima da média geral. É importante ressaltar que, para esse indicador, 28% dos estabelecimentos não responderam o que indica limitações importantes para sua análise.

Com relação à gestão da tecnologia de informação, a pesquisa TIC Saúde 2013 considera a presença de recursos humanos especializados na área de tecnologia da informação (TI) como um indicador relevante para medir a capacidade dos estabelecimentos de saúde em responderem aos desafios da implantação e da implementação de TIC e sistemas de informação. Os resultados mostraram que 22% do total dos estabelecimentos de saúde possuíam departamento ou área de TI, sendo que tal proporção chega a 79% entre aqueles que têm mais de 50 leitos de internação e é de apenas 14% entre os sem internação.

Considerando esses estabelecimentos que possuem área de TI, verificou-se que os privados têm, em geral, mais funcionários que os públicos: 18% dos estabelecimentos públicos têm quatro ou mais funcionários, enquanto que este número estava presente em 33% dos privados. Há mais funcionários também nos estabelecimentos com mais de 50 leitos de internação, nos quais 65% têm quatro ou mais funcionários, em comparação a 19% dos estabelecimentos sem internação.

Na maioria dos estabelecimentos, o principal responsável pelo suporte técnico em informática é um prestador de serviço contratado (63% do total). Por tipo de estabelecimento, há uma diferença no responsável pelo suporte entre os estabelecimentos com mais de 50 leitos de internação, onde 70% têm como principal responsável uma equipe interna do estabelecimento e 26% possuem um prestador contratado. Os estabelecimentos sem internação apresentaram proporções de 22% que contam com equipe própria e 66% que contratam prestadores de serviço.

Assim, é possível afirmar que a maior parte dos estabelecimentos de saúde já possuem equipamentos TIC, possibilitando o armazenamento de informações sobre as suas atividades. Além disso, os responsáveis pela área de TI geralmente são fornecedores externos. Tais aspectos devem ser levados em consideração na implementação de decisões e normas sobre a privacidade e confidencialidade das informações em posse dos estabelecimentos de saúde.

Disponibilidade de TIC

O uso de registros eletrônicos em saúde e a possibilidade de troca de informações entre profissionais e estabelecimentos estão no centro do debate sobre as potencialidades das TIC para a melhoria da gestão do sistema de saúde e da assistência médica.

A Organização Internacional para Padronização (ISO, International Organization for Standardization) define registro eletrônico em saúde como "informação relevante sobre o bem-estar, saúde e atendimento em saúde de um indivíduo que contenha ou virtualmente possa interligar os dados provenientes de múltiplos Registros Médicos Eletrônicos e Prontuários Eletrônicos Pessoais, e que devam ser compartilhados e/ou interoperáveis entre os setores de atendimento em saúde, sendo centrado no paciente".[8]

A informação disponível em formato eletrônico pode ser acessada com maior rapidez e está menos sujeita a problemas como ilegibilidade, ambiguidade e falta de padronização, além de poder estar disponível para diversos profissionais simultaneamente, seja de um mesmo estabelecimento ou não. Isso contribui para o processo de tomada de decisões por parte dos médicos,

8 Em seu relatório técnico ISO 14639-1:2012.

sobretudo em situações nas quais é necessária a atenção de profissionais de diferentes especialidades. A organização da informação permite melhor coordenação da provisão do serviço e maior eficiência no tratamento do paciente, evitando, por exemplo, diagnósticos duplos e diminuindo erros em termos de medicação (OCDE, 2010). Por outro lado, essa troca de dados deve ser precedida de cuidados com a segurança da informação de modo que seja garantida a confidencialidade e a privacidade no uso das TIC.

Com relação à mensuração da disponibilidade de informações e funcionalidades dos sistemas de informação, a TIC Saúde 2013 aponta que 70% dos estabelecimentos que utilizaram a Internet nos 12 meses anteriores à pesquisa possuíam algum tipo de registro eletrônico para informações médicas. Em 48% dos estabelecimentos, o registro dessas informações estava parte em papel e parte em forma eletrônica. Em 22% dos estabelecimentos, declarou-se utilizar registro totalmente eletrônico, sendo que nos estabelecimentos privados essa proporção é de 33%. Por outro lado, 30% dos estabelecimentos fazem os registros totalmente em papel e, neste caso, a proporção é 51% nos estabelecimentos públicos.

Em relação ao tipo de estabelecimento, a utilização de registros totalmente eletrônicos está mais presente nos estabelecimentos de apoio à diagnose e terapia (51%) e aparece com menor frequência nos estabelecimentos com internação, com pouca diferença em relação ao porte: 10% naqueles até 50 leitos e 9% nos de 50 leitos ou mais. Cabe notar que a adoção de soluções de registro completamente eletrônicos representa desafio maior para os estabelecimentos com internação, tendo em vista a complexidade das informações clínicas e administrativas.

A manutenção de informações médicas em formato eletrônico não caracteriza necessariamente, no entanto, a existência, a maturidade e a cobertura do sistema eletrônico nos estabelecimentos. Para compreender estas questões de forma mais aprofundada, é interessante observar o tipo de informação e as funcionalidades disponíveis eletronicamente.

Segundo os dados da TIC Saúde 2013, os registros de dados administrativos, como as informações cadastrais e demográficas (presentes em 79% dos estabelecimentos com acesso à internet) são os mais disponíveis e consultados eletronicamente. Além disso, 49% dos estabelecimentos

que utilizaram internet nos últimos 12 meses possuem resultados de exames laboratoriais em registros eletrônicos e 49% informações referentes a diagnóstico, problemas ou condições de saúde do paciente.

Por outro lado, as informações clínicas estão menos presentes eletronicamente, como aquelas sobre anotações clínicas sobre o atendimento (40%), vacinas tomadas pelo paciente (21%), alergias (31%), sinais vitais do paciente (27%) e anotações de enfermagem (22%).

Quanto ao tipo de estabelecimento, é possível observar que os estabelecimentos com mais de 50 leitos de internação apresentam maiores proporções nos diferentes tipos de dados clínicos sobre os pacientes disponíveis eletronicamente. Exemplo disso são os dados referentes à admissão, transferência e alta, que estão registrados eletronicamente em 39% do total de estabelecimentos que usaram a internet nos últimos 12 meses, mas em 90% dos estabelecimentos com mais de 50 leitos de internação.

Outro conjunto de informações a ser considerado para medir a disponibilidade de registros eletrônicos em saúde nos estabelecimentos se refere às funcionalidades existentes no sistema. Algumas delas, sobretudo vinculadas às atividades gerenciais, estavam presentes em cerca de metade dos estabelecimentos que usaram a internet nos últimos 12 meses, como a capacidade de agendar consultas, exames ou cirurgias (51%), de gerar pedidos de materiais e suprimentos (44%).

As funcionalidades voltadas especificamente, ou em maior parte, para a atenção clínica, estão menos disponíveis nos estabelecimentos. Apesar da possibilidade de, por exemplo, poder listar os resultados de exames laboratoriais de um paciente, em 38% dos estabelecimentos, a solicitação de exames de imagem está disponível em 34% deles, a prescrição médica em 33% e a listagem dos resultados de exames radiológicos de um paciente em apenas 22% dos estabelecimentos.

Locais de acesso e troca de informações e serviços oferecidos ao paciente

A tendência de ampliar a prestação de serviços on-line para pacientes e profissionais e estabelecimentos do sistema de saúde deve ser seguida de uma preocupação sobre a adequação desses serviços para

garantir a confidencialidade e a privacidade das informações, ou seja, é necessário que sejam realizadas precauções para que as informações não sejam acessadas por outras pessoas. Por exemplo, evitando que outras pessoas consigam acessar dados sobre a saúde de pacientes que queiram checar resultados de exames pela internet. Assim, se por um lado a disponibilização e troca de informações on-line pode gerar uma série de benefícios quanto ao acesso sobre dados de saúde tanto por pacientes quanto profissionais do setor, por outro lado também deve ser reforçada a preocupação sobre o sigilo dessas informações. Os resultados da TIC Saúde 2013 revelam o grau de utilização dessas novas formas de interação através do uso das TIC, especialmente a internet.

Quanto aos locais de acesso ao sistema, vale ressaltar que 65% dos estabelecimentos que usaram a internet nos últimos 12 meses possuem pontos de acesso fixos distribuídos pelo estabelecimento, 42% têm rede interna que pode ser acessada por um computador, celular ou *tablet* e 33% declaram ser possível o acesso ao sistema fora do estabelecimento.

Em relação à troca de informações, essa prática ainda é pouco utilizada nos estabelecimentos de saúde brasileiros. Dentre as diferentes funcionalidades de troca de informações, a mais encontrada nos sistemas eletrônicos é informações clínicas para profissionais de saúde de outros estabelecimentos, que está presente em 28% dos estabelecimentos. O envio ou recebimento da lista de medicamentos prescritos para outros estabelecimentos, por sua vez, está disponível em apenas 13% dos estabelecimentos.

A utilização das tecnologias da informação e da comunicação na saúde pode gerar formas inovadoras de assistência ao paciente, permitindo que este tenha acesso às suas informações e, consequentemente, tenha possibilidades de participar mais ativamente da tomada de decisões sobre sua própria saúde (OECD, 2012). Sistemas que permitem a marcação de consultas on-line, comunicação segura com médicos, sistemas de informação controlados pelos pacientes e uso de redes sociais estão entre os aspectos mais inovadores nesse campo (OECD, 2012):

> A presença do estabelecimento na Web, por exemplo, possibilita o uso de ferramentas que podem apoiar a comunicação do estabelecimento com o público em geral e a prestação de serviços de saúde, além da utilização à distância pelos profissionais da saúde do estabelecimento (CGI.br, 2014, p. 137).

Apesar disso, a pesquisa TIC Saúde 2013 aponta que 29% dos estabelecimentos possuem website, o que mostra um potencial para ampliação de uso desse tipo de ferramentas para melhoria dos serviços. No caso dos estabelecimentos públicos, o oferecimento de serviços pode ser realizado também a partir de sites de órgãos de governo, como secretarias de saúde, que costumam canalizar as ações de governo eletrônico. Nesse sentido, os estabelecimentos de saúde públicos podem oferecer esses serviços aos pacientes mesmo sem contar com sites próprios.

A pesquisa TIC Saúde mostrou também que 19% dos estabelecimentos que utilizaram a internet nos últimos 12 meses permitem que o paciente visualize resultados de exames on-line – proporção que é mais alta entre os estabelecimentos de Serviço de Apoio à Diagnose e Terapia (54%). Em relação a outros serviços, os resultados mostram que 18% dos estabelecimentos com acesso à internet permitem agendamentos de exames e 15% de consultas, enquanto apenas 4% permitem a visualização do prontuário.

Portanto, os serviços oferecidos pela internet por estabelecimentos de saúde ainda é pouco difundido no país. Entretanto, essa é uma situação que não ocorre apenas no Brasil. Um estudo realizado em 2013 mostrou que mesmo reconhecendo os potenciais benefícios da telemedicina, os países europeus também se encontram ainda em estágio inicial de desenvolvimento e pouco se conhece do que está realmente sendo aplicado em cada país, apontando como principais barreiras a infraestrutura, legislação, sustentabilidade, fatores culturais e as diferentes línguas (DOERING & COLS, 2013). Assim, é fundamental acompanhar a incorporação dessas funcionalidades ao longo do tempo e na medida em que se estabeleçam no sistema de saúde brasileiro.

Percepção dos profissionais de saúde sobre o papel das preocupações com confidencialidade para a implantação de sistemas eletrônicos

A pesquisa TIC Saúde 2013 investigou também a percepção de gestores, médicos e enfermeiros vinculados aos estabelecimentos de saúde selecionados sobre as possíveis barreiras para a implantação e o uso de sistemas eletrônicos.

Uma série de fatores que poderiam representar obstáculo à adoção de sistemas eletrônicos na gestão de informações de saúde dos pacientes e no apoio ao atendimento foi apresentada aos respondentes da pesquisa, e perguntou-se a eles se cada um daqueles fatores dificultava muito, dificultava, dificultava pouco ou não dificultava a implantação de sistemas nos estabelecimentos de saúde brasileiros. Pretendemos analisar neste capítulo a resposta destes profissionais em relação ao item "*Preocupações com a segurança e confidencialidade das informações*".

A importância de se garantir a segurança e a confidencialidade das informações dos pacientes é uma preocupação que deve ser sempre levada em consideração pelos desenvolvedores de sistemas eletrônicos na área da saúde (VIEIRA, 2014; SHORTLIFFE, 2014). Além disso, a literatura aponta as questões de privacidade e confidencialidade como uma das barreiras para a adoção de aplicativos e sistemas em TIC (RONCHI & SENNE, 2014):

> Muitas das preocupações e cautelas que os pesquisadores ou desenvolvedores expressam, referem-se à obtenção e à troca de informação segura e confiável em saúde, seguindo os requisitos de proteção, confidencialidade, segurança e privacidade da informação, o que nem sempre é verificado nesses aplicativos que hoje dominam o mercado e geram negócios de alto valor financeiro (MARIN, 2014).

Como pode ser observado na Tabela 1, uma proporção razoável dos profissionais demonstrou enxergar as preocupações desta ordem como fatores que dificultam a implantação de sistemas em estabelecimentos de saúde.

Tabela 1 - Proporção de gestores, médicos e enfermeiros, por percepção sore preocupações com segurança e confidencialidade das informações como barreira para implantação e uso de sistemas eletrônicos

Percentual sobre o total de estabelecimentos de saúde[1]

Percentual (%)	Preocupações com a segurança e confidencialidade das informações			
	Dificulta muito	Dificulta	Dificulta pouco	Não dificulta
Gestores	26	27	16	30
Médicos	48	16	11	22
Enfermeiros	27	31	15	27

[1]Base: 1685 estabelecimentos de saúde. Respostas estimuladas. Dados coletados entre fevereiro de 2013 e junho de 2013

É possível notar que entre gestores há uma distribuição mais equilibrada entre os que enxergam estas preocupações como fator que gera grande dificuldade ou dificuldade (53%, se somados) e os que as enxergam como geradora de pouca ou nenhuma dificuldade (46%, também somados).

Já entre médicos, verifica-se uma diferenciação maior entre estes dois "polos" agregados: enquanto 64% dos médicos veem as preocupações com segurança e privacidade como algo que dificulta muito ou dificulta a implantação e o uso de sistemas, 33% acreditam que estas preocupações geram pouca ou nenhuma dificuldade para a adoção de sistemas.

Entre enfermeiros, os resultados indicam, assim como para gestores, certa divisão entre as duas visões: 58% veem as preocupações anteriormente mencionadas como fator que gera muita dificuldade ou dificuldade, e 42% como responsável por pouca ou nenhuma.

É possível afirmar que as preocupações com segurança e privacidade constituem elemento que deve ser considerado no planejamento da implantação de sistemas de saúde, de forma que as soluções tecnológicas passem cada vez mais a garantir o devido sigilo das informações de saúde pessoais e, simultaneamente, garantam maior nível de interoperabilidade necessário a que sirvam, de fato, como ferramenta para a melhoria da qualidade do atendimento.

É importante notar ainda que, entre os diversos itens cujo impacto foi questionado aos profissionais quanto à implantação de sistemas, as preocupações com segurança e confidencialidade das informações aparecem sempre abaixo de outros itens, sobretudo entre médicos e enfermeiros.

Entre gestores, quando observamos a soma das opções "dificulta muito" e "dificulta", a proporção de respostas é maior do que no caso da preocupação com segurança e confidencialidade das informações para diversos itens, como, por exemplo: falta de suporte técnico em tecnologia da informação (61%), falta de treinamento das equipes (60%), equipamentos obsoletos (59%), baixa qualidade da conexão de Internet no estabelecimento (68%), falta de prioridade por parte das políticas públicas governamentais (65%) e falta de recursos financeiros para investimento em tecnologias (74%).

Já entre médicos, esta lista de itens que são vistos como fatores que geram mais dificuldade que as preocupações com segurança e confidencialidade inclui itens como: falta de motivação do corpo clínico para o uso de tecnologias (71%), baixa qualidade da conexão de Internet no estabelecimento (74%), falta de suporte técnico em tecnologia da informação (78%), falta de envolvimento do usuário no desenvolvimento e implantação do sistema (70%), falta de adaptação dos sistemas ou aplicativos eletrônicos para atender às necessidades dos profissionais envolvidos no atendimento, tais como médicos, enfermeiros e gestores (73%), falta de prioridade das políticas internas do estabelecimento (71%), equipamentos obsoletos (75%), falta de recursos financeiros para investimento em tecnologias (78%), falta de treinamento das equipes (81%) e falta de prioridade das políticas públicas governamentais (83%).

Entre enfermeiros, estes fatores que somam maior proporção nas opções "dificulta muito" e "dificulta" incluem: baixa qualidade da conexão de Internet no estabelecimento (66%), falta de envolvimento do usuário no desenvolvimento e implantação do sistema (65%), falta de adaptação dos sistemas ou aplicativos eletrônicos para atender às necessidades dos profissionais envolvidos no atendimento, tais como enfermeiros, enfermeiros e gestores (62%), falta de motivação do corpo clínico para o uso de tecnologias (64%), falta de prioridade das políticas internas do estabe-

lecimento (63%), falta de suporte técnico em tecnologia da informação (71%), equipamentos obsoletos (71%), falta de treinamento das equipes (71%), falta de prioridade das políticas públicas governamentais (72%) e falta de recursos financeiros para investimento em tecnologias (75%).

A observação da importância do papel das preocupações com confidencialidade na avaliação dos profissionais sobre possíveis barreiras à implantação de sistemas é importante, uma vez que ajuda a evidenciar um quadro mais amplo da percepção dos profissionais de saúde do país sobre esta questão.

Considerações finais

Por fim, gostaríamos de sumarizar aqui as contribuições deste capítulo para o debate em torno da adoção de TIC no sistema de saúde brasileiro e as implicações das tecnologias na implantação de sistemas eletrônicos, a partir da percepção dos profissionais envolvidos na gestão e no atendimento sem saúde.

No cenário brasileiro de e-saúde, existem ainda desafios para aprofundar a adoção de sistemas e realizar o potencial das tecnologias na efetiva melhora do atendimento. Do ponto de vista da infraestrutura tecnológica, há defasagens localizadas nos estabelecimentos públicos e sem internação no acesso a computador e internet. Do prisma da disponibilidade de informações e funcionalidades nos sistemas eletrônicos, existe um caminho maior a ser percorrido, sobretudo no que concerne às funções propriamente clínicas ou mais vinculadas ao atendimento clínico em si.

Quanto ao suporte à decisão, a adoção de sistemas com tais ferramentas no ponto de cuidado é ainda incipiente no país, assim como a troca de informações dentro de um estabelecimento e entre diferentes estabelecimentos. Os serviços oferecidos aos pacientes pela internet também se encontram num estágio inicial de desenvolvimento no país, o que não se distingue muito do cenário internacional, em que tais facilidades começam ainda a serem incorporadas nos sistemas de saúde.

Por fim, é importante observar se entre as barreiras para a adoção de sistemas eletrônicos por profissionais de saúde a privacidade e a con-

fidencialidade são percebidas como um fato que dificulta a implantação desse tipo de iniciativa. Entre os profissionais de saúde, os médicos, em sua maior parte, veem as preocupações com segurança e privacidade como algo que dificulta muito ou dificulta a implantação e o uso de sistemas (64%). Entre os gestores e enfermeiros há uma visão parecida: 53% e 58% desses profissionais, respectivamente, apontam as preocupações com a privacidade e a confidencialidade como fatores que geram grande dificuldade ou dificuldade. Além disso, outro ponto que chama a atenção é o fato de as preocupações com privacidade e confidencialidade não serem as mais citadas por esses profissionais. Outras barreiras, como falta de suporte técnico em tecnologia da informação, falta de treinamento das equipes, equipamentos obsoletos, entre outras, tiveram mais citações entre os profissionais.

Os resultados da pesquisa TIC Saúde, portanto, nos ajudam a compreender o cenário geral do acesso e uso de tecnologias nos estabelecimentos de saúde brasileiro. Do ponto de vista das preocupações com privacidade e confidencialidade das informações, os dados permitem uma observação inicial das percepções de gestores, médicos e enfermeiros sobre o tema. Além disso, conhecer o uso e a disponibilidade de TIC nos estabelecimentos de saúde no país auxiliam na compreensão do desafio de garantir tanto os benefícios dessa utilização nas atividades do setor de saúde, a exemplo da interação entre médico e paciente à distância, quanto o sigilo de seus dados de saúde. Essa abordagem, sem dúvida, representa um ponto de partida, e pode ser desenvolvida e aprofundada em estudos futuros para que se possam ampliar as conclusões sobre a melhor forma de equacionar o planejamento da implantação de sistemas de saúde no Brasil.

Referências

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. Alexandre F. Barbosa. São Paulo: CGI.br, 2014. Disponível em: <http://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf>. Acesso em: 20 jan. 2015.

CONSELHO FEDERAL DE MEDICINA. **Cartilha sobre Prontuário Eletrônico:** a Certificação de Sistemas de Registro Eletrônico de Saúde. Brasilia, D.F: CFB/SBIS,2012.

DOERRING, N; LEGIDO-QUIGLEY, H; GLINOS I.A. et al. A success-story in cross-border telemedicine in Europe: the use of intra-operative teleneuromonitoring during aorta surgery. **Health Policy and Technology**., v.2, n.1, p.4-9, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. Health informatics – Capacity-based e-Health architecture roadmap. Part 1: Overview of national e-Health initiatives. Relatório ISO/TR 14639-1:2012. Genebra: ISO, 2012. 54p.

INTERNATIONAL TELECOMMUNICATION UNION. World Telecommunication/ICT Development Report. Monitoring the WSIS targets, 2010. Geneva: ITU, 2010.

MARIN, H. F. **Informática em enfermagem**. São Paulo: EPU, 1995. 100 p.

_____. Tecnologia da informação e comunicação e a segurança do paciente. 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. Alexandre F. Barbosa. São Paulo: CGI.br, 2014. Disponível em: <http://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf>. Acesso em: 20 jan. 2015.

MASSAD, E; ROCHA, A. F. A construção do conhecimento médico. In: MARIN, H. F.; MASSAD, E.; AZEVEDO NETO, R. S. (Ed.) **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico.** São Paulo, 2003, p 21-37.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT-OECD. Improving Health Sector Efficiency: The Role of Information and Communication Technologies. Paris: OECD, 2010.

_____. International Workshop: Benchmarking Adoption and Use of Information and Communication Technologies in the Health Sector. Trends in the Adoption and Use of Health-Related Information and Communication Technologies. Paris: OECD ,2012.

RONCHI, E; SENNE, F. Melhores sistemas de medição são cruciais para concretizar todo o potencial das TIC no setor de saúde. In: COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. Pesquisa sobre o uso das tecno-

logias de informação e comunicação nos estabelecimentos de saúde brasileiros – TIC Saúde 2013, coord. Alexandre F. Barbosa. São Paulo: CGI.br, 2014. Disponível em: <http://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf>. Acesso em: 20 jan. 2015.

SHORTLIFFE, E. H. A evolucação acadêmica da informática biomédica: pesquisa, ensino e prática. 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. Alexandre F. Barbosa. São Paulo: CGI.br, 2014. Disponível em: <http://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf>. Acesso em: 20 jan. 2015.

VIEIRA, A. C. G. 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: <http://www.cetic.br/media/docs/publicacoes/2/tic-saude-2013.pdf>. Acesso em: 20 jan. 2015.

WORLD HEALTH ORGANIZATION. Building foundations for e-health. Genebra: WHO, 2006.

4

Privacidade na internet: o que está por trás das Políticas de Privacidade

Vergilio Ricardo Britto-da-Silva[1]
Edimara Mezzomo Luciano[2]
Guilherme Wiedenhöft[3]

Um breve contexto

O acesso à informação é cada vez mais fácil e instantâneo, permitindo que informações possam ser acessadas em qualquer lugar e a qualquer momento. A cada segundo uma grande quantidade de informações é gerada e enviada para a rede mundial de computadores. Atualmente existem mais computadores, periféricos e tecnologias gerando informações úteis, precisas, oportunas, a um custo menor, em menos tempo, usando menos recursos e gerando riquezas, citam Rezende e Abreu (2011). Os autores afirmam ainda que a informação tem um valor altamente significativo, podendo representar grande poder para quem a detém.

A internet rompeu barreiras geográficas e fez surgir inúmeras empresas que oferecem os mais variados serviços, muitos de forma gratuita, os quais

1 Vergilio Ricardo Britto-da-Silva (vergilio.britto@pucrs.br) é Bacharel em Administração, Mestre em Administração pelo Programa de Pós-Graduação em Administração da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e Pesquisador do Grupo de Pesquisas em Gestão e Tecnologia da Informação, no tema Privacidade.
2 Edimara Mezzomo Luciano é Bacharel em Ciência da Computação, Doutora em Administração e Professora Titular da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).
3 Guilherme Wiedenhöft é Bacharel em Administração/Gestão da TI pela PUCRS, Mestre em Administração pelo Programa de Pós-Graduação em Administração da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e Professor da Universidade do Vale do Rio do Sinos.

podem ser utilizados facilmente pelos usuários. Os serviços mais utilizados são as redes sociais, tais como Facebook, Twitter, e Linkedin, entre outras, e e-mails gratuitos, tais como Gmail e Hotmail, entre outros. Para utilizar estes serviços gratuitos, o usuário precisa fornecer informações pessoais ao se cadastrar, tais como nome, endereço, telefone, cartão de crédito, local de trabalho, entre tantas outras e conforme cada serviço. Estas empresas possuem Políticas de Privacidade, as quais precisam obrigatoriamente ser aceitas pelo usuário para que este possa usufruir destes serviços. Estas Políticas de Privacidade informam aos usuários quais informações são coletadas, como e para qual objetivo poderão ser utilizadas, e como estas informações podem ser compartilhadas pela empresa provedora destes serviços com seus parceiros.

Em função da grande oferta de serviços na internet, bem como pela facilidade de interação que esta propicia através das redes sociais e serviços de e-mails gratuitos, os usuários tem bombardeado a internet com informações pessoais, suas e de seus contatos, sem analisar a ameaça que isto representa para a sua privacidade. Os supostos benefícios em manter-se conectado com a possibilidade de receber atualizações instantâneas têm contribuído para diminuir a percepção do risco envolvido (LUCIANO, MAHMOOD e MAÇADA, 2010).

Muitas empresas varrem a internet à procura de dados dos usuários como hábitos de navegação, preferências em redes sociais e até mesmo localização através de *smartphones*. Esses dados são usados para traçar um perfil do usuário, com o objetivo de direcionar propagandas, ou até mesmo para ataques de Engenharia Social, através dos quais pessoas mal-intencionadas aproveitam-se do descuido ou ignorância dos usuários sobre o assunto para obter informações confidenciais que podem comprometer a segurança de uma organização (LUCIANO e KLEIN, 2014). Ao revelarem dados dos usuários, estes serviços podem violar a privacidade destes.

Estima-se que grande parte dos usuários destes serviços não lê a Política de Privacidade correspondente, e acaba aceitando os termos impostos, uma vez que não aceitar tal política implica em não poder utilizar o serviço. Entre os fatores que fazem com que estes documentos não sejam lidos está o fato de que estes são muito extensos, requerendo dispêndio de tempo para leitura, o que acaba por reduzir a quantidade de usuários que os leem. A confiança que os usuários têm em relação à empresa

fornecedora do serviço é outro fator determinante para a redução do risco percebido relacionado ao fato de aprovar algo que não foi lido: quanto mais os usuários confiam em uma determinada organização ou serviços, menos atentos ficarão a eventuais termos abusivos nas suas políticas de privacidade, e mais as aceitarão sem ler.

Ao aceitar a Política de Privacidade do serviço que pretende utilizar, o usuário concede poderes às empresas provedoras deste serviço, que podem colocar em risco a privacidade do usuário. Por exemplo, os usuários de um determinado serviço de compartilhamento de imagens, ao enviarem para o site uma foto, de acordo com o Contrato de Licença do Serviço, concedem automaticamente permissão para que a empresa utilize a foto como bem entender, até mesmo licenciando a foto para outras empresas. Isso quer dizer que este usuário pode ter publicado uma foto de sua família neste serviço, como forma de compartilhar um momento com seus contatos e esta mesma foto estampar uma campanha publicitária de uma empresa sem que o usuário soubesse previamente disso e sem receber dividendos por esta fotografia. No entanto, não dá para dizer que esta publicação não foi autorizada: se na política de privacidade consta a possibilidade de utilização da foto e o usuário deu o seu "de acordo", ele concordou previamente com a utilização da foto.

Alguns países têm promulgado leis que estabelecem controles na coleta, processamento e transmissão de dados pessoais. Dependendo da respectiva legislação nacional, tais controles podem impor responsabilidades sobre aqueles que coletam, processam e disseminam informações pessoais. No Brasil, a Constituição Federal de 1988, em seu Artigo 5º diz que "são invioláveis a intimidade, a vida, a honra e a imagem das pessoas, assegurando o direito e a indenização pelo dano material ou moral decorrente de sua violação".

A preocupação das empresas que mantêm redes sociais e serviços de e-mails gratuitos com as políticas de privacidade vêm no sentido da sua proteção em relação à legislação, pois elas constituem o seu argumento de defesa em situações de discussão acerca de violação da privacidade. Segundo Westin (1967), estudioso do tema por mais de 40 anos, a privacidade pode ser entendida como o conjunto de informações acerca do indivíduo, o qual ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições, sem a isso ser le-

galmente sujeito. Desta forma, as políticas de privacidade de redes sociais e serviços de e-mails gratuitos podem induzir o usuário para que este 'decida' por não manter em seu exclusivo controle as suas informações.

Por que se preocupar com privacidade na internet

Conforme já comentado, muitos usuários não leem a política de privacidade, dando o aceite e a concordância sem sequer saber o que a empresa provedora do serviço pode fazer com as suas informações, e assim sem ficar ciente, segundo Klein (2014), da severidade da ameaça à sua privacidade ou da possibilidade que a violação ocorra. Já outros usuários leem e decidem aceitar as cláusulas mesmo assim. Entre as razões para isso podem estar tanto a crença de que os riscos são pequenos quanto o fato de considerarem que mesmo que os riscos existam os benefícios os superam.

Em relação à primeira razão, a dos riscos (não) percebidos, é preciso ponderar que esta é uma percepção, e como toda percepção, é individual. Desta forma, fatores de contexto, culturais ou experiência pregressas podem fazer com que se perceba maior ou menor risco. Mas a falta de visão do todo pode falsear a percepção de risco, conforme pode ser observado na pesquisa feita por Acquisti e Grossklags (2005). Os autores observaram em sua pesquisa que quando eles perguntaram a pessoas sobre partes isoladas de informações pessoais, elas não estavam preocupadas se estas informações, quando conectadas, poderiam identificá-las.

E é justamente esta falta de percepção do todo que as empresas têm na coleta, armazenamento e venda de informações o seu negócio: as informações sobre um indivíduo são coletadas em redes sociais, em serviços de e-mail gratuitos, em buscadores de internet, e vão montando um conjunto muito detalhado de informações sobre este indivíduo, detalhando características, hábitos e práticas triviais de milhões de pessoas, revelando informações que podem passar despercebidas até mesmo pelos próprios usuários que forneceram estas informações, o que caracteriza uma ameaça à privacidade destes usuários. Nesta base de dados, há uma linha para cada indivíduo dos quais é possível coletar informações, e a cada rastro que ele deixa na internet (*log*) pode originar mais colunas

de informações a seu respeito, incluindo tanto opiniões sobre produtos ou serviços como posicionamentos políticos, manifestações e que tipo de assunto ele busca em provedores de internet (é preciso dizer, no entanto, que embora estas informações estejam disponíveis do ponto de vista computacional, nem todos os provedores de serviço as coletam). Esta base de dados sobre indivíduos pode ser usada por esta mesma organização para uma vender produtos ou serviços a estes indivíduos sobre os quais este não solicitou informações, mas podem ser também utilizadas para espionar ou prejudicar este indivíduo, por exemplo, utilizando as informações para chantagem ou para atos decorrentes da posse desta informação. Isto pode advir da empresa que montou as bases de dados, ou esta pode vender ou trocar estes dados com outras organizações privadas, públicas ou mesmo com o governo.

A segunda razão para a concordância à política de privacidade sem a ler ou ignorando os riscos à violação de sua privacidade é baseada no que Rose (2006) define como visão de troca, neste caso a troca das informações pelo serviços gratuitos. Observa-se então que os serviços são gratuitos do ponto de vista econômico/financeiro, já que não envolvem pagamento monetário, mas uma troca pelo fornecimento de informações. Acquisti e Grossklags (2005) afirmam que os indivíduos estão dispostos a trocar a privacidade por conveniência ou negociar a liberação de informações pessoais em troca de recompensas relativamente pequenas. A informação é um dos mais importantes ativos de uma empresa, e assim como qualquer outro ativo, é essencial para os negócios da organização e necessita ser protegida adequadamente. O mesmo ocorre com informações de indivíduos, mesmo que para estes as perdas possam não ser econômicas. Esta importância muitas vezes só é reconhecida quando a informação é perdida, roubada, destruída ou quando uma informação privada se torna pública sem o consentimento dos envolvidos. Atualmente, com os ambientes de negócio cada vez mais interconectados, a informação está exposta a um crescente número e uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005). O custo de proteger a informação contra uma ameaça deve ser menor do que o custo de recuperação desta informação se esta for atingida. Para se apurar este custo deve-se considerar não somente o custo financeiro, mas o impacto gerado para a reputação

da organização ou do indivíduo: violações de privacidade de alto impacto podem tanto acabar com uma organização quanto com um indivíduo.

Organizações coletam dados de seus usuários para fins econômicos, podendo, inclusive, conforme descrito em suas políticas de privacidade, vender as informações coletadas conforme acharem conveniente. Assim, o direito à privacidade dos usuários pode estar ameaçado. Está cada vez mais difícil manter a privacidade das pessoas que utilizam a rede mundial de computadores, na qual é possível encontrar centenas de sites vendendo listas de contatos e de e-mails. Antes do uso massivo da internet a privacidade também era violada. Por exemplo, era possível adquirir um CD-ROM com telefones de todos os usuários de telefonia de um importante estado, mesmo daquelas que pediam formalmente para que seus telefones não fossem divulgados, entre elas grandes empresários, políticos e atores. Da mesma forma, ao fazer a assinatura de uma revista de um grande grupo editorial, você passava a receber mala-direta pelo correio de um grande número de serviços, mesmo que tivesse marcado a opção de não divulgação dos seus dados quando da assinatura da revista. Estes dois casos são reais, e foram testados pelos autores.

Com os frequentes avanços da Tecnologia da Informação (TI) e o crescimento da internet, os serviços oferecidos através da internet coletam as mais variadas informações de seus usuários, o que pode colocar em risco a privacidade destes usuários. Os serviços de redes sociais Facebook, Twitter e Linkedin, bem como os de e-mail gratuito Gmail e Hotmail, são os mais populares e os mais utilizados no mundo, somando cerca de 3,2 bilhões de usuários. Muitos fatores contribuem para que as informações privadas dos usuários acabem vazando na internet, sendo um dos principais o fator humano. Os usuários não conseguem manter-se atualizados sobre as ameaças à segurança e privacidade existentes, em função de que estas estão em constante mudança.

Os usuários destes serviços, talvez por falta de conhecimento acerca dos riscos a sua privacidade envolvidos e pela percepção de confiança que têm em relação às empresas provedoras, de forma automática aprovam a Política de Privacidade destes serviços, sem saber que estão autorizando que suas informações privadas sejam manipu-

ladas e utilizadas da forma que estas empresas desejarem, o que pode ser uma brecha para invasão de privacidade destes usuários. Por invasão de privacidade entenda-se a violação de aspectos ou espaços que estão relacionados às particularidades de determinada pessoa, compreendendo-se o privado como o que está de fora da esfera pública (TEJERA, 2006).

Conceitos importantes

Esta seção aborda alguns conceitos fundamentais para o entendimento dos dados coletados e cuja análise está presente na seção seguinte.

Proteção de informações

Com grande capacidade de adicionar valor aos processos, produtos e serviços das empresas, a informação se tornou um recurso cada vez mais crítico para o alcance dos objetivos organizacionais. Estes recursos precisam ser protegidos contra ameaças que possam causar a sua indisponibilidade ou divulgação não autorizada. Sêmola (2003, p. 45) definiu Informação como "um conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais".

É preciso preservar os ativos de informação levando em conta três objetivos fundamentais, de acordo com Luciano e Klein (2014):

a) **Confidencialidade**: garantia de que o acesso à informação é restrito a seus usuários legítimos;

b) **Integridade**: garantia de criação legítima e da consistência da informação ao longo do seu ciclo de vida, em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações;

c) **Disponibilidade**: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.

Para que se possa mensurar claramente o escopo da proteção da privacidade, alguns conceitos precisam ser introduzidos (com base em SÊMOLA, 2003, e ABNT, 2005):

Ativos da informação: todo elemento que compõe os processos que manipulam e processam a informação, considerando a própria informação, o meio em que é armazenada, os equipamentos em que é manuseada, transportada e descartadas são formados por base de dados e arquivos, contratos e acordos, documentação de sistemas, manuais de usuários, materiais de treinamento, procedimentos de suporte, planos de continuidade, entre outros;

Ameaças: um evento ou atitude indesejável, tais como um roubo, incêndio, ataque de vírus, que potencialmente remove, desabilita, danifica ou destrói um recurso; são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade;

Vulnerabilidades: fragilidade associada a ativos que manipulam informações, que quando explorada por ameaças permitem a ocorrência de um incidente de segurança; são elementos passivos, precisando de uma ameaça para provocar um incidente. Podem ser físicas, que compreendem as precariedades das instalações prediais; naturais, tais como tempestades e terremotos; de hardware, que são as falhas nos recursos de tecnologia; de software, falhas na instalação ou configuração que causam acessos indevidos e vazamento de informações e humanas, causadas por falta de treinamento, omissões ou sabotagens;

Riscos: representam a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios;

Incidentes: evento causado por uma ameaça, que explora uma vulnerabilidade, levando a perda de confidencialidade, integridade e disponibilidade, gerando impacto aos processos de negócios da empresa. Sua gravidade é medida pelo seu impacto.

Desta forma, a proteção da privacidade envolveria a redução da vulnerabilidade a ameaças dos ativos de informação, reduzindo o risco de incidentes envolvendo a divulgação não autorizada de informações.

Privacidade na internet

Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles é comunicada aos outros (WESTIN, 1967; ROSE, 2006). Segundo Shin (2010), privacidade no contexto dos Serviços de Redes Sociais pode ser definida como o controle sobre o fluxo de informações pessoais de alguém, incluindo a transferência e troca de informações. Silva (2011, p. 206) afirma que a violação à privacidade constitui, em algumas hipóteses, ilícito penal.

Atualmente a privacidade dos usuários de redes sociais e e-mails gratuitos está cada vez mais exposta. Shin (2010) afirma que os dados pessoais sobre os usuários de serviços de redes sociais tornam-se disponíveis ao público de uma forma sem precedentes, incluindo grandes quantidades de imagens digitais e vídeos. O autor afirma ainda que os usuários enfrentam uma possível perda de controle sobre a forma como os outros irão usar os seus dados uma vez publicados na rede, e que conversas entre usuários podem ser pesquisadas, registradas indefinidamente, replicadas e alteradas, podendo inclusive ser acessadas por outros usuários sem o conhecimento das pessoas na conversa. Para o autor (2010), qualquer um que viole a segurança de um site de rede social abre a porta para o acesso fácil a informações privadas pertencentes a qualquer usuário. Segundo o autor, na prática os usuários muitas vezes esquecem ou ignoram as questões de segurança e privacidade dos sites destes serviços.

O Departamento de Proteção e Defesa do Consumidor (DPDC) do Ministério da Justiça do Brasil, através da Escola Nacional de Defesa do Consumidor, lançou a segunda edição do Caderno de Investigações Científicas "Proteção de Dados Pessoais: Para Além da Informação Creditícia", com o objetivo de subsidiar a reflexão sobre a titularidade do consumidor sobre seus próprios dados pessoais. No capítulo "Princípio de Proteção de Dados Pessoais" consta a publicação mais recente dos *Fair Information Principles*, realizada pelo Departamento de Segurança Interna dos Estados Unidos no ano de 2008, compostos por princípios que devem ser seguidos para garantir a privacidade dos dados pessoais

coletados pelas empresas. Os cinco princípios são transcritos no Quadro 1, a seguir.

Quadro 1 – *Fair Information Principles*

Princípio	Descrição
Transparência	O tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento
Qualidade	Os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade
Finalidade	Qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)
Livre acesso	O indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos
Segurança física e lógica	Os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Fonte: Departamento de Segurança Interna dos EUA apud Schwaig, Kane e Storey (2006)

Estes cinco princípios foram utilizados como base para analisar as Políticas de Privacidade e Termos de Uso dos serviços objetos deste estudo.

O que está por trás das Políticas de Privacidade e Termos de Uso?

As mídias sociais podem ser definidas como "a interação completa via internet", com um impacto avassalador na vida humana (RAMALHO, 2010, p.11). Com tamanho impacto, as empresas e as atividades econômicas não ficariam de fora da exploração comercial deste serviço. Segun-

do o autor, muitas redes sociais na internet têm uma população que as colocariam em segundo ou terceiro lugar no *ranking* de população dos países". Entre as redes sociais mais utilizadas estão o Facebook, Linkedin e Twitter.

O Facebook, que foi originalmente chamado Thefacebook, foi criado por Mark Zuckerberg enquanto estudava em Harvard University, focado nos alunos que estavam terminando o *High School* e os que estavam entrando na Universidade. Segundo Recuero (2009), o Facebook é hoje um dos sistemas com maior base de usuários no mundo. O Facebook funciona através de comunidades e perfis, nos quais é possível acrescentar módulos de aplicativos, tais como jogos e ferramentas. Segundo a autora, uma das inovações do Facebook foi permitir a criação de aplicativos para o sistema pelos usuários. O Facebook ampliou de 901 milhões para 1,23 bilhão o número de usuários ativos da rede social, tendo mais de 300 milhões de fotos postadas diariamente no serviço (PORTAL UOL, 2014). Segundo informado no site, 61,2 milhões de usuários são brasileiros, o que corresponde a 4,98%.

Outra rede social muito utilizada na Internet é o Twitter, um serviço de *microbloggin*, assim denominado pois permite que sejam escritos pequenos textos a partir da pergunta "*What's happening*?". Esta rede social é utilizada como um diário, permitindo aos usuários enviar textos com até 140 caracteres, chamados de *twittes*, sobre o que está fazendo num dado momento, bem como receber atualizações pessoais de seus contatos. Os *twittes* enviados podem ser protegidos para que somente os seguidores autorizados possam ler, ou caso o usuário não configure seu perfil desta forma, suas mensagens ficam expostas a todos os usuários desta rede social.

A rede social Linkedin é utilizada como uma rede de relacionamento profissional, possibilitando que seus usuários compartilhem seus currículos, oportunidades de emprego e contatos profissionais. É um serviço gratuito que está disponível a partir da realização de um cadastro, com fornecimento de informações pessoais do usuário.

As Políticas de Privacidade do Facebook, Twitter, Linkedin, Gmail e Hotmail foram analisadas sob a ótica dos *Fair Information Principles*, publicados pelo Departamento de Segurança Interna dos Estados Unidos

e citados pelo Ministério da Justiça do Brasil na segunda edição do Caderno de Investigações Científicas, Proteção de Dados Pessoais: Para Além da Informação Creditícia, compostos por cinco princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelas empresas. A escolha destas redes sociais e serviços de e-mails gratuitos teve como critério o fato de que estes serviços são os mais utilizados no mundo, conforme pesquisas de portais de notícias.

Informações solicitadas no cadastro

Conforme pode-se verificar no Quadro 2, o serviço que coleta a maior quantidade de informações é Facebook (30), seguido de Linkedin (30), Gmail (16), Hotmail (14) e Twitter (13). Fica claro também que os tipos de dados mais coletados pelos serviços de redes sociais são os dados Não Obrigatórios, enquanto que nos serviços de e-mail gratuitos os dados mais coletados são os Obrigatórios. O tipo de dado coletado em maior quantidade de forma obrigatória são os Dados Pessoais, enquanto que o tipo de dado coletado em maior quantidade de forma não obrigatória são os Dados de Localização.

Quadro 2 – Resumo das informações coletadas

Quantidade de dados coletados em cada serviço										
Tipos de dados	FACEBOOK		TWITTER		LINKEDIN		GMAIL		HOTMAIL	
	Obr	NObr	Obr	NObr	Obr	NObr	Obr	NObr	Obr	NObr
Acadêmico		3			1	1				
Família		1						1		1
Hábitos		1				1				
Localização		7		2	2	4	2	3	2	2
Pessoal	7	3	4	1	4	8	7		7	
Técnicos	6			6		6		1		
Trabalho		2			2	1		2		2
Subtotal	**13**	**17**	**04**	**09**	**09**	**21**	**09**	**07**	**09**	**05**
TOTAL	30		13		30		16		14	

Legenda: Obr = Obrigatórios; NObr = Não obrigatórios
Fonte: Dados da pesquisa (2015)

O Quadro 2 mostra ainda que o serviço que coleta a maior quantidade de dados de forma obrigatória é o Facebook (13), seguido por Gmail (09), Hotmail (09), Linkedin (09) e Twitter (04). Os dados técnicos indicam as informações coletadas de forma automática no momento em que os usuários acessam o site dos serviços, quais sejam IP do equipamento utilizado para acesso, sistema operacional, configurações de *hardware* e informações sobre o *browser* utilizado. A coleta destes dados é transparente para os usuários, que não percebem que os mesmos estão sendo coletados.

Política de Privacidade do Twitter

A Política de Privacidade do Twitter descreve as políticas e os procedimentos a respeito da coleta, uso e divulgação das informações coletadas dos usuários que enviam informações para o Twitter quando postam um *tweet* através do site, via SMS, aplicativos e APIs. Ao utilizar qualquer um dos serviços do Twitter, o usuário concorda automaticamente com a coleta, transferência, adaptação ou alteração, armazenamento, divulgação e outros usos de suas informações. Ao realizar o cadastro para utilização desta rede social, o usuário deverá informar obrigatoriamente nome, e-mail, senha e usuário. Posteriormente ele poderá ainda fornecer informações adicionais, tais como número e operadora de celular, localização (país, região), catálogo de endereços e foto. Por padrão, o perfil do usuário permite que qualquer outro usuário possa visualizar as informações postadas, e as informações públicas dos usuários são divulgadas amplamente de forma imediata pelo Twitter e outros serviços que reproduzem o seu conteúdo, tais como o Facebook.

Os serviços do Twitter são projetados para compartilhar as informações dos usuários com o mundo, e o usuário autoriza que a maioria das informações fornecidas sejam tornadas públicas. Por padrão o Twitter sempre torna públicas as informações que o usuário fornece, e segundo o que está descrito na Política de Privacidade, geralmente o Twitter oferece configurações de conta que permitem que o usuário torne as suas informações mais privadas, o que inclui não somente os *tweets* enviados e favoritos, mas também listas criadas pelo usuário, as pessoas que segue e muitas outras informações resultantes do uso deste serviço. Os servidores do Twitter registram automaticamente informações dos usuários

a partir do uso dos serviços. Estas informações podem conter o endereço IP, sistema operacional, tipo de navegador, páginas visitadas e operadora do dispositivo móvel.

O site do Twitter utiliza *cookies* para coletar informações referentes aos sites acessados pelos seus usuários. São utilizados *cookies* de sessão, os quais são armazenados na memória, perdendo as informações no momento em que o usuário fecha o navegador web, e também são utilizados *cookies* persistentes, que são aqueles que são gravados no disco rígido do computador.

As informações coletadas podem ser compartilhadas indevidamente com outros sites, o que pode acabar colocando em risco a privacidade dos usuários. Segundo o que está descrito em sua Política de Privacidade, a empresa utiliza alguns serviços de terceiros, como, por exemplo, para hospedar *blogs* e *wikis*. Estas empresas também podem coletar informações dos usuários através do Twitter, que pode ainda compartilhar com suas empresas fornecedoras as informações pessoais de seus usuários. Ao aceitar a Política de Privacidade do Twitter, além de autorizar todos os procedimentos detalhados acima, o usuário concorda ainda que, caso a empresa seja envolvida em fusão, falência ou aquisição, poderá vender ou transferir as informações de seus usuários como parte destas transações.

O Quadro 3 mostra a análise da Política de Privacidade do Twitter de acordo com os *Fair Information Principles.*

Quadro 3 – Resumo da análise da Política de Privacidade do Twitter

Princípio	Análise quanto ao princípio	Motivo
Transparência	Não atende	Não informa especificamente como os dados serão tratados
Qualidade	Atende parcialmente	A Política diz que os dados podem ser manipulados, com isso corre-se o risco de que as informações deixem de ser fiéis à realidade
Finalidade	Não atende	Os dados dos usuários podem ser coletados pelas empresas parceiras
Livre acesso	Atende parcialmente	O usuário não tem acesso aos dados coletados pelas empresas parceiras
Segurança física e lógica	Atende parcialmente	Ao compartilhar os dados com empresas parceiras, o provedor perde o controle sobre os riscos à privacidade dos usuários

Fonte: Dados da pesquisa (2015)

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Twitter atende parcialmente três princípios e não atende aos outros dois.

Política de Privacidade do Linkedin

Quando o usuário registra uma conta no Linkedin, deve fornecer obrigatoriamente nome, sobrenome, e-mail e senha. Após a validação do usuário, para que este possa utilizar o serviço oferecido por esta rede social, deverá informar, obrigatoriamente, país onde mora, código postal, empresa onde trabalha e cargo que ocupa. Outras informações complementares podem ser adicionadas ao perfil do usuário do Linkedin.

O provedor deste serviço recebe automaticamente a URL do site do qual o usuário veio e do site para o qual irá quando sair do site do Linkedin. Além disso, os anunciantes recebem a URL da página em que o usuário estava ao clicar em um anúncio veiculado pelo Linkedin, que também recebe o endereço IP e o sistema operacional do computador do usuário, o tipo de navegador utilizado, padrões de e-mail, tipo de aparelho celular e sistema operacional do aparelho (caso o usuário esteja acessando o Linkedin por celular), assim como o nome do provedor de internet ou da operadora de celular.

O Linkedin também poderá receber dados referentes à localização do usuário que possam ter sido transmitidos pelos serviços de terceiros ou dispositivos com GPS ativado. Segundo a Política de Privacidade do Linkedin, o usuário concede a este provedor direito não exclusivo, irrevogável, mundial, perpétuo, ilimitado e transferível, totalmente isento de *royalties*, de copiar, preparar trabalhos derivativos, melhorar, distribuir, publicar, excluir, guardar, acrescentar, processar, analisar, utilizar e comercializar, de qualquer maneira atualmente conhecida ou descoberta no futuro, quaisquer informações fornecidas pelo usuário, direta ou indiretamente, ao Linkedin, incluindo, entre outros, qualquer conteúdo gerado por usuário, ideias, conceitos, técnicas ou dados relacionados aos serviços que o usuário apresentar ao Linkedin, sem nenhum outro consentimento, aviso e/ou remuneração ao usuário nem a nenhum terceiro.

O Quadro 4 mostra a análise da Política de Privacidade do Linkedin de acordo com os *Fair Information Principles*.

Quadro 4 – Resumo da análise da Política de Privacidade do Linkedin

Princípio	Análise quanto ao princípio	Motivo
Transparência	Não atende	Conforme descrito na Política, o Linkedin pode realizar quaisquer operações com as informações coletadas, não especificando o que será feito
Qualidade	Não atende	Como as informações podem ser vendidas, não é possível garantir que após a venda permaneçam fiéis ao que fora publicado pelo usuário
Finalidade	Não atende	A Política informa que as informações podem ser comercializadas
Livre acesso	Atende parcialmente	Não é possível ter acesso às informações comercializadas com terceiros
Segurança física e lógica	Não atende	Ao comercializar as informações, não é possível protegê-las dos riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado

Fonte: Dados da pesquisa (2015)

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Linkedin atende parcialmente um dos princípios e não atende aos outros quatro.

Política de Privacidade do Facebook

Ao realizar o cadastro no site do Facebook, o usuário deverá informar nome, endereço de e-mail, data de nascimento e sexo. Informações adicionais podem ser inseridas pelo usuário, entre elas telefone, endereço, cidade natal, cidade onde mora, religião, empresa onde trabalha, cargo ocupado, formação acadêmica, foto, interesses, etc. Por padrão o perfil do usuário do Facebook é criado como público, sendo possível que qualquer usuário desta rede social possa visualizar as informações inseridas. Após a criação do perfil, a visualização pode ser modificada para grupos mais restritos.

O Facebook, além das informações inseridas diretamente pelos usuários, recebe informações quando os usuários interagem com a rede social, quando olham a linha do tempo de outra pessoa (chamados de amigos pela rede social), enviam ou recebem mensagens, procuram por um amigo ou uma página ou usam um aplicativo móvel do Facebook.

Quando o usuário publica fotos ou vídeos, dados relacionados são recebidos pelo Facebook, tais como hora, data e local em que a foto ou vídeo foram postados. Dados do computador, do telefone celular e de outros dispositivos que o usuário utiliza para acessar o Facebook são coletados. Essas informações podem incluir endereço IP, servidor de internet, localização, tipo de navegador, páginas que são visitadas. Quando o usuário acessa algum jogo, aplicativo ou site que utilize a plataforma do Facebook, as informações são enviadas ao Facebook através de *cookies*, podendo incluir data e hora em que o site foi acessado, sistema operacional e, caso o usuário esteja conectado ao Facebook, sua identificação de usuário.

O Facebook recebe informações sobre o usuário através de seus amigos, quando estes carregam informações de contato deste usuário, publicam uma foto, marcam o usuário em uma foto ou atualizações de *status*, ou quando o adicionam a um grupo. Além disso, as informações que um usuário compartilha pode ser compartilhadas novamente. Isso significa que se um usuário compartilha uma informação no Facebook, qualquer pessoa que puder vê-la, poderá compartilhá-la com outros usuários. Através de anunciantes parceiros, clientes e outras fontes que ajudam a fornecer anúncios, o Facebook pode receber informações de seus usuários. Um anunciante pode informar como um usuário respondeu a um anúncio no Facebook ou em outro site. O Facebook pode usar as informações que recebe sobre seus usuários da seguinte forma:

Como parte dos esforços para manter os produtos, serviços e integrações do Facebook seguros e protegidos;

Para proteger os direitos ou propriedades do Facebook e de outros;

Para fornecer recursos e serviços de localização, como informar o usuário e seus amigos quando algo está acontecendo nas redondezas;

Avaliar ou saber a eficiência dos anúncios que os usuários veem, incluindo fornecer anúncios relevantes para estes usuários;

Para fazer sugestões aos usuários do Facebook, tais como sugerir que outros usuários adicionem alguém como amigo porque este importou o mesmo endereço de e-mail ou sugerir que um usuário marque um amigo em uma foto que ele carregou e na qual este amigo esteja presente;

Para operações internas, que incluem correção de erros, análise de dados, testes, pesquisa, desenvolvimento e melhoria do serviço.

A Política de Privacidade do Facebook informa ainda que os jogos, aplicativos e sites são criados e mantidos por outras empresas e desenvolvedores que não fazem parte do Facebook, e por esta razão os usuários devem ler os Termos de Serviço e as Políticas de Privacidade destas empresas.

O Quadro 5 mostra a análise da Política de Privacidade do Facebook de acordo com os *Fair Information Principles*.

Quadro 5 – Resumo da análise da Política de Privacidade do Facebook

Princípio	Análise quanto ao princípio	Motivo
Transparência	Atende parcialmente	Um aplicativo instalado por um amigo da lista do usuário pode ter acesso aos seus dados deste usuário, mesmo que ele não o tenha instalado
Qualidade	Atende parcialmente	A Política não informa que tipo de tratamento de informações as empresas parceiras podem realizar
Finalidade	Não atende	O Facebook compartilha informações dos usuários com empresas de marketing para realizar publicidade dirigida
Livre acesso	Não atende	O Facebook não possibilita que os usuários corrijam informações incorretas a seu respeito quando estas são publicadas por outros usuários
Segurança física e lógica	Não atende	Uma vez que informações dos usuários são compartilhadas com empresas parceiras, o Facebook não tem como garantir a privacidade dos dados

Fonte: Dados da pesquisa (2015)

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Facebook atende parcialmente dois princípios e não atende aos outros três.

Política de Privacidade do Gmail

Ao criar uma nova conta no Gmail, o usuário deverá informar, obrigatoriamente, nome de usuário, senha, nome, sobrenome, e-mail alternativo, sexo, data de nascimento, telefone celular, país onde está localizado. O Gmail solicita uma confirmação de cadastro, que pode ser feita através do e-mail alternativo, ou enviando um código de validação por mensagem de texto para o telefone celular. Após a confirmação de cadas-

tro, o usuário poderá a seu critério informar endereço, telefone comercial e residencial, cidade e país onde mora, estado civil, escola ou faculdade onde estudou, empresa onde trabalha e cargo. Por padrão estas informações são públicas, sendo visíveis através de buscas mesmo para quem não tem conta no Gmail.

Além das informações inseridas pelo próprio usuário, o Gmail coleta dados a partir da utilização do seu serviço. São coletadas informações sobre o *hardware* utilizado, detalhes de como o usuário usou os serviços do Google, como sites visitados e pesquisas realizadas. Com a utilização dos serviços através de dispositivos móveis, são coletadas informações de telefonia como número de telefone, números chamados, horário e data das chamadas. *Cookies* também são utilizados para a coleta de informações. Segundo a Política de Privacidade do Gmail, as informações dos usuários são compartilhadas com empresas, organizações ou indivíduos externos ao Google, além de administradores de domínios, os quais têm acesso às informações da conta dos usuários, inclusive dados de e-mails. Caso o Google seja envolvido em uma fusão, aquisição ou venda de ativos, as informações pessoais de seus usuários poderão ser transferidas, ou submetidas a uma nova Política de Privacidade.

O Quadro 6 mostra a análise da Política de Privacidade do Twitter de acordo com os *Fair Information Principles.*

Quadro 6 – Resumo da análise da Política de Privacidade do Google

Princípio	Análise quanto ao princípio	Motivo
Transparência	Não atende	Não é informado como as empresas parceiras tratam as informações dos usuários
Qualidade	Não atende	Não é possível atender a este princípio ao compartilhar as informações com outras empresas
Finalidade	Atende parcialmente	Não atende à restrição de transferência de dados pessoais a terceiros
Livre acesso	Atende parcialmente	O usuário não tem acesso às informações armazenadas por empresas parceiras
Segurança física e lógica	Não atende	Ao compartilhar as informações com empresas terceiras, não é possível atender este princípio

Fonte: Dados da pesquisa (2015)

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Google atende parcialmente dois princípios e não atende aos outros três.

Política de Privacidade do Hotmail

Para realizar o cadastro de uma conta de usuário no Hotmail, deve-se inserir informações obrigatórias, tais como: usuário, senha, nome e sobrenome, e-mail alternativo, sexo, data de nascimento, código postal, país onde mora, e informações adicionais podem ser inseridas após a criação da conta, tais como: telefone comercial e residencial, empresa onde trabalha, cargo que ocupa, tipo de relacionamento em que está envolvido e país da localização atual. Segundo a Declaração de Privacidade *on-line* da Microsoft, provedora do serviço de e-mail do Hotmail, as informações coletadas podem ser combinadas a informações obtidas de outros serviços da Microsoft e de outras empresas.

O Quadro 7 mostra a análise da Política de Privacidade do Twitter de acordo com os *Fair Information Principles*.

Quadro 7 – Resumo da análise da Política de Privacidade do Hotmail

Princípio	Análise quanto ao princípio	Motivo
Transparência	Atende parcialmente	A forma como as empresas parceiras manipulam os dados dos usuários não é informada
Qualidade	Não atende	Não pode garantir que as informações sejam fiéis à realidade ao compartilhá-las com outras empresas
Finalidade	Não atende	Por compartilhar as informações com empresas terceiras
Livre acesso	Atende parcialmente	O usuário não tem acesso às informações que estão em posse das empresas parcerias
Segurança física e lógica	Não atende	Não pode garantir o cumprimento deste princípio, uma vez que as informações são compartilhadas com outras empresas

Fonte: Dados da pesquisa (2015)

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Hotmail atende parcialmente dois princípios e não atende aos outros três.

Identificação de potenciais ameaças à privacidade

A análise das Políticas de Privacidade realizada identifica a forma como as empresas provedoras dos serviços de rede social e e-mail gratuito coletam, armazenam e manipulam as informações dos usuários, e mostra também que nenhuma destas empresas atende totalmente aos Princípios de Proteção de Dados Pessoais que compõem o *Fair Information Principles*. Com isso conclui-se que a privacidade dos usuários destes serviços está exposta às seguintes ameaças primárias:

Coleta de informações sem conhecimento dos usuários: todos os provedores dos serviços de redes sociais e e-mail gratuito utilizam *cookies* para coleta de dados. Estes *cookies* coletam informações além das necessárias para utilização destes serviços. A partir destas informações é possível conhecer as preferências dos usuários, as quais podem ser utilizadas, por exemplo, para direcionar publicidade, ou mesmo para espionagem de hábitos do usuário do serviço;

Uso indevido de informações: as informações divulgadas podem ser utilizadas para ataques de força bruta, que consiste em utilizar um algoritmo para analisar as informações com o objetivo, por exemplo, de descobrir as senhas, criação de perfil falso de usuário, golpes de engenharia social e responder questões de segurança para recuperação de senhas (por exemplo, a verificação do nome de filhos ou animais de estimação podem ser utilizadas para responder perguntas comumente feitas para recuperação de senhas quando se clica no 'esqueci minha senha'.

Quando as ameaças listadas acima ocorrem trazem como consequência mais algumas ameaças (ameaças secundárias), quais sejam:

Ataques de engenharia social: através das informações que podem ser obtidas nas redes sociais é possível criar perfis de usuários, com características que podem ser exploradas em ataques de Engenharia Social, que normalmente são realizadas enviando e-mails com mensagens que despertem o interesse dos usuários, fazendo com que executem arquivos anexos que podem ter como objetivo coletar contas e senhas de banco;

Invasão de privacidade: é impossível controlar as informações que os usuários repassam sobre seus contatos. Quando maior a rede de contatos dos usuários, maior o número de pessoas que terão acesso às informações publicadas;

Disponibilização de informações para criminosos: através das informações disponíveis nas redes sociais é possível conhecer os hábitos do usuário, locais que costuma frequentar, tais como restaurantes, bares e casas noturnas. Estas informações podem ser usadas para roubo de bens e tentativas de sequestro;

Perda de controle sobre as informações: todas as empresas provedoras dos serviços objetos deste estudo compartilham as informações de seus usuários com empresas terceiras. Os usuários não têm acesso às informações armazenadas pelas empresas parceiras, não sendo possível removê-las ou controlar o uso futuro destas informações;

Furto de identidade: através da grande quantidade de informações que podem ser obtidas nas redes sociais pode-se criar um perfil falso para que alguém se passe por outra pessoa, o que muitas vezes tem por objetivo obter informações sobre os amigos deste usuário ou publicar informações que possam denegrir a imagem do usuário, ou mesmo se passar por este usuário na utilização de um serviço.

O Quadro 8 traz um resumo das análises realizadas nas políticas de privacidade, indicando o nível de atendimento de cada princípio, onde pode-se perceber que nenhum dos princípios é atendido na totalidade pelos serviços de redes sociais e e-mail gratuitos. Nenhum dos serviços analisados atende parcialmente a todos os princípios, sendo o Twitter o serviço que mais 'atende parcialmente' e o Linkedin o serviço com mais frequência para 'não atende'.

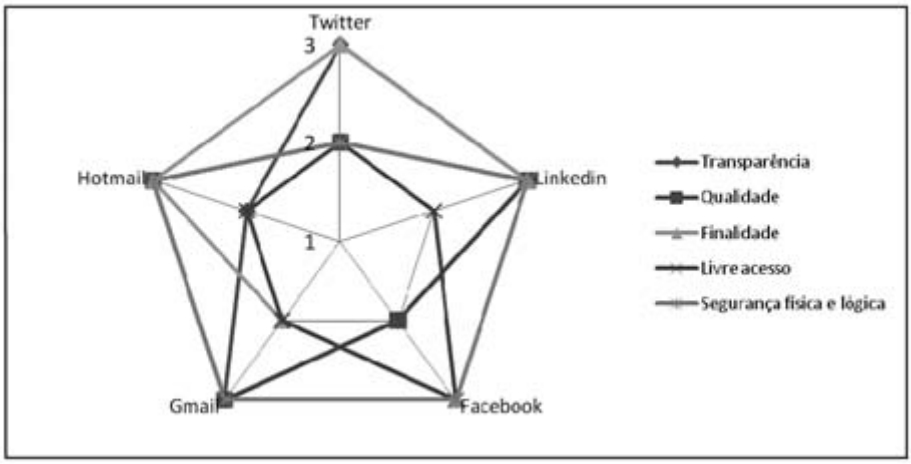
Quadro 8 – Resumo das análises realizadas

Princípios	Serviços				
	Twitter	Linkedin	Facebook	Gmail	Hotmail
Transparência	Não atende	Não atende	Atende parcialmente	Não atende	Atende parcialmente
Qualidade	Atende parcialmente	Não atende	Atende parcialmente	Não atende	Não atende
Finalidade	Não atende	Não atende	Não atende	Atende parcialmente	Não atende
Livre acesso	Atende parcialmente	Atende parcialmente	Não atende	Atende parcialmente	Atende parcialmente
Segurança física e lógica	Atende parcialmente	Não atende	Não atende	Não atende	Não atende

Fonte: Dados da pesquisa (2015)

Atribuindo-se valores aos resultados obtidos e considerando que o atendimento aos *Fair Information Principles* representa um risco menor, é possível identificar o nível de risco à privacidade causado pelas empresas provedoras dos serviços de redes sociais e e-mails gratuitos em cada princípio (Figura 1).

Figura 1 – Nível de risco à privacidade



Legenda: 1 – Atende (risco baixo), 2 – Atende Parcialmente (risco médio), 3 – Não Atende (risco alto)

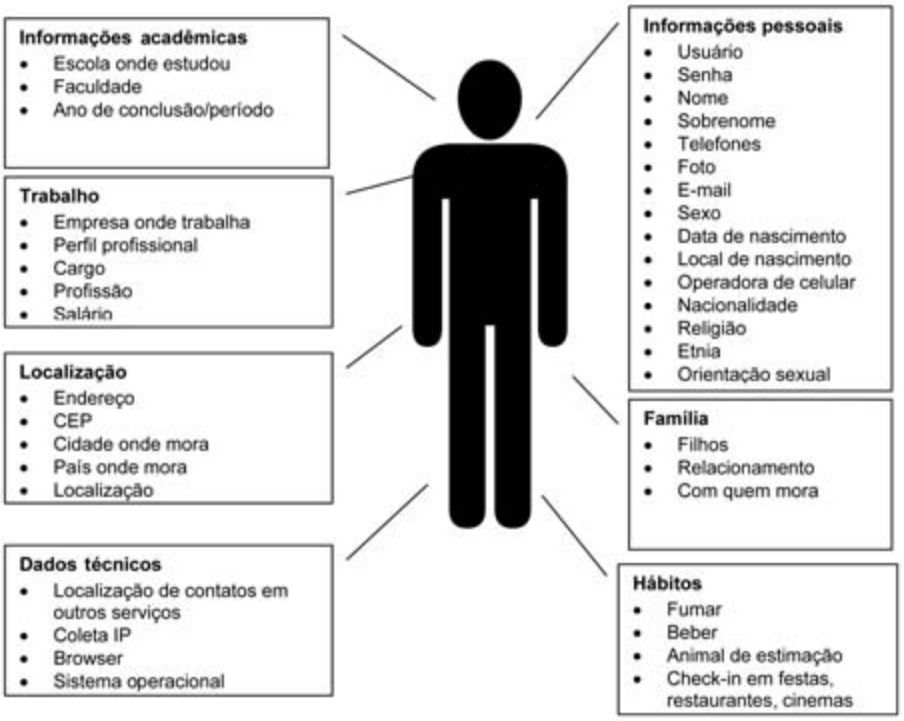
Fonte: Dados da pesquisa (2015)

A Figura 1 nos mostra que o risco à privacidade dos usuários dos serviços objetos deste estudo varia de Médio a Alto Risco, sendo que a maior ocorrência é de Alto Risco, e em especial afetando os princípios de finalidade e o de segurança física e lógica, ou seja, os riscos mais significativos são de que os dados não sejam utilizados apenas para a finalidade primária sem a autorização do usuário e de que os dados não sejam adequadamente protegidos contra extravio, destruição, modificação, transmissão ou acesso não autorizado. Representam, portanto, riscos bastante significativos à privacidade dos usuários.

Os riscos mostrados nos Quadros 2 a 8 e na Figura 1 aumentam significativamente na medida em que mais informações são coletadas dos

usuários. A Figura 2 mostra que é expressiva a quantidade e diversidade de informações sobre os usuários dos serviços de redes sociais e e-mails gratuitos que estão disponíveis nas bases de dados dos provedores destes serviços, e que estão expostas a este Alto Risco.

Figura 2 – O que se pode saber sobre os usuários



Fonte: Dados da pesquisa (2015)

A partir das análises realizadas é possível concluir que a privacidade dos usuários de redes sociais e e-mails gratuitos não pode ser garantida pelas empresas provedores destes serviços, fazendo com que a privacidade destes usuários esteja exposta a diversas e significativas ameaças. Conforme descrito nas políticas de privacidade analisadas, os provedores destes serviços compartilham com empresas parceiras as informações dos usuários, seja para que estas empresas prestem serviços para os provedores, seja como parte de alguma negociação comercial. Uma vez que as informações são compartilhadas, não é possível garantir que estas

não venham a ser utilizadas para fins indevidos. Da mesma forma não é possível garantir que, caso o usuário exclua seu perfil ou sua conta, suas informações sejam totalmente eliminadas. Tanto os provedores dos serviços quanto seus parceiros mantêm cópias de segurança das informações armazenadas em seus bancos de dados, e fica difícil garantir que estas cópias não serão utilizadas mesmo após a exclusão do perfil ou conta.

Os provedores não informam especificamente como as empresas parceiras tratam, armazenam ou utilizam as informações dos usuários, sendo estas ações realizadas sem o conhecimento do titular dos dados, o que caracteriza uma potencial ameaça à privacidade dos usuários dos serviços de redes sociais e de e-mails gratuitos. O usuário destes serviços tem acesso somente às informações que estão em seus perfis e suas contas, mas não tem acesso às informações que foram repassadas às empresas parceiras dos provedores, não sendo possível acessá-las, perdendo-se assim o controle sobre estas informações. Esta prática fere o princípio de livre acesso, uma vez que o usuário não tem livre acesso ao total das suas informações.

O princípio da qualidade não é atendido, uma vez que as informações são compartilhadas com empresas terceiras, o que faz com que os provedores não tenham como garantir que estas informações permaneçam fiéis à realidade, completas e relevantes. A própria política de privacidade de uma das redes sociais, o Twitter, informa que a informações poderão ser adaptadas ou alteradas.

Pode-se concluir que o princípio da finalidade, o qual restringe a transferência de dados para terceiros, não é cumprido pelos provedores dos serviços de rede social e e-mails gratuitos, uma vez que compartilham as informações de usuários com empresas parceiras com as quais terceirizam parte de seus serviços.

Considerando a grande quantidade de informações coletadas (Figura 2), a baixa aderência aos *Fair Information Principles* (Quadro 8) e o risco associado a esta baixa aderência (Figura 1), pode-se perceber a dificuldade de garantir a privacidade das informações pessoais dos usuários dos serviços de redes sociais e de e-mails gratuitos. A grande quantidade de informações fornecidas por si só já expõe a privacidade dos usuários a um grande risco, e o fato das empresas compartilharem as informações de seus usuários com empresas terceirizadas potencializa estes riscos.

No entanto, os tempos atuais (e possivelmente os futuros) são de uso intensivo de dispositivos tecnológicos, que muito embora possam trazer riscos para a privacidade também trazem informação, diversão e contato com colegas e familiares. O caminho para manter a privacidade não é deixar de utilizar os recursos disponíveis, mas se informar sobre o assunto, ler a política de privacidade e a partir do conhecimento dos riscos decidir de maneira consciente se quer ficar exposto a eles. Westin, a partir dos seus estudos, trouxe a noção de privacidade como direito, mas também a responsabilidade de cada indivíduo. Desta forma, a privacidade é mantida com o comportamento responsável a respeito de que tipo de informação deve ser divulgada e em que veículo. Ao mesmo tempo em que se mantém a atenção às mudanças nas políticas de privacidade e se cobra das organizações para que estas sejam honestas em relação a como usam as informações fornecidas e que o uso preserve o cuidado e respeito pertinente a uma informação de um indivíduo, é necessário verificar se a cada postagem ou acesso não estamos nos expondo em demasia em troca de benefícios efêmeros.

Referências

ACQUISTI, A.; GROSSKLAGS, J. Privacy and rationality in individual decision making. **Security & Privacy,** v. 3, n. 1, p. 26-33, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 17799: Tecnologia da informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação.** Rio de Janeiro, 2005.

BANKS, A. **2012 BRAZIL DIGITAL FUTURE IN FOCUS**. Disponível em: <http://www.comscore.com/por/Press_Events/Press_Releases/2012/3/Brazil_s_Social_Networking_Activity_Accelerates_in_the_Past_Year>. Acesso em: 14 de maio de 2012.

BRASIL. Ministério da Justiça do Brasil. Secretaria de Direito Econômico. Departamento de Defesa e Proteção do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da Informação creditícia. Brasília, D.F.: ENDC, 2010. 121 p. (Caderno de Investigações Científicas, 2)

COMSCORE. Brazil Digital Future in Focus. Disponível em: <http://www.comscore.com/por/Press_Events/Press_Releases/2012/3/Brazil_s_Social_Networking_Activity_Accelerates_in_the_Past_Year>. 2012. Acesso em: 14 maio 2012.

HUI, K., et al. The value of privacy assurance: An exploratory field experiment. **MIS Quarterly**, v.31, n.1, p. 19-33, 2007.

KLEIN, R.H. **Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à segurança da informação**. 2014. Dissertação (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre, 2014. Disponível em: <http://repositorio.pucrs.br:8080/dspace/handle/10923/5771>. Acesso em: 3 fev. 2015.

LUCIANO, E.M.; MAHMOOD, M.A.; MAÇADA, A.C. The influence of human factors on vulnerability to information security breaches. In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS, 16., Lima-Peru, 2010.

LUCIANO, E.M.; KLEIN, R.H. Gestão da segurança da Informação. In: PRADO, E.P.V.; SOUZA, C. A. (Org.). **Fundamentos de Sistemas de Informação.** São Paulo: Elsevier, 2014. p. 125-150.

O'BRIEN, J.A. **Sistemas de Informação:** e as decisões gerenciais na era da internet. 2. ed. São Paulo : Saraiva, 2004.

PORTAL UOL. Facebook tem 1,23 bilhão de usuários mundiais; 61,2 milhões são do Brasil. 2014. Disponível em: <http://tecnologia.uol.com.br/noticias/afp/2014/02/03/facebook-em-numeros.htm>. Acesso em: 01 de fevereiro de 2015.

RAMALHO, J.A. **Mídias sociais na prática**. São Paulo: Elsevier, c2010.

RECUERO, R. C. Redes sociais na internet. Porto Alegre: Sulina, 2009.

REINALDO FILHO, D.R. **Direito da Informática:** temas polêmicos. São Paulo: Edipro, 2002.

REZENDE, D.A.; ABREU, A.F. **Tecnologia da informação aplicada a sistemas de informação empresariais:** o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2011.

ROSE, E. A. An examination of the concern for information privacy in the New Zealand regulatory context. **Information & Management**, v. 43, n. 3, p. 322-335, 2006.

SCHWAIG, K.S.; KANE, G.C.; STOREY, V.C. Compliance to the Fair Information Practices: how are the fortune 500 handling online privacy disclosures? **Information & Management**, v.43, n. 7, p. 805-820, 2006.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, c2003.

SHIN, D. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. **Interacting with Computers**, v. 22, n. 5, p. 428-438, 2010.

SILVA, J.A. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2011.

TEJERA, M.H.D. A esfera privada na pós-modernidade: uma análise a partir de práticas na internet. 2006. 130 p. Dissertação (Mestrado em Comunicação Social) – PPGCOM/PUCRS. Porto Alegre, 2006.

Twitter atinge meio bilhão de contas. Mais de 140 milhões de pessoas nos EUA. Disponível em: <http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US>. Acesso em: 9 out 2012.

Twitter busca conquistar a preferência de empresas e usuários. Disponível em: <http://mundodomarketing.com.br/reportagens/22438/twitter-busca-conquistar-a-preferencia-de-empresas-e-usuarios.html>. Acesso em: 3 maio 2012.

WESTIN, A.D**. Privacy and Freedon**. New York: Athenum, 1967.

II

Proteção à privacidade das informações em saúde e direitos

5

O direito fundamental à privacidade e as informações em saúde: alguns desafios

Ingo Wolfgang Sarlet[1]
Tania Margarete Mezzomo Keinert[2]

Introdução

A sociedade atual, marcada pela grande evolução das tecnologias de informação e comunicação, coloca a privacidade como uma complexa e importante questão, tanto para os operadores do direito quanto para os gestores e, especialmente, para os cidadãos. O presente estudo, utilizando-se de pesquisa bibliográfica e documental, tem como objetivo discutir os desafios colocados à proteção da privacidade como direito fundamental, especialmente no que se refere às informações em saúde, já que em geral classificáveis como "dados sensíveis" e particularmente carentes de garantias efetivas, com destaque para o marco jurídico-constitucional brasileiro. Para tanto, inicia-se com uma breve contextualização do problema, situando-o na esfera da assim chamada "sociedade da informação", que, ademais, também é, em certo sentido, uma "sociedade do risco" (noção que não se aplica apenas ao domínio infor-

1 Ingo Wolfgang Sarlet (iwsarlet@gmail.com) é Doutor em Direito pela *Ludwig Maximillians Universität München* (1997), Professor Titular da Faculdade de Direito e coordenador do Programa de Pós-Graduação em Direito - Mestrado e Doutorado – da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e Juiz de Direito de Entrância Final (RS).

2 Tania Margarete Mezzomo Keinert (taniak@isaude.sp.gov.br) é administradora pública e bacharel em Direito, Mestre e Doutora em Administração Pública pela FGV/SP com pós-doutorado em Gestão de Qualidade de Vida na Universidade do Texas/Austin (EUA) e Pesquisadora Científica IV do Instituto de Saúde.

macional), onde a informação adquire um caráter e valor de mercadoria. Na sequência, a privacidade vai apresentada na sua condição de direito humano e fundamental com forte conexão com a dignidade da pessoa humana, seguindo-se com a delimitação do conteúdo, das funções e dos limites do direito à privacidade (ou vida privada). Por derradeiro, a privacidade é examinada no campo das informações na esfera da saúde, destacando-se o potencial discriminatório da violação da privacidade nessa seara, bem como o problema do impacto das mudanças tecnológicas nesse contexto, sem deixar de examinar a tensão que se estabelece entre a dimensão pública da saúde e a sua dimensão privada, tudo a embutir uma dose significativa de complexidade numa questão que vem se tornando cada vez mais crucial para o desenvolvimento da própria medicina, bem como para a formulação e implementação das políticas públicas de saúde.

Breve contextualização

Vivemos na assim chamada Sociedade da Informação, caracterizada essencialmente pela aceleração dos processos de produção e disseminação da informação e do conhecimento a velocidades e quantidades antes inimagináveis. As transmissões de dados são de baixo custo e as tecnologias de armazenamento são amplamente utilizadas, muitas vezes em centrais virtuais de dados, o que pode fragilizar sua segurança e implicar violação da privacidade (GERMAN, 2000; MARQUES, e MARTINS, 2000; WERTHEIN, 2000).

A expressão sociedade da informação define uma nova forma de organização social, política e econômica em que ocorre intensivo uso de tecnologias para coleta, produção, processamento, transmissão e armazenamento de informações. A informação, por si só, surge como a principal matéria-prima desse novo modelo econômico. No cenário da sociedade da informação, cresce o interesse tanto dos governos quanto da iniciativa privada em relação ao acesso a informações pessoais, com reflexos evidentes na privacidade. Por exemplo, o mercado impõe como um dos critérios para avaliação do valor de venda de corporações

a quantidade de informações pessoais de que essas entidades dispõem sobre seus clientes, o Estado, por sua vez, investe em poderosos bancos de dados para interconexão e processamento de informações pessoais, a fim de traçar o perfil dos cidadãos. Assim, o comportamento das pessoas torna-se cada vez mais controlado por meio de câmeras e de outros meios de vigilância instaladas e disseminados por toda parte: as empresas incrementam procedimentos de monitoramento das comunicações dos empregados, surgem companhias especializadas na coleta e no processamento de dados pessoais para fins de marketing e de publicidade, as agências de inteligência governamentais firmam acordos, a fim de interceptar comunicações ao redor de todo o mundo, de tal sorte que essa mesma sociedade de informação cada vez mais assume também a condição de uma sociedade de vigilância, mediante o recurso a artefatos tecnológicos novos e cada vez mais sofisticados (VIEIRA, 2007; RODOTÁ, 2008)

A sociedade de informação, ademais, caracteriza-se por constantes mudanças quanto aos meios de comunicação, especialmente no que diz com a redução das distâncias e a minimização do tempo da comunicação, que chega ser praticamente a do tempo real, tudo isso a propiciar e exigir também uma mudança cultural, no âmbito do que se convencionou designar de uma "cultura internet" (CASTELLS, 2003). O autor ressalta que a tecnologia da informação poderia ser utilizada para o fortalecimento das democracias, ampliando a participação dos cidadãos na gestão dos recursos públicos. Ao invés, salienta que os governos utilizam a internet para vigiar as pessoas, sendo que as pessoas é que deveriam utilizar a rede para vigiar os governos – o que, de fato, representa um direito desses indivíduos, já que, nas democracias, teoricamente, o povo é o soberano. Os governos deveriam disponibilizar na *web* um amplo espectro de informações não sigilosas de interesse da coletividade, abrir canais para solicitação de serviços públicos e possibilitar a fácil comunicação entre a população e seus representantes. Entretanto, a maioria dos estudos e relatórios descreve um quadro melancólico e, com a possível exceção de alguns países escandinavos, ainda prevalece a aplicação dos recursos tecnológicos para vigilância e controle dos indivíduos, enquanto mecanismo de poder do Estado e

não como um instrumento de fortalecimento da democracia participativa (CASTELLS, 2003).

O conceito de paradigma tecnológico cunhado pelo mesmo Castells ajuda a compreender a essência da transformação tecnológica atual. Os aspectos centrais desse paradigma, no conjunto, formam a base material da sociedade da informação: 1) a informação é a matéria-prima do novo paradigma; 2) como a informação é parte fundamental da atividade humana, os novos meios tecnológicos moldam diretamente a esfera da existência individual e coletiva; 3) a lógica das redes envolve qualquer tipo de relações usando as novas tecnologias de informação; 4) as tecnologias específicas tendem a convergir para um sistema altamente integrado. Dessa forma, as novas tecnologias da "sociedade em rede" passam a interferir diretamente na vida cotidiana e privada das pessoas.

Percebe-se menor preocupação com as questões de espaço e o tempo, uma vez que surge uma nova dinâmica de vida e de relações, a qual exigirá cada vez menos que as pessoas estejam num determinado lugar em determinada hora, pois as interações podem ser feitas virtualmente. (NEGROPONTE, 1995, p. 159). Assim, o "ciberespaço" é o mais novo local de "disponibilização" de informações possibilitado pelas novas tecnologias. A perspectiva da digitalização geral das informações provavelmente já está transformando o ciberespaço no principal canal de comunicação e suporte de memória da humanidade nesse limiar do Século XXI (LÉVY, 2000, p. 92-93).[3]

Mas a Sociedade de Informação é também uma Sociedade do Risco – e o risco assume nesse contexto algumas peculiaridades, uma vez que o avanço tecnológico também torna vulneráveis os mecanismos de proteção e de controle dos riscos sociais, políticos, econômicos e industriais. Beck explicita que, nesse novo contexto, a noção de risco toma um significado bastante específico, baseando-se em interpretações causais dos acontecimentos com impacto maior em projeções para o futuro do que

3 Para esse autor, o termo especifica não apenas a infraestrutura material da comunicação digital, mas também todo o universo de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo. Ver, por exemplo, MONTEIRO, S. D. O Ciberespaço: o termo, a definição e o conceito. **Data Grama Zero - Revista de Ciência da Informação**, Rio de Janeiro, v.8 n.3, jun.2007.

no presente. Daí a importância das informações como possíveis causadores de perigo social, de um lado, ou de mecanismos de reconhecimento e proteção destes riscos, de outro.[4]

Nesse sentido, a sociedade da informação chancela-se com as marcas vigorosas do progresso, pelo fortalecimento das ciências, especialmente da tecnologia da informação, pela substituição da informação ao capital e ao trabalho, como recurso estratégico da economia, assim como pela expansão dos riscos de base tecnológica. Nessas perspectivas, impõem-se, destarte, como uma sociedade cujos valores imateriais, dados, informações, conhecimento científico e tecnológico, constituem a força motriz da formação e do desenvolvimento sociais, de tal sorte que se verifica, inclusive, uma expansão do próprio conceito de "informação" que abrange a imagem, a voz e todo e qualquer dado em formato eletrônico (GONÇALVES, 2003).

Consoante já adiantado, esse cenário gera expectativas, tanto positivas quanto negativas, conforme alguns estudos indicam. Com efeito, a nova forma de organização social, denominada de *sociedade da informação,* configura-se como uma oportunidade histórica de realização dos direitos de cidadania, especialmente das liberdades de informação e expressão em geral. As possibilidades técnicas de informação e de comunicação permitem aos cidadãos desfrutar, com plenitude, direitos e liberdades, na medida em que esses indivíduos dispõem de mais e de melhores meios de expressão, criação e interação, o que, por sua vez, pode ampliar os níveis de participação democrática. Tome-se, apenas como exemplo, as redes sociais virtuais, as quais propiciam o desenvolvimento de ações coletivas e se constituem como importantes espaços que permitem ampliar as potencialidades de articulação social dos indivíduos. (RHEINGOLD, 1996; CASTELLS, 2003; BOYD e ELLISON, 2007; AGUIAR, 2007; RODOTÀ, 2008; SANTOS JÚNIOR E MANTOVANI, 2010).

Outros autores, porém, ponderam que a sociedade da informação agrava o risco de se ampliarem as desigualdades sociais, em virtude

4 Do original de BECK, U. **Risikogesellschaft. Auf dem Weg in eine andere Moderne**. Frankfurt: Suhrkamp, 1986.[Trad. port.: *Sociedade de Risco*: rumo a uma outra modernidade. São Paulo: Editora 34, 2011].

das agudas diferenças que se verificam no que diz com as condições de acesso, ou não, à informação, aumentando o fosso entre as classes sociais mais pobres e os economicamente favorecidos, além de representar um perigo de reforço da vigilância por parte dos *aparelhos de Estado*[5] sobre os indivíduos. (VIEIRA, 2007; GONÇALVES, 2003; CASTELLS, 2003; RODOTÀ, 2008; DONEDA, 2006).

Há que considerar, não obstante, o fato de que, na sociedade atual, desenvolveu-se um robusto sistema de proteção aos Direitos Humanos, especialmente a partir das atrocidades cometidas durante a Segunda Guerra Mundial. Nesse sentido, há consenso em torno da ideia de ser a privacidade um princípio fundamental da moderna legislação sobre os Direitos Humanos, dado que é protegida em nível internacional por meio de pelo menos três instrumentos essenciais – também para o caso brasileiro, designadamente, a Declaração Universal dos Direitos Humanos (DUDH), o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP) e a Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica), sem prejuízo de outros documentos, da Convenção Europeia dos Direitos do Homem, e, por último, tendo em conta sua relevância, da Carta Europeia de Direitos Fundamentais.

Apenas para ilustrar, o artigo 12 da Declaração Universal dos Direitos Humanos, adotada pela Assembleia Geral das Nações Unidas (1948), estabelece que o direito à vida privada é um direito humano, prescrevendo que "ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques", formulação que praticamente foi incorporada ao artigo 17 do Pacto Internacional dos Direitos Civis e Políticos, adotado pela Assembleia Geral das Nações Unidas, em 1966[6]. A Convenção Americana, por sua vez, no seu artigo 11, inclui o respeito e

5 Assume-se aqui – com as ressalvas em relação a uma leitura dominantemente marxista – a noção de *aparelhos de Estado,* em sentido similar a da noção *de aparelhos ideológicos de Estado*, a superestrutura de poder integrada por instituições distintas e especializadas, como a igreja, a escola, a família, a imprensa e o Estado, propriamente dito, tal como formulada por ALTHUSSER, Louis. Aparelhos ideológicos de Estado: nota sobre os aparelhos ideológicos de Estado. Rio de Janeiro: Edições Graal, 1985, p. 68. *Apud* VIEIRA, 2007.

6 Artigo 17: 1) "Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais a sua honra e reputação. 2) Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques." *Disponível em: http://www.dhnet.org.br/direitos/sip/onu/doc/pacto2.htm*

proteção à vida privada no contexto da proteção da honra e da dignidade, explicitando, ademais, o liame entre esta última e o direito à privacidade. No plano constitucional, a privacidade também já se faz presente na expressiva maioria das constituições, ostentanto a condição de direito fundamental, inclusive e especialmente na vigente Constituição da República Federativa do Brasil de 1988 (doravante apenas CF), que, em seu artigo 5º, inciso X, dispõe, que"são invioláveis a intimidade, à vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

Todavia, a despeito do reconhecimento e proteção jurídica no plano internacional e nacional, assumindo a dupla condição de direito humano e direito fundamental, os desenvolvimentos precedentes já são suficientes para afirmar que no contexto atual da sociedade da informação, a privacidade tem sido colocada à prova quanto ao seu real significado. Também tem sido cada vez mais problematizado até que ponto o seu reconhecimento como direito humano e fundamental tem tido o condão de assegurar uma proteção minimamente efetiva do referido bem jurídico. Se migrarmos então para o domínio do direito à saúde, onde informação precisa e atual assume caráter, em muitos casos, radicalmente vital ao mesmo tempo que a privacidade segue tendo uma expectativa legítima de respeito e proteção, ver-se-á que o problema é altamente complexo e relevante para a própria preservação e promoção da dignidade da pessoa humana. Por outro lado, ainda que a dignidade seja também um direito humano, do ponto de vista do direito internacional, aqui será priorizada a dimensão constitucional, ou seja, da privacidade na condição de direito fundamental da pessoa humana, sem que com isso se esteja a desconsiderar ou mesmo menosprezar os influxos do sistema internacional.

A privacidade na condição de direito fundamental na ordem constitucional brasileira

Dos direitos fundamentais que dizem respeito à proteção da dignidade e personalidade humanas, o direito à privacidade (ou vida privada) é um dos mais relevantes, embora nem sempre tenha sido contemplado

nas constituições, ao menos, não expressamente.[7] É o caso, por exemplo, do direito constitucional norte-americano, onde, a despeito de inexistir referência expressa ao termo privacidade no texto da Constituição e das subsequentes emendas contendo os diversos direitos e garantias fundamentais, o direito à privacidade, na acepção cunhada pelo então Juiz da Suprema Corte, Louis Brandeis, seria o mais abrangente e valioso de todos os direitos para o homem civilizado.[8]

No caso da evolução constitucional brasileira, foi apenas na CF, já citada, que a proteção da vida privada e da intimidade foi objeto de reconhecimento de modo expresso.

Por outro lado, o direito à vida privada articula-se com outros direitos fundamentais, como é o caso da proteção da intimidade (vida íntima) e também da inviolabilidade do domicílio, que é o espaço onde se desenvolve a vida privada, mas também dialoga com a proteção da vida familiar, sendo nesse contexto reconhecido em documentos internacionais e constitucionais. Também tais direitos, em especial a intimidade, nem sempre são expressamente positivados nos textos constitucionais e internacionais, pois em geral a intimidade constitui uma dimensão (esfera) da privacidade. Na CF, todavia, embora ambas as dimensões (privacidade e intimidade) tenham sido expressamente referidas, haverão de ser analisadas em conjunto, pois se cuida de esferas (níveis) do direito à vida privada.

Por outro lado, muito embora também exista uma forte conexão com os direitos à honra e à imagem, esses dizem mais de perto com a identidade e integridade moral da pessoa humana, razão pela qual aqui não serão versados, ainda que no campo da responsabilidade civil seja possível uma conexão com o ambiente da saúde. De alta relevância é a relação da privacidade com a proteção de dados pessoais, o que também será objeto de consideração. De qualquer sorte, os pontos de contato en-

7 Sobre a evolução do reconhecimento de um direito à privacidade, v., entre outros, na literatura brasileira, a síntese de Teixeira, Eduardo Didonet; Haeberlin, Martin. *A proteção da privacidade – Aplicação na quebra do sigilo bancário e fiscal*, p. 37 e ss.; Doneda, Danilo. *Da privacidade à proteção de dados pessoais*, p. 7 e ss.

8 Cf. o texto original em inglês, extraído da decisão da Suprema Corte no caso *Olmstead v. United States* (1929), "the most comprehensive of rights and the right most valued by civilized men", citado por Solove, Daniel. *Understanding Privacy*, p. 1. No âmbito da literatura brasileira, v. a síntese oferecida por Cachapuz, Maria Cláudia. *Intimidade e vida privada no novo Código Civil brasileiro – Uma leitura orientada no discurso jurídico*, p. 80-98, analisando a evolução da noção de privacidade no direito anglo-saxão.

tre o direito à privacidade e os demais direitos ora referidos não afastam importantes conexões entre a privacidade e outros direitos fundamentais, mas que aqui não poderão ser exploradas.[9] Por outro lado, necessária a definição do conteúdo (ou âmbito de proteção) do direito à vida privada, pois é a partir da determinação do conteúdo que se poderá examinar, na sequência, como a privacidade comporta, ou não, restrições com fundamento em direitos (princípios) conflitantes, apenas para citar uma situação corriqueira e que também se verifica quando em causa informações (dados) em matéria de saúde.

Como já referido, diversamente de outras ordens constitucionais, a CF não reconheceu apenas um genérico direito à privacidade (ou vida privada), mas optou – pelo menos do ponto de vista textual – por referir tanto a proteção da privacidade, quanto da intimidade, como bens autônomos, tal como no caso da honra e da imagem. Todavia, o fato de a esfera da vida íntima (intimidade) ser mais restrita que a da privacidade, cuidando-se de dimensões que não podem pura e simplesmente ser dissociadas, recomenda um tratamento conjunto de ambas as situações.

Por outro lado, é preciso reconhecer que, dadas as peculiaridades da ordem constitucional brasileira, especialmente à vista do reconhecimento de outros direitos pessoais no plano constitucional e da cláusula geral representada pela dignidade da pessoa humana, o direito à privacidade – a exemplo do que ocorre também em Portugal – não merece a abrangência que lhe foi dado no direito constitucional norte-americano, onde assumiu a função equivalente a um direito geral de personalidade.[10]

Com isso, todavia, não se lhe está a negar relevância, notadamente pelos já referidos pontos de contato com outros direitos fundamentais, mas em especial com a dignidade da pessoa humana, pois é líquido que a preservação de uma esfera da vida privada é essencial à própria saúde mental do ser humano e lhe assegura as condições para o livre desenvolvimento de sua personalidade.[11]

9 Assim, por exemplo, a proteção da vida privada coincide com diversos elementos de outros direitos fundamentais, como é o caso dos direitos à segurança, à liberdade de imprensa, à liberdade de expressão do pensamento. Nesse sentido, v., também, Rivero Jean; Moutouh, Hughes. *Liberdades públicas*, p. 450-451.

10 Cf., por todos, Miranda, Jorge; Medeiros, Rui. *Constituição portuguesa anotada*, p. 290.

11 Cf. Mendes, Gilmar Ferreira; Branco, Paulo Gustavo Gonet. *Curso de direito constitucional*, p. 315-316.

Embora exista quem – no direito constitucional brasileiro e em virtude do texto da CF – busque traçar uma distinção entre o direito à privacidade e o direito à intimidade, de tal sorte que o primeiro trataria de reserva sobre comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, incluindo as relações comerciais e profissionais, ao passo que o segundo guardaria relação com a proteção de uma esfera mais íntima da vida do indivíduo, envolvendo suas relações familiares e suas amizades etc.,[12] tal distinção é difícil de sustentar, especialmente em virtude da fluidez entre as diversas esferas da vida privada (incluindo a intimidade), de modo que também aqui adotaremos uma noção abrangente, incluindo a intimidade no âmbito de proteção mais amplo do direito à vida privada (privacidade).[13]

A noção, desenvolvida por setores da doutrina e pela jurisprudência constitucional alemã, de que se podem, no âmbito do direito à privacidade, distinguir três esferas (a assim chamada teoria das esferas), uma esfera íntima (que constitui o núcleo essencial e intangível do direito à intimidade e privacidade), uma esfera privada (que diz com aspectos não sigilosos ou restritos da vida familiar, profissional e comercial do indivíduo, sendo passível de uma ponderação em relação a outros bens jurídicos) e uma esfera social (onde se situam os direitos à imagem e à palavra, mas não mais a intimidade e a privacidade), tem sido criticada como insuficiente para dar conta da diversidade de casos que envolvem a proteção da vida privada,[14] por mais que possa servir de referencial importante – mas não rígido – para a distinção das diversas situações concretas e seu enquadramento no âmbito de proteção do direito.

De qualquer sorte, é preciso levar em conta a dificuldade que se enfrenta quando se busca reduzir a privacidade a um sentido bem definido, pois não raras vezes a privacidade se presta a certa manipulação pelo próprio ordenamento jurídico, sendo até mesmo utilizada para suprir algumas de suas necessidades estruturais, assumindo, por tal razão, sentidos diversos em função das peculiaridades de um determinado ordenamento e dificultando ainda mais a identificação de um sentido comum.[15]

12 Idem, p. 315.
13 Cf., por todos, para o direito brasileiro, Tavares, André Ramos. *Curso de direito constitucional*, p. 676.
14 Cf. bem anotam Miranda, Jorge; Medeiros, Rui. *Constituição portuguesa anotada*, p. 290.
15 Cf. Doneda, Danilo. *Da privacidade à proteção de dados pessoais*, p. 101 e ss.

Assim, a despeito da existência de parâmetros já bastante consolidados e de ser possível visualizar âmbitos mais íntimos e mais abertos da vida privada (tal como sugerido pela teoria das esferas), o fato é que uma violação do direito à privacidade somente poderá ser adequadamente aferida à luz das circunstâncias do caso concreto.[16]

As considerações precedentes apenas reforçam a tese de que não se logrou até o momento definir com precisão em que consiste o direito à privacidade (e intimidade)[17] e que se deve refutar toda e qualquer catalogação prévia e fechada de situações que possam se enquadrar no seu âmbito de proteção. Com isso, contudo, não se afasta, como já referido, a possibilidade de identificar alguns parâmetros e elementos do direito que tem sido objeto de ampla aceitação, seja no direito estrangeiro, seja no âmbito do direito brasileiro, além de reconhecidos ao nível do direito internacional dos direitos humanos.

Assim, não se coloca em causa que o direito à vida privada consiste, a exemplo do que emblematicamente já se disse no direito norte-americano, no direito de se estar só e de se ser deixado só (*the right to be let alone*),[18] no sentido, portanto, de um direito a viver sem ser molestado pelo Estado e por terceiros no que toca aos aspectos da vida pessoal (afetiva, sexual etc.) e familiar.[19] Em causa, portanto, está o controle por parte do indivíduo sobre as informações que em princípio apenas lhe dizem respeito, por se tratar de informações a respeito de sua vida pessoal, de modo que se poderá mesmo dizer que se trata de um direito individual ao anonimato.[20] Dito de outro modo, o direito à privacidade consiste num direito a ser deixado em paz, ou seja, na proteção de uma esfera autônoma da vida privada, na qual o indivíduo pode desenvolver a sua individualidade, inclusive e especialmente no sentido da garantia de um espaço para seu recolhimento e reflexão,

16 Cf., por todos, Horn, Hans-Detlef. Allgemeines Freiheitsrecht, Recht auf Leben u.a. In: Stern, Klaus; Becker, Florian. *Grundrechte Kommentar*, p. 197.

17 Cf. Royo, Javier Pérez. *Curso de derecho constitucional*, p. 303.

18 Cf., entre tantos, lembra Royo, Javier Pérez. *Curso de derecho constitucional*, p. 303, mediante referência ao conhecido artigo publicado por Charles Warren e Louis Brandeis, em 1890, na *Harvard Law Review*.

19 Cf., por exemplo, Rivero Jean; Moutouh, Hughes. *Liberdades públicas*, p. 447-448: "A vida privada é esfera de cada existência em que ninguém pode imiscuir-se sem ser convidado. A liberdade da vida privada é o reconhecimento, em proveito de cada qual, de uma zona de atividade que lhe é própria, e que ele pode vedar a outrem".

20 Cf. Mendes, Gilmar Ferreira; Branco, Paulo Gustavo Gonet. *Curso de direito constitucional*, p. 517.

sem que ele seja compelido a determinados comportamentos socialmente esperados.[21]

À vista do exposto, é possível acompanhar a lição de J. J. Canotilho e Vital Moreira, quando sustentam, em passagem aqui transcrita, que "o direito à reserva da intimidade da vida privada e familiar analisa-se principalmente em dois direitos menores: (a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. Alguns outros direitos fundamentais funcionam como garantias deste: é o caso do direito à inviolabilidade do domicílio e da correspondência, da proibição de tratamento informático de dados referentes à vida privada. Instrumentos jurídicos privilegiados de garantia deste direito são igualmente o sigilo profissional e o dever de reserva das cartas confidenciais e demais papéis pessoais".[22]

Não sendo fácil, como em geral admitido, distinguir os diversos níveis de proteção do direito à privacidade, em especial o âmbito que diz respeito ao campo mais reservado da intimidade da vida pessoal e familiar (aquilo que em princípio não interessa ao Estado e às demais pessoas), da esfera mais aberta, ou seja, que diz com a inserção social do indivíduo, e desde logo reforçando a tese da insuficiência de qualquer categorização fechada, é possível, contudo, distinguir um âmbito que, ao menos em princípio, é – já pela sua conexão com a dignidade da pessoa humana – absolutamente protegido, insuscetível, portanto, de intervenção estatal, e uma esfera mais aberta, onde a pessoa se encontra entre pessoas e com elas interage, que, por sua vez, é passível de intervenção, desde que mediante estrita observância dos critérios da proporcionalidade e para salvaguardar outros direitos fundamentais ou bens e interesses constitucionalmente assegurados, o que será, mais adiante, objeto de nossa atenção[23].

Por outro lado, sendo possível distinguir dados (informações) que dizem respeito, em primeira linha, a situações pessoais, tais como

21 Horn, Hans-Detlef . Allgemeines Freiheitsrecht, Recht auf Leben u.a. In: Stern, Klaus; Becker, Florian. *Grundrechte Kommentar*, p. 195.
22 Cf. Canotilho, J. J. Gomes; Moreira, Vital. *Constituição da República Portuguesa anotada*, p. 467-468.
23 Cf., por todos, Kloepfer, Michael. *Verfassungsrecht II*, p. 151.

a orientação e as preferências sexuais, anotações em diários, entre outras, de informações em princípio mais triviais, necessário que não se sucumba à tentação de considerar os dados de forma isolada, mas, sim, a partir de uma perspectiva integrada, que perceba os dados pessoais a partir da relação que possa existir entre eles, pois há casos em que dados (informações) aparentemente triviais podem, no âmbito de uma combinação de dados aparentemente aleatórios, implicar uma lesão do direito à privacidade.[24]

Por derradeiro, é de se adotar o entendimento de que o critério (principal) de determinação do âmbito de proteção do direito à privacidade deverá ser material e não formal. Com efeito, ao passo que, numa perspectiva estritamente formal, privado (ou íntimo) seria tudo aquilo que uma pessoa decide excluir do conhecimento alheio, de tal sorte que o âmbito de proteção da privacidade seria variável consoante a particular visão do titular do direito, de um ponto de vista material o direito à privacidade cobre os aspectos da vida pessoal que, de acordo com as pautas sociais vigentes, costuma ser tido como reservado e indisponível ao legítimo interesse do Estado e de terceiros, especialmente tudo que tiver de ficar oculto para assegurar ao indivíduo uma vida com um mínimo de qualidade.[25] Que tal orientação não dispensa uma cuidadosa avaliação das circunstâncias de cada caso convém seja aqui relembrado.

Dada a sua dupla dimensão objetiva e subjetiva, o direito à privacidade opera, na condição de direito subjetivo, em primeira linha como direito de defesa (idem), portanto, como direito à não intervenção por parte do Estado e de terceiros no respectivo âmbito de proteção do direito e, como expressão também da liberdade pessoal, como direito a não ser impedido de levar sua vida privada conforme seu projeto existencial pessoal e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal e que não interferem em direitos de terceiros. Assim, o direito à privacidade é também direito de autodeterminação do indivíduo. Por sua vez, da perspectiva objetiva decorre, além da assim chamada eficácia irradiante e interpretação da legislação civil

24 Cf. Callejón, Maria Luisa Balaguer. Principio de igualdad y derechos individuales. In: Callejón, Francisco Balaguer (coord.). *Manual de derecho constitucional*, 5. ed., vol. 2, p. 135.
25 Cf., para o direito espanhol, Díez-Picazo, Luís María. *Sistema de derechos fundamentales*, p. 289.

(notadamente no campo dos direitos de personalidade), um dever de proteção estatal, no sentido tanto da proteção da privacidade na esfera das relações privadas, ou seja, contra intervenções de terceiros, quanto no que diz com a garantia das condições constitutivas da fruição da vida privada.[26]

Mas também o direito à privacidade, no convívio com outros direitos fundamentais e bens jurídico-constitucionais, como é o caso, *v.g.*, da segurança (de particular relevância na assim chamada sociedade de vigilância), não é ilimitado e imune a restrições.

Todavia, ao não prever, para a privacidade e intimidade, uma expressa reserva legal (que assume a condição de uma expressa autorização constitucional para uma restrição levada a efeito pelo legislador), além de afirmar que se cuida de direito inviolável, há que reconhecer que a CF atribuiu a tal direito um elevado grau de proteção, de tal sorte que uma restrição apenas se justifica quando necessária a assegurar a proteção de outros direitos fundamentais ou bens constitucionais relevantes (no caso, portanto, de uma restrição implicitamente autorizada pela CF), de modo que é em geral na esfera dos conflitos com outros direitos que se pode, em cada caso, avaliar a legitimidade constitucional da restrição.

É precisamente nessa esfera onde, como já frisado, incidem os critérios da proporcionalidade, de acordo com os quais uma intervenção restritiva por parte dos atores estatais (e mesmo de particulares, a depender do caso), deve ser adequada a promoção do resultado almejado, necessária, no sentido de ser utilizado o meio adequado que menos restringe a privacidade para efeito de proteção de outro direito, bem como, caso não resolvida a questão pelos critérios anteriores, deverá ser atentado para o equilíbrio na relação entre meios e fins, preservando-se sempre o núcleo essencial do direito[27].

De qualquer sorte, impende consignar que o quanto a vida privada é, em cada caso, protegida, também guarda relação com o próprio modo de vida individual (pessoas com vida pública, tais como artistas e políticos naturalmente estão mais expostas), de modo que é possível

26 Cf. Kloepfer, Michael. *Verfassungsrecht II*, p. 152.
27 Sobre os critérios da proporcionalidade, ver, por todos, ÁVILA, Humberto. Teoria dos Princípios. São Paulo: Malheiros, 2008.

aceitar, dadas as circunstâncias, uma redução, mas jamais uma anulação dos níveis de proteção individual na esfera da privacidade e intimidade.[28] Como tais questões acabam por se tornar operativas na esfera das informações em matéria de saúde será objeto de análise mais detida na sequencia.

O problema da proteção da privacidade das informações em saúde

A proteção à saúde, por sua vez, também é um direito fundamental garantido constitucionalmente, tanto quando individual, quanto coletivamente considerada, o que reforça o argumento da interdependência e mútua conformação de todos os direitos humanos e fundamentais. Precisamente no caso do direito à saúde e das informações que são geradas e processadas nessa seara o direito à privacidade deve ser especialmente garantido, considerando o caráter sensível e pessoal de muitas das informações; o que resulta evidente, e tem gerado muitos problemas e desafios, notadamente pela complexidade das relações e tensões que se estabelecem entre os diversos atores, direitos e princípios incidentes.

Tomando como ponto de partida a noção de privacidade oriunda do direito norte-americano, no sentido de um direito à reserva de informações pessoais e da própria vida privada (o assim chamado *right to be let alone*), tal como já referido no item anterior, é preciso lembrar, contudo, que alguns autores consideram ser esta definição insuficiente na atualidade, conforme se explicita a seguir.

A privacidade é uma noção extremamente dinâmica e que responde rapidamente às mudanças na esfera tecnológica e que acabam acarretando novos territórios de vulnerabilidade a exigirem uma satisfatória proteção pelo Direito, como, aliás, se verifica no domínio das tecnologias da informação em geral, mas também no caso das tecnologias de reprodução assistida e da engenharia genética, apenas para referir exemplos que dizem respeito à saúde.

28 Cf., por todos, Mendes, Gilmar Ferreira; Branco, Paulo Gustavo Gonet. *Curso de direito constitucional*, p. 319.

Na sociedade contemporânea as definições de privacidade ampliaram-se e "fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim, a privacidade também pode ser definida, numa perspectiva mais atual, como o "direito de manter o controle sobre as próprias informações". (RODOTÀ, 2008, p. 92)

O direito à privacidade, pode ser concebido como uma tríade de direitos – direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido (direito de não ter registros pessoais publicados) – e "transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar um dos fundamentos do Estado democrático de direito" (VIANNA, 2007, p. 116).

O cientista da informação Rainer Kuhlen concebe o conceito de "privacidade" (*Privatheit*) não apenas como proteção de dados ou como o direito de ser deixado em paz, mas também como "autonomia informacional" (*informationelle Selbstbestimmung*), ou seja, a capacidade de escolher e utilizar o conhecimento e a informação autonomamente, em um ambiente eletrônico, e de determinar quais atributos de si serão usados por outros.[29]

Assim, o direito à privacidade constitui-se na "faculdade inerente a cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como na prerrogativa de controlar informações pessoais, evitando-se o acesso e a divulgação de tais dados sem a anuência do referido titular[30]. Assim, de acordo com Vieira (2007), a privacidade poderia ser classificada em cinco categorias, ampliando o leque antes apresentado: a) privacidade física (incolumidade do corpo físico); b) do domicílio (inviolabilidade do domicílio); c) das comunicações (inviolabilidade das comunicações); d) decisional (poder do indivíduo de se auto-

29 Sobre o conceito de "autonomia informacional" da perspectiva da privacidade do cidadão ver KUHLEN, R. **Informationsethik. Umgangmit Wissenund Information in elektronischen Räumen**. *Universitätsverlag Konstanz*, 2004. O conceito de autonomia parece-nos igualmente servir para a análise da sociedade informacional cf. BREY, P. Worker Autonomy and the Drama of Digital Networks in Organizations**.** Canada: **Journal of Business Ethics** vol. 22, 1999, pp. 15-25.

30 A intimidade e a privacidade podem ser distinguidas da seguinte forma: a intimidade corresponde à esfera mais interior do indivíduo, onde se aninham informações mais sensíveis, pensamentos e crenças; enquanto a vida privada corresponde à esfera que custodia fatos da vida particular, os que não revelam aspectos extremamente reservados da personalidade da pessoa, mas que se deseja preservar da divulgação ou do conhecimento por terceiro em geral. VIEIRA, T. M. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris, 2007. p. 305.

determinar); e e) informacional (poder do titular de controlar e proteger seus dados pessoais). [31]

Independentemente da correção (ou precisão) de cada um dos conceitos referidos, o que merece ser fixado é que a privacidade aparece como um conjunto ou um sistema de direitos, onde um dá sustentação ao outro, indissociáveis, portanto. O mesmo ocorre em relação à saúde, conquanto direito fundamental autônomo, apresenta interconexões desde a proteção da saúde, individual e coletivamente considerada, até uma série de outros direitos e interesses tutelados pelo sistema constitucional pátrio protegendo outros bens fundamentais, com os quais apresenta zonas de convergência e mesmo de superposição (direitos e deveres), fato que reforça a tese da interdependência e mútua conformação de todos os direitos humanos e fundamentais.

Assim, verificam-se, na questão da privacidade, quatro tendências que podem ser sintetizadas da seguinte forma: a) do direito a ser deixado só ao direito de manter controle sobre as informações que lhe digam respeito; b) da privacidade ao direito à autodeterminação informativa; c) da privacidade à não discriminação; d) do sigilo ao controle das informações (RODOTÀ, 2008. p. 95-98).

De qualquer sorte, também se percebe, mesmo na atualidade, que o "núcleo duro" da privacidade é ainda constituído por informações que refletem a tradicional necessidade de sigilo (por exemplo, aquelas relacionadas à saúde ou aos hábitos sexuais). Internamente, porém, assumiram cada vez maior relevância outras categorias de informações, protegidas sobretudo para evitar que pela sua circulação possam surgir situações de discriminação, com danos aos interessados. Trata-se, em especial, de informações relacionadas às opiniões políticas e sindicais, além daquelas relativas à raça ou ao credo religioso.

O potencial discriminatório da ausência de privacidade

Uma das preocupações em relação à quebra de privacidade ou ao vazamento total ou parcial de informações sobre a saúde das pessoas é o seu potencial discriminatório. Já em 2005, o Relator Especial sobre o

31 Vieira, T. M. *Op. Cit.*

Direito à Saúde das Nações Unidas ao propor uma "estrutura analítica do direito à saúde", alertava para a necessidade de não discriminação, igualdade e proteção à vulnerabilidade de certos grupos.[32]

Além dos aspectos clássicos da privacidade das informações em saúde sujeitas a sigilo profissional, atualmente se necessita de um maior controle da circulação dessas informações a fim de evitar a incidência de casos de discriminação em relação a doenças (e, por conseguinte, em relação às pessoas com tais doenças) ainda estigmatizadas, como é o caso da Aids, das patologias relacionadas à genética humana, tratamento de dados de idosos, crianças, adolescentes, assim como determinadas doenças mentais, por exemplo, todas conectadas com o fenômeno da privacidade.

No tratamento dessas informações, sua classificação na categoria de dados "**sensíveis**"[33], particularmente protegidos contra os riscos da circulação, se faz imperiosa, especialmente em virtude de seu potencial uso discriminatório. Exatamente para garantir plenitude à esfera pública, determinam-se rigorosas condições de circulação dessas informações, que recebem um estatuto "privado", o qual, por sua vez, se manifesta sobretudo pela proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de circulação.[34]

---

32 Por exemplo, ver Relator Especial sobre o Direito à Saúde das Nações Unidas, Relatório sobre deficiência mental [originalmente, *Report on mental disability*], E/CN.4/2005/51, 10 de fevereiro de 2005.

33 O anteprojeto de lei de proteção de dados pessoais (atualmente sob consulta pública em plataforma digital no site do Ministério da Justiça) classifica, respectivamente, dados pessoais e dados sensíveis, da seguinte forma, em seu artigo 4º: Dados Pessoais: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores (Inciso I); e Dados Sensíveis: dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos e biométricos (Inciso IV). Disponível em: <http://www.acessoainformacao.gov.br/menu-de-apoio/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf> Acesso em: 11.03.2015.

34 Ver, por exemplo, AKOWUAH, F. ; YUAN, X. ; XU, J. ; WANG, H. **A survey of U.S. laws for health information security & privacy**. Arlington – Virginia, USA: International Journal of Information Security and Privacy, out – dez, 2012, vol. 6, p.40. Neste trabalho são discutidas a história e os antecedentes das disposições legislativas, destaques do que as leis exigem e os desafios que as organizações enfrentam no cumprimento das leis. Como as organizações de saúde e seus parceiros de negócios operam em um mundo tecnológico cada vez mais complexo, existem ameaças à segurança e ataques que tornam vulneráveis as informações de saúde individualmente identificáveis. Nos Estados Unidos, existem uma série de leis para que os prestadores de cuidados de saúde tomem medidas práticas para lidar com as necessidades de informação de saúde, segurança e privacidade. Este artigo fornece uma pesquisa de leis norte-americanas relacionadas com a segurança da informação da saúde e da vida privada, que incluem a *Health Insurance Portability e Accountability Act* (HIPAA), a *Gramm-Leach-Bliley, Sarbanes-Oxley Act* de 2002, a *Patient Safety and Quality Improvement* Act de 2005, e a Lei *Health Information Technology for Economic and Clinical Health* (HITECH).

A necessidade de se garantir uma tal "privacidade informática" sugere que o direito de buscar, receber e difundir informações, bem como o direito à autodeterminação informativa, necessita de novos marcos regulatórios, seja ao nível da garantia dos direitos fundamentais, seja dos direitos humanos, especialmente os relacionados aos dados sensíveis, como é o caso da saúde, e, particularmente, se estes forem dados identificados (ou seja, não anonimizados).[35]

Por outro lado, as modernas tecnologias da informação podem fazer com que, inclusive, dados anonimizados sejam facilmente relacionáveis entre si, podendo, a partir de determinado tratamento e busca, tornarem-se identificáveis.[36]

Determinados dados sensíveis específicos, como os relacionados à saúde, merecem proteção especial, não somente por se referirem a fatos íntimos, mas, também, e, às vezes, sobretudo, pelo risco que seu conhecimento possa provocar discriminações. Partindo desta consideração, podem ser corretamente enfrentadas algumas questões surgidas em torno da Aids e dos dados relativos às características genéticas de uma pessoa, por exemplo.

35 Ver, para esta discussão a revisão sistemática efetuada por LOVETT, R. ; FISHER, J. ; AL-YAMAN, F. ; DANCE, P. ; VALLY, H.*A review of Australian health privacy regulation regarding the use and disclosure of identified data to conduct data linkage* .**Australian and New Zealand Journal of Public Health**, 2008, Vol.32(3), pp.282-285. O trabalho objetiva rever a legislação australiana sobre a privacidade, com foco nas regulamentações para conduzir pesquisas de saúde, utilizando dados identificados na região do ACT (*Australian Capital Territory*). Uma revisão sistemática da *Commonwealth*e regulamentos jurídicos de privacidade na saúdefoi realizada. A Austrália tem uma série de normas para a proteção da privacidade das informações de saúde. Além de leis de privacidade baseadas na C*ommonwealth*, existem regulamentos de jurisdição em matéria de proteção de informações de saúde. Estes variam de nenhuma legislação específica, na Austrália Ocidental, a um código de boas práticas na Austrália do Sul, e da legislação *Commonwealth* que lida com o uso e divulgação de informações de saúde identificados para a realização de pesquisas em saúde (artigos 95 e 95A do*Privacy Act*de 1988. O *ACT Health Records (Privacy and Access*) *Act* mostrou-se incompatível com a regulamentação australiana sobre a utilização dos dados de saúde identificados na pesquisa em saúde. As implicações das informações obtidas na revisão sistemática realizada serviu para informar o governo do ACT que seus regulamentos de privacidade em saúde eram inconsistentes com o restante da Austrália e resultaram em sua na alteração. A legislação do ACT foi alterada para incluir disposições relativas à divulgação de informações de saúde identificados para a pesquisa em saúde em circunstâncias controladas.

36 Sobre a "anonimização de dados", há indícios que, atualmente, é quase impossível coletar dados que não deem uma indicação quase precisa de quem é o cidadão/cidadã a quem se referem. As pesquisas apontam que a partir de dois ou três dados e mais algumas buscas na Internet uma pessoa ou dado deixa de ser anônimo. Disponível em: CARDOSO, M. "Privacidade na internet: chega de andarmos todos nus." Carta Capital, ver: http://www.cartacapital.com.br/blogs/intervozes/privacidade-na-internet-chega-de-andarmos-todos-nus-5930.html. Acesso em: 10.03.2015 e também: "ONU pode criar relatoria especial sobre privacidade"; a iniciativa, uma parceria entre Brasil e Alemanha, indica a necessidade de proteção ao indivíduo num contexto de vigilância nas comunicações digitais. Ver: http://www.cartacapital.com.br/tecnologia/onu-pode-criar-relatoria-especial-para-o-direito-a-privacidade-1283.html. Acesso em: 10.03.2015.

Não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado. Explica-se assim a tendência a proibir, exceto em casos especiais, a comunicação das informações citadas a empregadores e companhias seguradoras, reforçando a tutela da privacidade para essa categoria especialíssima de dados sensíveis. [37]

As informações genéticas, crescentemente identificadas e disponibilizadas em sistemas de informação, assumem um valor *constitutivo* da esfera privada bem mais forte do que qualquer outra categoria de informações pessoais. Isso resulta do fato de que elas estão relacionadas à própria estrutura da pessoa e não são modificáveis pela vontade do interessado. Exatamente por seu "caráter *estrutural* e *permanente*, as informações genéticas constituem a parte central do 'núcleo duro' da privacidade das informações em saúde, e, por fornecerem um perfil definido das pessoas, estão, assim, na base de ações discriminatórias". (RODOTÀ, 2008).

As políticas ou programas de saúde coletiva nem sempre são submetidos a uma análise no sentido de verificar se respeitam os direitos humanos e fundamentais, avaliando de modo adequado suas vantagens e desvantagens. Por exemplo, a exigência de testes de HIV obrigatórios é tida, em geral, como ofensiva aos direitos humanos, mas também implica violação de direitos fundamentais, muito embora no Brasil – convém sublinhar – tal prática já foi proibida.[38] Nesse contexto, Mann (1996) sugere

37 Sobre a questão da privacidade dos dados relacionados à Aids e também a informações genéticas ver N.A. Holtzman, *Proceed with Caution,* cit.; H. L. Dalton, S. Burris, *Aids and the Law,* New Haven, London, 1987; P. Sieghart, *Aids.*A UK Perspective, London, 1989; R. M. Cook-Deegan, *Public Policy Implications of the Human Genome Project*, in Z. Bankowski, A. M. Capron, *Genetics, Ethics and Human Values*, Geneva, 1991, p. 62.

38 O Ministério do Trabalho e Emprego (MTE) baixou a Portaria nº 1.249/2010, publicada no Diário Oficial em 31 de Maio – baseada na Lei 9.029 (abril/1995) e fundamentada na Portaria Interministerial nº 869 (Agosto/1992) , que proíbe que as empresas do Brasil exijam de seus funcionários o teste de HIV em exames médicos admissionais e demissionais, avaliações periódicas ou em decorrência de mudanças de cargo do trabalhador, de forma direta ou indireta, onde é vedada a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de emprego ou à sua manutenção. Ainda assim, a discriminação em geral persiste, e muitos soropositivos declaram-se constrangidos em manifestar sua condição em Unidades Básicas de Saúde de seus bairros de residência, por exemplo.

que devem existir negociações para um maior ajustamento das políticas ou programas de saúde (tais como os testes voluntários, e a atenção aos impactos sociais potencialmente desfavoráveis para as pessoas infectadas com o HIV) e as exigências relativas aos direitos humanos. Esta prática tem melhorado tanto a qualidade da saúde pública quanto a sensibilidade em relação aos direitos humanos e fundamentais e seu devido respeito e proteção no domínio da saúde. Assim, embora a existência de situações de discriminação, é de se questionar o acerto da proposição do mesmo autor quando sugere que mesmo sendo inadvertida e não intencional a discriminação é tão generalizada que seria mais adequado considerar toda a política e programa de saúde como de caráter discriminatório, salvo prova em contrário,[39] o que não significa, de outra parte, que a suspeita em relação ao cunho discriminatório não possa ser justificada em determinado contexto.

Mudanças tecnológicas, privacidade e informações em saúde

Informações em saúde são dados administrativos, assistenciais, epidemiológicos e clínicos,obtidos do cidadão por meio da prestação direta de serviços de saúde. A Lei nº 8.080/1990[40] normatiza as obrigações do Estado em relação ao direito à saúde, organização e funcionamento dos serviços de saúde no âmbito do SUS no Brasil. Além disso, garante o direito à informação do cidadão e impõe ao Estado o dever de implementar suas políticas e ações sanitárias, destacando a importância da informação na efetivação do direito à saúde. (VENTURA, 2013).

As novas tecnologias podem auxiliar a solucionar determinados problemas do sistema de saúde brasileiro relacionados às suas dimensões continentais, à deficiência na infraestrutura dos serviços de saúde, à desigualdade no acesso e até mesmo quanto às questões mais especí-

39 Quadro bastante catastrófico em relação ao desrespeito aos direitos humanos pelos programas de saúde pública é colocado por MANN, J. **Saúde Pública e Direitos Humanos**. Rio de Janeiro: PHYSIS. Saúde Coletiva, 6 (1/2), 1996, pp.139-140.

40 Brasil. Lei ordinária nº 8.080, de 19 de setembro de 1990. Lei Orgânica da Saúde. Diário Oficial da União 1990; 20 set.

ficas, como é o caso da falta de suporte para a obtenção de uma segunda opinião profissional. Nesse sentido, o uso das tecnologias de informação e comunicação representa boa possibilidade de melhorar esse cenário.[41] Uma das possibilidades para responder a tal demanda é a utilização de redes de telessaúde, no caso brasileiro, denominadas "Telessaúde Brasil Redes", gerenciadas pelo Ministério da Saúde, as quais consistem num suporte tecnológico para a transmissão de informações em saúde, viabilizando o envio eficiente de dados, imagens, registros, textos e sons a partir de qualquer computador.[42]

A telessaúde[43], conforme REZENDE et. al (2013), pode representar recurso que contribui para melhorar a qualidade da assistência e reduzir o tempo entre o diagnóstico e a terapêutica. Embora esse novo recurso proporcione benefícios na área da saúde, também atrai riscos que podem estar relacionados ao fator humano e às questões tecnológicas. A perda da confidencialidade das informações prestadas pelos pacientes constitui-se em um desses riscos, quando os pacientes são atendidos por meio da telessaúde, sejam essas informações arquivadas ou transmitidas por computadores. Assim, ainda que represente um avanço em termos de conexão de profissionais de várias localidades, tal prática acarreta preocupações relacionadas aos aspectos éticos e legais que possam garantir a privacidade pertinente a esta tecnologia por onde transitam informações de saúde dos usuários.

Para assegurar o respeito e a proteção da dignidade da pessoa e do correlato direito à privacidade faz-se necessário o uso de senhas e o controle de quem pode ter acesso às informações, porém, sobretudo, torna indispensável uma maior capacitação e formação ética para garantir

41 Ver a este respeito **World Health Organization. Information technology in support of health care [Internet]**. 2005, Geneva: Disponível em: <http://www.who.int/healthacademy/news/en/> acesso em: 05.03.2015.

42 Outro termo – a telemedicina – atualmente muito utilizado para se referir à assistência à saúde que utiliza tecnologias de comunicação, seja nos setores privados ou públicos. Há também publicações recentes que citam o *m-Health*, que corresponde à utilização da comunicação móvel e sem fio para a prestação de cuidados à saúde. Como o termo telemedicina está restrito às atividades médicas, prefere-se atualmente o termo telessaúde, que é mais abrangente e ainda muito utilizado, pois os serviços de saúde preconizam a dinâmica de atendimento multidisciplinar, cuja assistência à saúde inclui atividades dos demais profissionais da saúde ligados ao tema. Ver Conselho Brasileiro de Telemedicina e Telessaúde. Departamento de telemedicina. [Internet]. São Paulo; 2010. Disponível em: http://cbtms.com.br/departamentos/departamento-de-telemedicina/ acesso em 05/03/2015.

43 Ver, a título de exemplo, o Programa de Telessaúde do Ministério da Saúde: disponível em: http://www.telessaudebrasil.org.br.

a confidencialidade e a justa utilização de instrumentos como o Termo de Consentimento Livre e Esclarecido (TCLE). Ressalte-se que essas inovações tecnológicas tornam mais vulnerável a privacidade, uma vez que dados pessoais (e sensíveis) transitam em redes informatizas de várias instituições. Tais práticas, portanto, ainda carecem de melhor normatização, especialmente por parte dos conselhos de classe profissionais. A elaboração de protocolos específicos de proteção à privacidade dos usuários também pode auxiliar na proteção à privacidade dos dados pessoais.

Situação semelhante ocorre em relação ao prontuário do paciente, "documento único constituído por 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, utilizado para possibilitar a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo" (CFM 2002, artigo 1º.).

Justamente por receber registros de equipes multiprofissionais, qualquer prontuário apresenta inúmeras fontes de dados, incluindo procedimentos realizados em diversos setores por diferentes tipos de profissionais de saúde, o que resulta em significativa heterogeneidade no registro de dados, podendo apresentar desorganização e desagregação das informações, o que dificulta sua utilização e amplia os riscos de vazamento das informações. (MAJEWSKI & AZAMBUJA, 2004).

A tendência atual, dados os avanços na tecnologia da informação, é utilizar-se a modalidade eletrônica de prontuário, a qual possibilita que os dados do paciente sejam compartilhados em rede por toda a equipe que atende o paciente, sendo este intercâmbio possível inclusive entre diferentes instituições e longas distâncias (em nível nacional ou internacional). O Prontuário Eletrônico do Paciente (PEP) elimina o problema da ilegibilidade das informações, normalmente escritas à mão pelos profissionais nos prontuários de papel, fato que pode gerar interpretações errôneas dos dados dos pacientes. Todavia, em contrapartida, dada a maior facilidade de compartilhamento e a ampla disponibilidade de dados, o PEP propicia o risco de acesso indevido, uso inadequado e quebra de privacidade de indivíduos e instituições.

A solução tecnológica para a proteção dos dados constantes nos PEPs é conceber modelos de autorização e controle de acesso, prática

considerada indispensável para viabilizar o uso em larga escala do PEP em grandes instituições de saúde. MOTTA (2003) propõe um destes modelos destinados a dar tratamento adequado às exigências de controle de acesso ao PEP, buscando assegurar a privacidade do paciente e a segurança de acesso aos seus dados. Não obstante, o próprio autor destaca a privacidade como o principal problema ético relativo ao PEP lembrando que: a) o conteúdo do prontuário pertence ao paciente; b) as instituições e os profissionais envolvidos são obrigados a não revelar as informações fornecidas em confidência sem autorização prévia do paciente; e c) as instituições de saúde são responsáveis pelo estabelecimento de normas, rotinas de controle de acesso e de identificação dos usuários do PEP.

É importante ressaltar, ainda nesse contexto, que os dados constantes no PEP pertencem ao paciente, não aos profissionais nem às instituições. Em princípio, só com o seu consentimento poderia haver a revelação do conteúdo do prontuário, através do princípio ético da autonomia, o qual preconiza que o paciente tem direito de escolha, de que seja respeitada sua vontade, valores e crenças, de que se reconheça seu domínio sobre a própria vida e que se respeite sua privacidade e intimidade. A informatização dos prontuários sem os devidos cuidados com a confidencialidade e a segurança das informações dos usuários vem facilitando seu extravio e seu acesso indevido; os sistemas que utilizam redes de computadores tornam estes dados vulneráveis a acessos não autorizados; a facilidade de alteração de dados registrados eletronicamente traz perigos adicionais à vida e ao bem-estar dos pacientes, além de, por vezes, facilitar a fraude (SALVADOR E ALMEIDA FILHO, 2005).

Possíveis medidas para aumentar a segurança das informações em saúde que trafegam nas redes informatizadas passam pela criptografia forte[44] dos dados, centrais comutadoras e roteadores fiscalizados, homologados e livres de programas espiões (*backdoors*). [45] No caso específico

44 A criptografia é uma área de especialização da matemática e da engenharia que oferece técnicas de proteção a mecanismos de acesso e à integridade de dados, e ferramentas de avaliação da eficácia dessas técnicas. A criptografia fraca parece idêntica à criptografia forte na vitrine de software. Dois produtos de "encriptação" de correio eletrônico no mercado têm interface de usuário praticamente idênticas, enquanto um deles é seguro e o outro permite bisbilhotagem. Uma tabela contendo comparações entre recursos pode sugerir que dois produtos tenham funcionalidade similar, embora um possa ter furos comprometedores de segurança e o outro não. Um criptógrafo experiente pode reconhecer a diferença. Determinados tipos de criminosos também poderão.

45 *Backdoor* é uma espécie de porta virtual secreta, embutida em softwares, acionável remotamente por quem a conhece para dar passagem a dados.

dos dados de um paciente, registrados em um PEP, uma *backdoor* pode ser programada para "grampear por atacado o fluxo que por ali passa, em todo ou em parte selecionáveis por área de origem". Uma das possíveis medidas para aumentar a segurança do tráfego das informações em saúde é a adoção de softwares livres como alternativa aos softwares proprietários[46], para "utilizar a internet de forma mais segura contra a interceptação de terceiros, quando devidamente fiscalizada nas pontas de uma comunicação corretamente criptografada" (CORTIZO, 2007).

Porém, nada garante a segurança das informações sem o componente humano. Aqui convém lembrar que a relação entre os profissionais de saúde e os usuários, de maneira geral, pode ser considerada assimétrica, pois os primeiros detêm o maior número de informações e o controle do próprio instrumental tecnológico. O usuário, nesse sentido, pode ser considerado vulnerável, tendo em conta o seu estado de saúde e, na maior parte das vezes, o seu desconhecimento técnico e tecnológico. Por tais motivos fala-se em "corpo eletrônico" (uma extensão do corpo físico, formada pelos dados da pessoa que circulam virtualmente, uma espécie de "avatar") ao qual deveria ser estendida a tutela da personalidade "virtual" dos pacientes como derivação do próprio princípio da dignidade da pessoa humana. (RODOTÀ, 2008).

As informações privadas e a dimensão pública

Não obstante todas as garantias que devem ser asseguradas às informações privadas dos cidadãos, o seu direito à privacidade não é absoluto. Não por acaso, o desenvolvimento da legislação sobre a proteção dos dados pessoais foi acompanhado pela difusão de leis sobre o acesso às informações, normalmente públicas, mas em certos casos também privadas.[47]

46 Software livre é todo o programa que possui quatro liberdades: A liberdade de executar o programa, para qualquer propósito; A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades. Acesso ao código-fonte é um pré-requisito para esta liberdade; liberdade de redistribuir cópias de modo que você possa beneficiar o próximo; A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie. Acesso ao código-fonte é um pré-requisito para esta liberdade (CORTIZO, 2007).

47 Há leis que disciplinam conjuntamente a privacidade e o direito de acesso às informações, como, por exemplo, o *"Freedom of Information and protection of Privacy Act"*, 1987, Ontário.

No Brasil, assim como a privacidade das informações pessoais, o acesso à informação pública é um direito fundamental do cidadão, que estabelece a natureza pública e a disponibilidade de toda a informação produzida ou em poder do Estado. A recente Lei no 12.527/2011[48] regulamenta o amplo direito ao acesso à informação pública, determinando deveres estatais de gerir de forma eficiente a documentação governamental ou as informações que estejam sob sua guarda, viabilizando o seu conhecimento e a consulta a todos. Disponibilidade, autenticidade, integridade são os principais atributos legais da informação pública. A referida lei, contudo, admite restrições ao acesso às informações classificadas como sigilosas por razões de segurança e saúde pública, e às pessoais, cuja confidencialidade protege o direito à privacidade. (VENTURA, 2013).

A noção de privacidade atualmente abriga a noção da "proteção de dados", reconfigurando a discussão sobre a tutela individual e coletiva das informações, podendo a primeira sofrer limitações. As formas de limitação mais difundidas, que chegam a sacrificar a proteção da privacidade em prol de outros interesses, considerados – temporariamente ou não – prevalecentes, são bem conhecidas e em muitos casos estão previstas na própria legislação sobre bancos de dados. Dizem respeito, sobretudo, a interesses do Estado (segurança interna ou internacional, polícia, justiça) ou a relevantes direitos individuais e coletivos (tradicionalmente, o direito à informação, sobretudo como liberdade de imprensa; e cada vez mais intensamente o direito à saúde, principalmente em sua dimensão coletiva). (RODOTÀ, 2008)

O conhecimento científico sobre o estado de saúde das populações, por exemplo, está, cada vez mais, baseado no acúmulo de informações específicas sobre o tema. Assim, quanto maior o número de variáveis que se puder conhecer e controlar a respeito de cada evento do processo saúde/doença, maior a possibilidade de compreender esse processo, suas causas e suas condições. A existência de bancos de dados que permitam a identificação do indivíduo, de seu ambiente social, físico e, muitas vezes,

48 Brasil. Lei Ordinária nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º. No inciso II do § 3º. do art. 37 e no § 2º. do art. 216 da CRFB. Diário Oficial da União 2011; 18 nov.

econômico, representa um instrumento importante para o planejamento em saúde, o que, aliás, é do interesse da própria sociedade. Porém, a proteção do indivíduo, de sua dignidade, dos direitos humanos e fundamentais que lhe são correlatos, é igualmente um interesse da sociedade. Por essa razão, fala-se do "direito à liberdade informatizada", que foi elaborado por derivação do direito à privacidade. Equilibrar de forma justa a proteção à privacidade dos indivíduos e o desenvolvimento social que necessita de informações coletivas, como é o caso da saúde, constitui-se em grande desafio. (DALLARI, 2007).

Um exemplo desta dicotomia entre a necessidade de proteger a privacidade do indivíduo, por um lado, e, por outro, disponibilizar os dados agregados aos gestores e pesquisadores pode ser o Cartão Nacional de Saúde, instrumento que possibilita a vinculação dos procedimentos executados no âmbito do Sistema Único de Saúde (SUS) ao usuário, ao profissional que os realizou e também à unidade de saúde onde foram realizados. Para tanto, é necessária a construção de cadastros de usuários, de profissionais e de unidades de saúde. A partir desses cadastros, os usuários e os profissionais de saúde recebem um número nacional de identificação. O Sistema Cartão é coordenado pelo Ministério da Saúde, mas o seu desenvolvimento, guarda e manutenção das bases de dados situa-se na esfera da responsabilidade do Departamento de Informática do SUS (DATASUS/MS). Ainda que a Portaria[49] que o regulamenta proponha-se a garantir a segurança tecnológica da base de dados, respeitando-se o direito constitucional à intimidade, à vida privada, à integralidade das informações e à confidencialidade, bem como possibilitar o acesso do usuário do SUS aos seus dados, há muitos problemas relacionados à sua implementação, que já dura mais de dez anos.[50]

49 BRASIL. Ministério da Saúde. PORTARIA Nº 940, DE 28 DE ABRIL DE 2011. Regulamenta o Sistema Cartão Nacional de Saúde (Sistema Cartão). Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html> Acesso em: 11.03.2015

50 CUNHA, R. E. da. Cartão Nacional de Saúde, os desafios da concepção e implantação de um sistema nacional de captura de informações de atendimento em saúde. **Ciência Saúde Coletiva,** Rio de Janeiro, vol.7 nº 4, 2002.

Considerações finais

De tudo o que foi exposto e a partir dos exemplos citados, percebe-se que a garantia da privacidade das informações em saúde e a necessidade de uso público de determinados dados é altamente preocupante, especialmente quando se conhece as inúmeras possibilidades de geração de novas informações a partir dos dados inicialmente registrados. A atual sociedade da informação e as rápidas mudanças tecnológicas fazem com que se produzam paradoxos – entendidos no sentido de situações nas quais a privacidade aparentemente entra em contradição consigo mesma ou produz situações também inesperadas.

Trata-se de uma questão complexa e de difícil aprofundamento no âmbito do presente ensaio, pois, como bem coloca Rodotà (2008), exige articular ulteriormente a definição de privacidade, que, por um lado, se apresenta como o direito de manter o controle sobre as próprias informações, e, de outro, corresponde ao direito de determinar as modalidades de construção da própria esfera privada, dado que o objeto desse direito pode ser identificado como "patrimônio informativo atual ou potencial" de um determinado sujeito.

Na questão da privacidade das informações em saúde, ao mesmo tempo em que a tecnologia ajuda a moldar uma esfera privada mais rica, a torna mais frágil, cada vez mais exposta a ameaças, daí derivando a necessidade do fortalecimento contínuo de sua proteção jurídica e da ampliação das fronteiras do direito à privacidade, ainda que se saiba que do ponto de vista fático a violação da privacidade é algo que já se situa na ordem do dia e que a proteção do ponto de vista jurídico-normativo cada vez mais se revela de difícil concretização, revelando cada vez maiores défices de eficácia.

Com efeito, a sociedade atual, baseada na informação e no conhecimento, tornou mais frágeis as possibilidades de proteção à privacidade. A informação é a matéria-prima do novo paradigma e, como a informação é parte fundamental da atividade humana, os novos meios tecnológicos moldam diretamente a esfera da existência individual e coletiva. Assim a existência dessas novas tecnologias cria uma nova infraestrutura

material da comunicação digital, denominada "ciberespaço", que, além de todo o universo de informações que abriga, inclui os seres humanos que ali navegam e que alimentam esse espaço virtual com informações. Além disso, o fato de vivermos numa "Sociedade de Risco", onde o avanço tecnológico torna vulneráveis os mecanismos de proteção e de controle dos riscos sociais, políticos, econômicos e tecnológicos, evidencia que as informações podem ser possíveis causadores de perigo social, mas também podem operar como mecanismos de reconhecimento e proteção contra tais riscos.

Nesse contexto, para efeito de preservar o ser humano, sua dignidade e privacidade, algumas medidas práticas têm sido levadas a efeito, como a criptografia dos dados, o uso de senhas e o controle de quem pode ter acesso às informações em saúde, porém, sobretudo, torna-se indispensável uma maior capacitação e formação ética para garantir a confidencialidade e a justa utilização de instrumentos como o Termo de Consentimento Livre e Esclarecido (TCLE).

Faz-se necessária, outrossim, uma maior consciência cidadã no sentido de que fique claro que os dados pertencem aos usuários, não às instituições ou aos profissionais, podendo os primeiros requisitarem, averiguarem ou, inclusive, se recusarem a prestar determinadas informações, sem prejuízo dos serviços a que têm direito. Isto pode (e deve) ser feito diretamente durante os atendimentos de saúde ou, caso não se logre êxito, judicialmente, por meio dos instrumentos processuais disponíveis, como é o caso do *habeas data*. Por outro lado, cabe destacar que as instituições de saúde são as responsáveis pelo estabelecimento de normas e rotinas de controle de acesso e de identificação dos usuários das informações.

Dado que, de certa forma, não há como conter a quantidade e a qualidade das informações coletadas a respeito da saúde de determinado usuário, é preciso que este possa acessá-las e manter a possibilidade efetiva de controle sobre elas. A "autodeterminação" informacional deve garantir o direito de conhecer e alterar as próprias informações. Além disso, já num outro plano, há de ser assegurado o direito à não discriminação com base nas informações existentes.

As ações para superar os desafios e assegurar o devido respeito aos direitos fundamentais no que tange às informações em matéria de saúde

são de múltipla natureza, seja no plano da ética institucional, pessoal (na relação entre os profissionais e os pacientes), ou na esfera jurídica. O que mais se verifica, porém, é a necessidade de que sejam estabelecidos novos e eficazes marcos regulatórios, indispensáveis para o fortalecimento da privacidade como direito fundamental, especialmente no tocante aos dados pessoais e "sensíveis" como os constantes das informações em saúde.

Referências

AGUIAR, S. Redes sociais na internet: desafios à pesquisa. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 30., Santos, 2007. **Anais**... Santos: Intercom, 2007a. Disponível em: <http://www.sitedaescola.com/downloads/portal_aluno/Maio/Redes%20sociais%20na%20internet-%20desafios%20%E0%20pesquisa.pdf> Acesso em: 12 jan. 2015.

BECK, U. **Sociedade de risco**: rumo a uma outro modernidade, trad. Sebastião Nascimento. 2.ed. São Paulo: Editora 34, 2011.

BOYD, D. M.; ELLISON, N. B. Social network sites: definition, history, and scholarship. **Journal of Computer-Mediated Communication**, v.13, n.1, p.210-230, 2007. Disponível em: < http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> Acesso em: 27 fev. 2012.

CAPACHUZ, M. C. **Intimidade e vida privada no novo Código Civil brasileiro:** uma leitura orientada no discurso jurídico. Porto Alegre: Sérgio Antônio Fabris , 2006

CANOTILHO, J. J. G.; MOREIRA, V. **Constituição da República Portuguesa anotada**. 4. ed. Coimbra:Coimbra Editora, 2007. v.1.

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

CERQUEIRA, M.; KEINERT, T.; KEINERT, R. et al. Relatos sobre o cotidiano da população pobre e o princípio constitucional da dignidade da pessoa humana. **Boletim do Instituto de Saúde-BIS,** v. 12, n. 3, p. 220, dez. 2010.

CONSELHO FEDERAL DE MEDICINA. Resolução 1.638, de 09 de agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Brasília, D.F.: 2002.

CORTIZO, Carlos Tato. Sistemas de informática e informação da atenção básica do Sistema Único de Saúde e o software livre: possibilidades e perspectivas. (Dissertação de Mestrado) Faculdade de Saúde Pública da USP. São Paulo, 2007.

DALLARI, S. A justiça, o direito e os bancos de dados epidemiológicos**. Ciênc. saúde coletiva ,**v.12, n.3. Maio/Jun, 2007.

DÍEZ-PICAZO, L. M. **Sistema de derechos fundamentales**. 2.ed. Madrid: Civitas, 2005.

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

FIGUEIREDO, M. F. Algumas notas sobre a eficácia e efetividade do direito fundamental à saúde no contexto constitucional brasileiro**. Boletim do Instituto de Saúde –BIS,** v.12, n. 3, p. 220, dez. 2010.

GERMAN, C. **O caminho do Brasil rumo à era da informação**. São Paulo: Konrad-Adenauer-Stiftung, 2000.

GONÇALVES, M. E. **Direito da informação**: novos direitos e modos de regulação na sociedade da informação. Coimbra: Almedina, 2003.

HORN, H. Allgemeines Freiheitsrecht, Recht auf Leben u.a. In: Stern, K; Becker, F (Coord). **Grundrechte Kommentar.** Köln: Carl Heymanns, 2010.

KEINERT, T. M.; PAULA, S. H.B.; BONFIM, J.R.A. (Org.). **As ações judiciais no SUS e a promoção do direito à saúde**. São Paulo: Instituto de Saúde, 2009. (Temas em saúde coletiva, 10)

KLOEPFER, M. **Verfassungsrecht II – Grundrechte**. München: C.H. Beck, 2010.

LÉVY, P. **Cibercultura**. São Paulo: Ed.34, 2000.

LOJKINE, J. **A revolução informacional**. São Paulo: Cortez, 1995.

LOVETT, R. ; FISHER, J. ; AL-YAMAN, F. et al. A review of Australian health privacy regulation regarding the use and disclosure of identified data to conduct data linkage. **Australian and New Zealand Journal of Public Health**, v.32, n.3, p.282-285, 2008.

MANN, J. Saúde pública e direitos humanos. Physis: Rev. Saúde Coletiva, v.6, n.1-2, p.139-140, 1996.

MARQUES, G.; MARTINS, L. **Direito da informática**. Coimbra: Almedina, 2000.

MAJEWSKI, C.; AZAMBUJA, G. **Implantação do PEP na ótica dos usuários**. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS), 9., Ribeirão Preto, 2004. Ribeirão Preto, 2004. Disponível em: <http://telemedicina.unifesp.br/pub/SBIS/CBIS2004/trabalhos/arquivos/612.pdf>. Acesso em 5 março 2015.

MENDES, G.F.; BRANCO, P.G.G. **Curso de direito constitucional**. 6.ed. São Paulo: Saraiva, 2011.

MIRANDA, J.; MEDEIROS, R. **Constituição portuguesa anotada**. Coimbra: Coimbra Editora, 2005. v.1.

MONTEIRO, S.D. O Ciberespaço: o termo, a definição e o conceito. **DataGramaZero - Revista de Ciência da Informação**, Rio de Janeiro, v.8 n.3, jun.2007.

MORAES, I. H. S.; GÓMEZ, M. N. G. Informação e informática em saúde**:** caleidoscópio contemporâneo da saúde. **Ciência & Saúde Coletiva**, v.12, n.3, p.553-565, 2007.

MOTTA, G. H. M. B. **Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos.** 2003**.** Tese – Escola Politécnica da USP. São Paulo, 2003. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3142/tde-05042004-152226/publico/tese_Gustavo_Motta.pdf>. Acesso em: 5 março 2015.

NEGROPONTE, N. **Vida digital**. 2.ed. São Paulo: Companhia das Letras, 1995.

REZENDE, E.J.C.; TAVARES, E.C.; SOUZA, C. et al. Telessaúde: confidencialidade e consentimento informado. **Rev. Med. Minas Gerais**, v. 23, n.3,p. 367-373, 2013.

RHEINGOLD, H. **Comunidade virtual**. Trad. Helder Aranha. Lisboa: Gradiva, 1996.

SALVADOR, V.;FILHO, F**.** Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: JORNADA DO CONHECIMENTO E DA TECNOLOGIA, 2., Marilia, SP 22- 26 ago. 2005. Marília: UNIVEM, 2005. Disponível em: <http://www.uel.br/projetos/oicr/pages/arquivos/Valeria_Farinazzo_aspecto_etico.pdf>. Acesso em: 5 março 2015.

SANTOS JÚNIOR, D. L.; MANTOVANI, D. M. N. Comunicação nas redes sociais: um estudo com usuários das comunidades do Orkut. **Análise,** Porto Alegre**,** v.21, n.1, p.30-41, jan./jun., 2010. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/face/article/viewFile/8235/5905> Acesso em: 17 jan. 2012.

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

ROYO, J.P.. **Curso de derecho constitucional**, 12.ed. Madrid: Marcial Pons, 2010.

SARLET, I. W. **Dignidade da pessoa humana e direitos fundamentais na Constituição de 1988**. Porto Alegre: Livraria do Advogado, 2012.

_____. **A eficácia dos direitos fundamentais**. 12.ed. Porto Alegre: Livraria do Advogado, 2015.

SARLET, I. W.; FIGUEIREDO, M. F. Algumas considerações sobre o direito fundamental à proteção e promoção da saúde aos 20 anos da Constituição Federal de 1988. In*:* KEINERT, T. M.; PAULA, S.H.B; BONFIM, J.R.A (Org.). **As ações judiciais no SUS e a promoção do direito à saúde**. São Paulo: Instituto de Saúde, 2009. (Temas em saúde coletiva, 10)

SILVA, C. V. M. Direitos humanos e direitos fundamentais: realidade e herança da humanidade. In: BUCCI, D.; SALA, J. B.; CAMPOS, J. R. **Direitos humanos**: proteção e promoção. São Paulo: Saraiva, 2012.

SOLOVE, D. **Understanding Privacy.** Cambridge: Harvard University, 2008.

TEIXEIRA, E. D.; Haeberlin, M. **A proteção da privacidade:** aplicação na quebra do sigilo bancário e fiscal. Porto Alegre: Sérgio Antônio Fabris, 2005.

VENTURA, M. Lei de acesso à informação, privacidade e a pesquisa em saúde. **Cad. Saúde Pública,** v.29, n.4, p.636-638, abr. 2013.

VIANNA, T. **Transparência pública, opacidade privada.** Rio de Janeiro: Revan, 2007.

VIEIRA, T. M. **O direito à privacidade na sociedade da informação**. Porto Alegre: Sergio Antonio Fabris, 2007.

WERTHEIN, J. **A sociedade da informação e seus desafios**. Brasília, D.F.: Ciência da Informação, 2000.

6

Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde – privacidade e e-Health

Danilo Doneda[1]
Marília de Aguiar Monteiro[2]

Introdução

Steven Keating é um estudante do Instituto de Tecnologia de Massachussetts (MIT). Em 2007, aos 26 anos, uma tomografia de seu cérebro revelou uma pequena anormalidade, que deveria ser monitorada – o que foi realizado com bastante esmero pelo próprio estudante, que debruçou-se sobre estudos sobre a sua patologia até refazer o exame em 2010, revelando normalidade. Em suas pesquisas, ele sabia que sua anomalia encontrava-se perto da zona olfativa do cérebro. Em 2014, ao começar a sentir constantemente fragrâncias de vinagre, ele refez seus exames e foi operado de um tumor no cérebro do tamanho de uma bola de tênis. Durante todo esse processo, Steven Keating esteve em posse de todas as suas informações médicas, contabilizando um total de 70 gigabytes de prontuários, exames, consultas, etc; tais informações lhe permitiram monitorar, estudar e acompanhar de perto sua condição.

1 Danilo Doneda (ddoneda@gmail.com) é Bacharel em Direito pela Universidade Federal do Paraná (1995), Doutor em Direito pela Universidade do Estado do Rio de Janeiro (2004), Professor visitante na Faculdade de Direito da Universidade do Estado do Rio de Janeiro e Assessor do Ministério da Justiça.
2 Marília de Aguiar Monteiro possui graduação em Direito pela Fundação Getúlio Vargas (2012).

Para muitos especialistas, o caso de Steven Keating é uma prova cabal dos benefícios gerados aos pacientes do acesso total às suas informações médicas. Diante do controle sobre suas próprias informações, médicos acreditam que os pacientes serão mais diligentes para com suas condições físicas, seguirão de forma restrita as recomendações médicas e serão mais atentos a sinais recentes.

Uma maior proteção aos dados pessoais e também maior acesso a informações médicas são ambas condições para o empoderamento do cidadão em relação às suas próprias informações e para a diminuição das assimetrias de poder em relação a quem realiza o tratamento de suas informações pessoais. Ao mesmo tempo, o compartilhamento de informações sobre saúde é capaz de gerar consequências positivas para a sociedade, como no caso, por exemplo, do controle de epidemias, da troca de inteligência e várias outras situações, o que faz com que a delimitação da aplicação de regras de proteção à privacidade e de compartilhamento de informações seja bastante complexa.

Emblemático e inovador, no entanto, o caso de Steven Keating não pode ser visto propriamente como regra para o desenvolvimento de políticas públicas para saúde na sociedade da informação. Para Salah Mandil (2015), consultor sênior da Organização Mundial da Saúde (OMS) e da União Internacional de Telecomunicações para e-Health e e-Strategies e ex-Diretor para Health Informatics and Telematics da OMS, o desenvolvimento e investimento em computação, redes e comunicações para a saúde não deve ser realizado tendo parâmetro dominante a capacidade de inovação da indústria de tecnologia, mas sim mensurando seus efeitos na transformação do setor de saúde:

> "*Two core lessons have emerged from the practical experiences with e-Health of several countries. First, as the experiences of Singapore and Turkey have shown, e-Health support must not be tackled as an "information technology or IT project" but as a means for improving health care services. In other words, e-Health support must be conceived and managed as a means for health and clinical care transformation. Second, and as far as technology is concerned, the "solutions" must not*

> *be conceived as once-and-for-all, but must follow a judicious cost-effective approach of adopting and adapting the technologies and related procedures"* (MANDIL, 2015).

Termos como "em observação" ou "vigilância" são de longa data associados ao setor de saúde. Na sociedade da informação, tais associações ganham um caráter duplamente significativo. O uso de tecnologias de informação e comunicação em serviços de saúde tem o potencial de trazer diversos benefícios para a saúde pública e individual, uma vez que possibilita a criação de registros mais acurados sobre o cidadão e um compartilhamento mais eficiente e ágil de tais informações entre profissionais na saúde do que as formas tradicionais de registros de informações médicas.

Na perspectiva de proteção de dados, no entanto, os sistemas de informação de saúde também têm o potencial adicional de gerar e processar um número incrivelmente maior de dados pessoais – a maior sensibilidade e capacidade de coleta de informações de pacientes estão presentes tanto no novo instrumental do setor médico como em novos *gadgets* de uso cotidiano que, cada vez mais, vêm acompanhados de sensores capazes de monitorar aspectos referentes ao comportamento e condição de saúde de seus usuário. Isto amplia potencialmente o número de indivíduos capazes de acessar essas informações – gerando incentivos para que terceiros não envolvidos, necessariamente, na prestação do serviço ou do tratamento de saúde também possam querer acessar tais informações, como seguradoras de saúde.

Desta forma, a proteção de dados pessoais enquanto um direito fundamental atenta para o fato de que a agregação de informações de saúde do cidadão constantes em distintas fontes e bases de dados pode facilitar o acesso a informações sensíveis do cidadão. Colocamo-nos, portanto, diante de um cenário de análise de riscos distinto daquele já vivenciado por cidadãos e profissionais da saúde, diante de novas possibilidades de mau uso de informações de saúde, capaz de causar danos à privacidade ou a discriminação do cidadão.

A proteção especial dada aos dados de saúde nas legislações internacionais deriva não só da natureza muito mais íntima e reveladora desses dados, como dos potenciais riscos de discriminação a que o indivíduo

pode ser submetido diante das possibilidades de mau uso desses dados. A consideração de que a proteção de dados pessoais deva ser considerada como um direito fundamental do cidadão na sociedade da informação deriva, em grande parte, do fato de que esta proteção não visa somente à tutela de escolhas pessoais sobre a exposição da personalidade em público mas também visa garantir a liberdade do indivíduo em uma sociedade na qual um cidadão pode ser facilmente discriminado, pode perder oportunidades ou ser estigmatizado a partir de um tratamento abusivo de seus próprios dados – realidade esta que é mais patente e mais concreta quando os dados tratados são dados concernentes à saúde de um cidadão.

O direito fundamental à proteção de dados pessoais é algo que se vislumbra, talvez, na sua forma mais clara quando os dados pessoais tratados são dados de saúde. Neste sentido, é relevante que se vislumbre as características principais de um marco regulatório de proteção de dados pessoais.

A partir desta problemática, o presente texto tem por objetivo apresentar uma breve construção da noção de proteção de dados pessoais enquanto direito fundamental e apresentar como as primeiras normativas neste sentido lidaram com questões relacionadas a dados de saúde. Tradicionalmente, o tratamento de dados de saúde importa em desafios para padrões mínimos de proteção de dados pessoais como o consentimento, a responsabilidade dos atores envolvidos, segurança e integridade das informações, transparência, acesso e compartilhamento dos dados, seja em transferência internacional ou em comunicação e interconexão de bancos de dados.

A proteção de dados pessoais como direito fundamental

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação. Os dados pessoais (LYON, 1998,

p.384; CASTELLS, 1999) muitas vezes são a única representação do próprio indivíduo em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável.

O tratamento de dados pessoais, em particular aquele realizado por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais; na eventualidade destes dados não serem corretos e representarem erroneamente seu titular; em sua utilização por terceiros sem o conhecimento de seu titular, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo a proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e é considerada como um direito fundamental.

Informação e dados pessoais

Uma determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação refere-se às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta, e tantas outras. É importante estabelecer este vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem este vínculo objetivo; também a produção intelectual de uma pessoa, em si considerada, não é *per se* informação pessoal (embora o fato de sua autoria o seja). Podemos concordar com Pierre Catala, que identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> *"Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade"* (CATALA, 1983, p. 20).

O Conselho Europeu, através da sua Convenção 108, de 1981, ofereceu uma definição que condiz com esta ordem conceitual. Nela, informação pessoal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação" (CONSELHO DA EUROPA, 1981) [3]. É claro, portanto, o mecanismo pelo qual é possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

A informação pessoal está ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno desta relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Com o aludido aumento da importância da informação de uma forma geral, foi justamente em torno dela que a temática da privacidade passou a orbitar, em especial ao se tratar de dados pessoais. Esta guinada, que acabou por plasmar o próprio (DONEDA, 2006) conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas poderiam ser a concepção de uma *informational privacy* nos Estados Unidos, cujo "núcleo duro" é composto pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Federal

3 Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º.

alemão e a Diretiva 95/46/CE da União Europeia[4] (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), com todas suas consequências.

O ponto fixo de referência neste processo é que, entre os novos prismas para enquadrar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias.

Através da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser levados em consideração pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. Esta vinculação do tratamento de dados pessoais com o controle foi bem caracterizada pelo Ministro Ruy Rosado de Aguiar ainda em decisão de 1995:

> *"A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar*

4 A sentença de 15 de dezembro de 1983 do Tribunal Constitucional Federal alemão consolidou a existência de um "direito à autodeterminação informativa" (*informationelle selbstestimmung*), que consistia no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e transmissão de dados relativos à sua pessoa.

> *contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador"*[5].

Desenvolvimento das leis de proteção de dados

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos. E é caso emblemático de uma tendência que veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados. Este desenvolvimento foi intenso nas mais de quatro décadas que a disciplina ostenta (MAÑAS, 2005, p. 19). A mudança do enfoque dado à proteção de dados neste período pode ser brevemente entrevisto na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger (1997, p. 219), que vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais.

A primeira destas quatro gerações de leis [6] era composta por normas que refletiam o estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo destas leis girava em torno da concessão de autorizações para a criação destes bancos de dados e do seu controle *a posteriori* por órgãos

5 STJ, Recurso Especial nº 22.337/RS, rel. Min. Ruy Rosado de Aguiar, *DJ* 20/03/1995, p. 6119.

6 Exemplo destas leis de primeira geração são a Lei do *Land* alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados, sueca, que foi o Estatuto para bancos de dados de 1973 – *Data Legen 289,* ou *Datalag*, além do *Privacy Act* norte-americano de 1974.

públicos (SAMPAIO, 1997, p. 490). Estas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) destas normas. Esta primeira geração de leis vai aproximadamente até a *Bundesdatenschutzgesetz,* a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado desta tecnologia, sem que se soubesse ao certo suas consequências, fez com que se optasse por princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados, além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados (SIMITIS, 1997, p. 565). Este enfoque era natural, visto a motivação destas leis ter sido a "ameaça" representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática destas leis era tecnocrática e condicionada pela informática – nelas, tratava-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo (MAYER-SCÖNBERGER, 1997, p. 223).

Estas leis de proteção de dados de primeira geração não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento. A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da "diáspora" dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a lei francesa de proteção de dados pessoais de 1978, intitulada *Informatique et Libertées*[7], além da já mencionada *Bundesdatenschutzgesetz*. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas na consideração da privacidade e na proteção

7 Lei 78-17 de 6 de Janeiro de 1978.

dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da lei francesa). [8]

Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses. Além disso, o controle, nos moldes das leis anteriores, tornou-se inviável, dada a fragmentação dos centros de tratamento dos dados pessoais. Assim, criou-se um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela.

Estas leis apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente na sua exclusão de algum aspecto da vida social. Uma terceira geração de leis, surgida na década de 1980, procurou sofisticar a tutela dos dados pessoais, que continuou centrada no cidadão, porém passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa.

A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas neste sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não

8 Como representante desta geração de leis, podemos mencionar também a lei austríaca (*Datenschutzgesetz* (DSG), Lei de 18 de outubro de 1978, nº 565/1978); além de que as constituições portuguesa e espanhola apontam neste sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde.

da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

A autodeterminação informativa era, porém, o privilégio de uma minoria que decidia enfrentar os custos econômicos e sociais do exercício destas prerrogativas. Verificado este caráter exclusivista, uma quarta geração de leis de proteção de dados, como as que existem hoje em vários países, surgiu e caracterizou-se por procurar suprir as desvantagens do enfoque individual existente até então. Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nesta relação que não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa. Outra técnica é, paradoxalmente, a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre por conta do pressuposto que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual – como é o caso para certas modalidades de utilização de dados sensíveis.

Outras características são a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessárias com a diminuição do poder de "barganha" com o indivíduo para a autorização ao processamento de seus dados e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que um tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas Europeias em matéria de proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas).

Princípios de proteção de dados pessoais

A aludida "progressão geracional" das leis sobre proteção de dados pessoais faz referência, não por acaso, a uma linguagem própria da informática e exprime a lógica da busca por modelos jurídicos mais ricos e completos (RODOTÀ, 1999, p. 103). Não obstante essa sua marcada mudança de perfil com os anos, é possível reagrupar materialmente seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em diversos graus em ordenamentos vários – no que podemos verificar uma forte manifestação da convergência das soluções legislativas sobre a matéria em diversos países, bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais.

Destes princípios, alguns se encontram já presentes nas leis de primeira e segunda geração, tendo sido desenvolvidos pelas leis posteriores. Uma busca mais larga poderá, porém, retraçar suas origens em uma série de discussões que, na segunda metade da década de 1960, acompanhou a tentativa do estabelecimento do *National Data Center*, que consistiria basicamente em um gigantesco e jamais realizado banco de dados sobre os cidadãos norte-americanos para uso da administração federal (GARFINKEL, 2000, p. 13; MILLER, 1971). [9]

Após o fracasso da tentativa de instituição deste banco de dados centralizado, vários dos temas que foram levantados em meio à discussão sobre sua possibilidade continuaram a ser desenvolvidos, pois se o *National Data Center* particularmente não vingou, a realidade era que muitos outros bancos de dados pessoais de menor âmbito iam se estruturando. Uma das áreas na qual esta discussão ecoou com maior força foi justamente a da saúde, pela fundada preocupação com o tratamento de dados médicos por sistemas informatizados. No início da década de 1970,

9 O *National Data Center* foi projetado para reunir as informações sobre os cidadãos norte-americanos disponíveis em diversos órgãos da administração federal em um único banco de dados – a partir de um projeto original, que pretendia unificar os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Simson Garfinkel. *Database nation.* Sebastopol: O'Reillly, 2000, p. 13. Após acirradas discussões sobre a ameaça potencial que representaria às liberdade individuais, o governo norte-americano desistiu do projeto. V. Arthur Miller. *Assault on privacy*. Ann Arbor: University of Michigan, 1971.

a *Secretary for Health, Education and Welfare* reuniu um comissão de especialistas que divulgou, em 1973, estudo que conclui pela relação direta entre a privacidade e os tratamentos de dados pessoais, além da necessidade de estabelecer a regra do controle sobre as próprias informações:

> *"A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais for a destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei"* (EUA, 1973).

Uma concepção como esta requer que sejam estabelecidos meios de garantia para o cidadão, que efetivamente vieram descritos como:

> *"• Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.*
> *• Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.*
> *• Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.*
> *• Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.*
> *• Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados*" (EUA, 1973).

Tais regras contidas no documento, de caráter marcantemente procedimental, apresentaram um conjunto de medidas que passou a ser encontrado em várias das normativas sobre proteção de dados pessoais, às quais se passou a referir como *Fair Information Principles* (BENNET, 1992, p. 98). Este "núcleo comum" encontrou expressão como um conjunto de princípios a serem aplicados na proteção de dados pessoais principalmente com a Convenção 108 (CONSELHO DA EUROPA, 1981) e nas Diretrizes da OCDE (OECD, 2013; WUERMELING, 1996, p. 416) [10] [11] que serão tratados de forma mais detalhada em seções a seguir, no início da década de 1980. É possível elaborar uma síntese destes princípios (RODOTÀ, 1999, p. 62; SAMPAIO,1997, p. 509) :

1. *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência; ou do envio de relatórios periódicos.
2. *Princípio da exatidão*: Os dados armazenados devem ser fieis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.
3. *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um cri-

10 Convenção nº 108 do Conselho Europeu – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.

11 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, disponível em: < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >. Estes princípios seriam: "(1) collection limitation principle; (2) data limitation principle; (3) purpose specification principle; (4) use limitation principle; (5) security safeguard principle; (6) openness principle; (7) individual participation principle". Ulrich Wuermeling. "Harmonization of European Union Privacy Law", in: 14 *John Marshall Journal of Computer & Information Law* 411 (1996), p. 416.

tério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

4. *Princípio do livre acesso*, pelo qual o indivíduo tem acesso ao banco de dados onde suas informações estão armazenadas, podendo obter cópias destes registros, com a consequente possibilidade de controle destes dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.
5. *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais. E é bastante significativo que o documento que pode ser tido como fundador em relação aos princípios de proteção de dados hoje presentes em praticamente toda legislação sobre o tema, tenha sua origem em discussões internas em um órgão responsável pelo setor de saúde.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e a sua consideração como um direito fundamental em diversos ordenamentos. Alguns países que sofreram uma mudança de regime político que lhes proporcionou a reelaboração de suas cartas fundamentais foram os primeiros nos quais foi possível observar uma tendência à consideração da problemática relacionada à informática e à informação pessoal em nível constitucional. Neste sentido, nas constituições da Espanha e de Portugal se encontram dispositivos destinados a afrontar os problemas da utilização da informática e, no caso da Constituição portuguesa,

uma referência explícita à proteção de dados pessoais (ESPANHA, 1978; PORTUGAL, 2005). [12] [13]

É possível considerar a Convenção 108 como o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais. Em seu preâmbulo, a convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao artigo 8º da Convenção Europeia para os Direitos do Homem. Posteriormente, também transparece com clareza a presença dos direitos fundamentais na Diretiva 95/46/CE [14] [15] sobre proteção de dados pessoais na União Europeia. Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais".

12 A **Constituição espanhola** de 1978 contém os seguintes dispositivos:

Art. 18. – (...) 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

(...) Art. 105. – (...) b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

13 A **Constituição portuguesa** de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:

"Artigo 35.º (Utilização da informática)

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

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

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

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

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

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

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

14 Cujo teor é o seguinte:

1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

15 Mencione-se, de passagem, que a expressão "direitos fundamentais" é evocada por seis vezes nas considerações iniciais da Diretiva.

O documento europeu que levou mais adiante esta sistemática foi, certamente, a Carta dos Direitos Fundamentais da União Europeia, proclamada em 7 de dezembro de 2000. Seu artigo 8º, que trata da "proteção de dados pessoais", inspira-se no artigo 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286 do tratado instituidor da União Europeia (PARLAMENTO EUROPEU, 1995; UNIÃO EUROPEIA, 2006) [16]. Não obstante, nota-se um duplo matiz: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio através do estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais (MACARIO, 1997, p. 8) [17].

Proteção de dados no ordenamento brasileiro

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

16 De seguinte teor:

"Artigo 286.

1. A partir de 1 de Janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.

2. Antes da data prevista no nº 1, o Conselho, deliberando nos termos do artigo 251, criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adoptará as demais disposições que se afigurem adequadas".

17 Este caráter levou alguns autores a desencorajarem a leitura da diretiva em chave de direitos fundamentais do homem em relação à informação pessoal, apesar de reconhecerem que, "dal punto di vista più genuinamente privatistico, non v'è dubbio che la direttiva ... sia destinata a diventare un punto di riferimento fondamentale nella ricostruzione sistematica dei diritti della personalità, almeno nella misura in cui il concetto di personalità si trovi a far i conti con la realtà informatica e telematica". v. Francesco Macario. "La protezione dei dati personali nel diritto privato europeo", in: Vicenzo Cuffaro. Vicenzo Ricciuto. *La disciplina del trattamento dei dati personali*. Torino: Giappechelli, 1997, p. 8-9.

A bem da verdade, pode-se encontrar uma menção ao caráter de direito fundamental da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo governo brasileiro em 15 de novembro de 2003. No item 45 da referida Declaração, lê-se que:

> *"Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade."*

A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição brasileira contempla o problema da informação inicialmente através das garantias à liberdade de expressão (BRASIL, 1988b) [18] e do direito à informação (BRASIL, 1988a) [19], que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro (CARVALHO, 2003, p. 77).

18 Constituição brasileira, art. 5º, IX; art. 220.

19 Constituição brasileira, art. 5º, XIV; art. 220; incluindo o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos (art. 5º, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5º, XXXIV).

O *habeas data*, instituto que no direito brasileiro tem a forma de uma ação constitucional, foi introduzido pela Constituição de 1988 (BRASIL, 1988c) [20]. Com um *nomen iuris* original, introduziu em nosso ordenamento o direito de acesso, carregando com si algo da carga semântica do *habeas corpus*. A sua influência em outras legislações latino-americanas chegou a provocar a discussão sobre a existência de um modelo de proteção de dados que circule dentro do subcontinente. Cabe ressaltar que o *habeas data* brasileiro surgiu basicamente como um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e sem maiores vínculos, portanto, com uma eventual influência da experiência europeia ou norte-americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época (PUCCINELLI, 1999). Posteriormente o *habeas data* foi regulamentado pela Lei 9.507, de 1997.

O modelo de proteção de dados da União Europeia

A base normativa fundamental para a proteção de dados pessoais na União Europeia é formada pela Diretiva 46/95/EC (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) e pela Diretiva 2002/58/EC (relativa à privacidade e às comunicações eletrônicas). Quando, em 1995, a Diretiva de Proteção de Dados foi aprovada, o objetivo foi justamente, a partir da uniformização de regras concernentes à proteção de dados, assegurar o livre fluxo de dados pelos países do bloco, garantindo maior eficiência a uma economia fortemente baseada em serviços e no fluxo de informações. Para tal, partiu-se de um modelo normativo instituído sobre o reconhecimento da proteção dos dados pessoais como um direito fundamental na Sociedade da Informação.

20 Constituição Federal, art. 5º, LXXII:

"Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo"

Materialmente, a diretiva apresenta instrumentos de proteção de dados que podem ser lidos como uma derivação direta das regras presentes na Convenção 108 do Conselho da Europa (Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais) (CONSELHO DA EUROPA, 1981). Essa Convenção orienta os Estados-membros a adotarem normas específicas para o tratamento de dados pessoais, em obediência aos parâmetros de proteção que ela própria apresentava. Sua perspectiva, aliás, não é meramente europeia, tendo sido aberta para adesões também de países não membros do Conselho da Europa[21].

A importância fundamental da Convenção reside em um motivo: o Conselho da Europa entende a proteção de dados como uma questão inserida na esfera dos direitos humanos, considerando a proteção de dados como elemento essencial para a proteção da liberdade e da privacidade.

A Diretiva 46/95/EC, estruturada a partir deste marco, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, porém procura igualmente fomentar o comércio através do estabelecimento de regras comuns para proteção de dados na região, consideradas as exigências de um mercado unificado como o europeu em harmonizar as regras relativas a dados pessoais.

A influência dos direitos fundamentais na Diretiva é clara. Nesse sentido, seu artigo 1º expressa uma primeira finalidade do texto legal ao afirmar que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais". Já de acordo com sua segunda finalidade, "(...) os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso econômico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos". Há, portanto, dois eixos em torno dos quais a inteira disciplina se estrutura e que consideram os dados pessoais como

21 Mesmo países que não são membros do Conselho da Europa, como Marrocos e Uruguai, solicitaram a adesão à referida Convenção.

direito fundamental – a proteção da pessoa e a necessidade de proporcionar a livre circulação de "pessoas, mercadorias, serviços e capitais" no espaço comunitário, o que implica a circulação de dados pessoais.

A estrutura da Diretiva foi transposta para a legislação de todos os países da União Europeia – os quais, não raro, utilizaram-se inclusive de técnicas legislativas semelhantes. Tal estrutura compreende a definição de uma terminologia específica combinada com princípios gerais de proteção de dados e o estabelecimento de regras materiais básicas a serem seguidas, como a necessidade da coleta, tratamento e utilização dos dados pessoais estar vinculada àqueles princípios. Os princípios da Diretiva devem ser incluídos pelos Estados-membros em suas legislações internas, de modo a garantir a defesa dos interesses protegidos, além de compreenderem uma série de limites e exceções ao tratamento de dados pessoais. Além disso, a Diretiva submete indistintamente tanto setor público quanto privado à mesma disciplina de proteção de dados.

A Convenção 108 do Conselho da Europa

O Conselho da Europa foi criado em 1949 com o objetivo de engajar entre seus países-membros valores democráticos, de direitos humanos e do Estado de Direito (BENETT e RABB, 2006). A partir da década de 1960, por sua vez, um Comitê de Especialistas (*Committee of Experts*) foi criado no âmbito do Conselho da Europa para discutir recomendações para a proteção da privacidade ante o avanço da computação moderna. Diante do avanço da utilização de sistemas automatizados e dos potenciais impactos que estas tecnologias poderiam significar para a vida dos cidadãos europeus, as regras existentes para proteção à privacidade foram consideradas inadequadas e insuficientes.

Adotada em 1981, a Convenção 108 – Convenção para a Proteção de Indivíduos em relação ao processamento automáticos de dados pessoais – é o primeiro instrumento jurídico internacional em respeito à proteção de dados pessoais. Embora não obrigue juridicamente seus signatários, a Convenção 108 acabou por tornar-se um texto – quadro para países ausentes de uma normativa de proteção de dados pessoais, ao estabelecer

padrões mínimos de proteção contra abusos emergentes da coleta e do processamento de dados pessoais.

O aspecto fundamental da proteção de dados pessoais é expresso no parágrafo 25 da explanação de motivos ao determinar que o direito à proteção de dados pessoais compreende a proteção da privacidade, no entanto é estendido para além deste, compreendendo demais direitos e liberdade fundamentais:

> *"The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms [...] it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example: privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field."* (CONSELHO DA EUROPA, 1981)[22]

O artigo 5º pode ser visto como um dos primeiros princípios para o processamento e coleta de dados pessoais:

> *a. obtained and processed fairly and lawfully;*
> *b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
> *c. adequate, relevant and not excessive in relation to the purposes for which they are stored;*
> *d. accurate and, where necessary, kept up to date;*
> *e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*

22 Convention 108 < http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

Em seu artigo 6º, a Convenção 108 introduz a ideia de que certas categorias especiais de dados pessoais não deveriam ser tratados senão diante de salvaguardas jurídicas no ordenamento jurídico nacional. Dados relacionados à saúde caem nesta categoria especial de dados:

> *Article 6 – Special categories of data*
> *Personal data revealing racial origin, political opinions or religious or other beliefs, as well as* ***personal data concerning health*** *or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.*

Um Comitê *Ad Hoc* para Proteção de Dados Pessoais (CAHDATA), no âmbito do Conselho da Europa, aprovou em 3 de Dezembro de 2014 as propostas de modernização da Convenção 108.

As Diretrizes de Privacidade da OCDE

Em 1978, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) criou um grupo de especialistas em tráfego transfronteiriço de dados com o propósito de elaborar um modelo (*model law*) para o tráfego internacional de dados. O grupo teve como base inicial um conjunto de princípios idealizados pelo Departamento de Saúde, Educação e Bem Estar Social dos EUA para potencializar a utilização da informática sem prejudicar a privacidade: os Princípios Justos de Informação (*Fair Information Principles*). O resultado foi a elaboração, em 1980, das *Guidelines on the Protection of Privacy and Transboarder Flows of Personal Data* – a qual nos referiremos como Diretrizes de Privacidade da OCDE, ou simplesmente Diretrizes. O documento passou a estabelecer uma série de parâmetros para a regulação da proteção de dados, enunciados em princípios sobre os quais deveriam se basear as atividades. Foram traçados oito princípios: 1) limitação da coleta; 2) qualidade dos dados; 3) especificação do propósito; 4) limitação do uso; 5) salvaguardas à segurança; 6) abertura; 7) participação individual; e 8) transparência (DONEDA, 2006; BENNET e RAAB, 2006) .

As Diretrizes representam a primeira tentativa de lidar com a transferência transfronteiriça de dados no âmbito global. Os seus princípios têm um duplo objetivo: promover um padrão mínimo de proteção à privacidade e aos dados pessoais e evitar, sempre que possível, a restrição ao fluxo transfronteiriço de dados por parte dos países. O principal foco das Diretrizes é o tráfego dos dados e não propriamente a tutela do seu titular (KUNER, 2011; DONEDA, 2006). Nesse sentido, a Seção 18 da Diretriz aconselhou os países a evitarem o desenvolvimento de leis e práticas de proteção da privacidade e de liberdades individuais que possam criar obstáculos ao tráfego transfronteiriço de dados pessoais e que excedam as exigências para tal proteção. Os países só poderiam impor restrições à transferência quando o outro país envolvido não observasse a Diretriz ou quando a reexportação de tais dados pudesse violar a legislação doméstica de privacidade. As restrições poderiam, ainda, dizer respeito a certas categorias de dados pessoais com regulação específica presente na legislação doméstica e para os quais o outro país não oferecesse proteção equivalente (BENNET e RAAB, 2006)

A despeito de sua importância, os princípios previstos pelas Diretrizes acabaram por se tornar apenas um documento de referência comum na área, uma vez que os países integrantes da OCDE não foram obrigados a implementá-la em seu ordenamento interno. Outro fator que influenciou o enfraquecimento do documento da OCDE foi a iniciativa do Conselho da Europa de regular a matéria através de uma convenção – a Convenção 108/1981 –, que se tornaria, posteriormente, um primeiro passo para a criação de um sistema integrado europeu de proteção aos dados pessoais (DONEDA, 2006).

Em 1985, os Ministros dos países da OCDE adotaram uma Declaração sobre Fluxo Transfronteiriço de Dados (*Declaration on Transborder Data Flows*), na qual reconheceram a diversidade dos participantes envolvidos nos tráfegos internacionais de dados e sua crescente importância e benefícios para a economia internacional. Por meio dessa declaração, os países se comprometeram a: (i) promover o acesso a dados, informações e serviços relacionados, bem como evitar a criação de barreiras injustificadas à troca internacional de dados e informação; (ii) buscar transparência nas regulações e políticas relacionadas a serviços de informação,

computação e comunicações que afetam os tráfegos transfronteiriços de dados; (iii) desenvolver abordagens comuns para lidar com questões relacionadas ao tráfego transfronteiriço e, quando apropriado, desenvolver soluções harmônicas; e (iv) considerar possíveis implicações para outros países quando tratarem de dado relacionado ao tráfego transfronteiriço de dados (BENNET e RAAB, 2006).

Outras duas Diretrizes relacionadas foram lançadas na década de 1990 pela OCDE. A primeira foi um conjunto de orientações sobre Segurança dos Serviços de Informação (*Security of Information Services*), com o propósito de fornecer um quadro para a proteção da disponibilidade, integridade e confidencialidade dos sistemas de informação (computadores, instalações de comunicações, redes de computadores e de comunicação). O segundo instrumento, as Diretrizes para Política de Criptografia (*Guidelines for Cryptography Policy*), de 1997, teve como foco os direitos dos usuários de escolherem métodos criptográficos, a liberdade do mercado para desenvolvê-los, a interoperabilidade, as consequências para a proteção dos dados pessoais e da privacidade, o acesso legal a dados criptografados e a redução das barreiras ao comércio internacional (BENNET e RAAB, 2006).

Em 2013, após um processo de revisão que foi iniciado em 2010 por ocasião dos 30 anos das *Guidelines*, foi aprovada e publicada a sua versão atualizada [23].

As Diretrizes de Privacidade da cooperação econômica da Ásia e do Pacífico (APEC)

A APEC – *Asia-Pacific Economic Cooperation* – ou Cooperação Econômica da Ásia e do Pacífico consiste em um fórum econômico composto por 21 países (economias-membro oficiais) criado com o intuito de promover o livre comércio e a cooperação econômica na região do Pacífico e da Ásia [24]. O fórum é composto em grande parte por economias de industrialização recente e conta com 21 países-membros, sendo eles: Austrália,

23 http://www.oecd.org/sti/ieconomy/privacy.htm>
24 http://www.apec.org/About-Us/About-APEC.aspx

Brunei, Canadá, Chile, China, Indonésia, Japão, Coreia do Sul, Malásia, México, Nova Zelândia, Papua-Nova Guiné, Peru, Filipinas, Rússia, Singapura, Taiwan, Tailândia, Estados Unidos da América, Vietnã e Hong Kong.

Em 2004, foram introduzidas no âmbito da APEC as Diretrizes de Privacidade (*APEC Privacy Framework*), com o fim de encorajar o livre fluxo de dados para incremento da área negocial, consumerista e governamental na região. As diretrizes estabelecem princípios comuns de privacidade de dados para jurisdições na região pacífico-asiática, sem, contudo, obrigar a adoção interna ou a aplicação da diretriz pelos membros. O modelo permite que os países regulem as matérias avaliando os meios mais convenientes para implementar as diretrizes, seja através da via legislativa, seja administrativa ou mesmo por meio da autorregulamentação da indústria. O objetivo é evitar barreiras desnecessárias ao livre fluxo de informações, também no que tange à transferência de dados, estimulando o livre comércio (TAN, 2008).

Os nove princípios constantes das Diretrizes de Privacidade da APEC são: 1) prevenção de dano; 2) aviso prévio; 3) limitações de coleta; 4) uso de informações pessoais; 5) escolha; 6) integridade das informações pessoais; 7) garantias de segurança; 8) acesso e correção; e 9) *accountability* (responsabilidade ou prestação de contas) (APEC, 2005; PINHO e SACRAMENTO, 2009). [25]

Além destes nove princípios, o modelo prevê: o aprimoramento do compartilhamento de informações entre órgãos governamentais; a facilitação da transferência segura de informações entre as economias; um conjunto comum de princípios de privacidade; o uso de dados eletrônicos como meio de aprimorar e expandir negócios; e a cooperação mútua entre as economias no tratamento político e regulatório da privacidade.[26]

25 De acordo com o texto original em inglês os princípios são: 1) preventing harm; 2) notice; 3) collection limitations; 4) uses of personal information; 5) choice; 6) integrity of personal information; 7) security safeguards; 8) access and correction; 9) accountability. Disponível em: http://www.apec.org/Groups/Committee-on-Trade-and--Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx. Acesso em: 7 Mar 2013. Optamos por manter o princípio de accountability em inglês por não haver termo em português que o traduza em sua plenitude. Para mais sobre o assunto, veja. PINHO, J. A. G; SACRAMENTO, A. R. S. **Accountability: já podemos traduzi-la para o português?** Revista de Administração Pública (RAP). Rio de Janeiro, 43(6):1343-1368, nov./dez. 2009. Disponível em: http://www.scielo.br/pdf/rap/v43n6/06.pdf. Acesso em 7 Mar 2013.

26 http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

As Diretrizes de Privacidade da APEC não proíbem a exportação de dados para países cujo grau de proteção não seja adequado – ao contrário da Diretiva 46/95/EC. O modelo encoraja o liberalismo informacional e estimula a cooperação transfronteiriça em investigação e implementação de suas recomendações entre os países. As Diretrizes de Privacidade da APEC são uma tentativa de atingir um balanço regulatório que seja útil tanto para indivíduos quanto para empresas.[27]

Graham Greenleaf, em análise comparativa entre o modelo das Diretrizes da APEC e o modelo europeu, identifica quatro pontos em que o primeiro se distancia do segundo:

> *(i) seu conjunto de princípios pode ser caracterizado como 'OECD Lite' (Greenleaf, 2004), mais fraco que o da Diretiva ou a maioria das leis regionais, e sem valor adicional (Greenleaf 2008); (ii) uma completa falta de obrigações para aplicação dos princípios através da lei (autorregulação sem legislação de apoio é aceita pela APEC), ou mesmo uma recomendação de legislação; (iii) não há obrigação complementar de garantia do livre fluxo de dados pessoais em troca da adoção de padrões básicos (na melhor das hipóteses, há um encorajamento do desenvolvimento de regras sobre fluxo transfronteiriço de dados mutuamente acordadas pelas empresas; e (iv) um princípio de 'Accountability' que consiste em um substituto incoerente aos limites à exportação de dados (...)"*

Adicionalmente, o autor aponta que as Diretrizes de Privacidade da APEC têm fracassado em termos de adoção por economias-membro da APEC e as critica pela falta de obrigatoriedade de internalização e de mecanismos para aplicação e cumprimento das diretrizes. Ao invés disso, GREENLEAF (2013) demonstra que as economias da região têm sido muito mais influenciadas pelos padrões europeus da Diretiva de Proteção de Dados 46/95/EC.

27 http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Conclusão

A evolução das normativas de proteção de dados pessoais não é uma mera adequação regulatória a uma nova dimensão do fenômeno tecnológico referente ao tratamento de dados pessoais – tanto não o é que não é possível perceber na atual disciplina da proteção de dados pessoais uma mera atualização da normativa que, classicamente, esteve ligada ao tema da privacidade. Novas demandas e a necessidade de garantir outra ordem de direitos e de valores viram-se incluídas na disciplina de proteção de dados pessoais, tais como a necessidade de estabelecer ferramentas contra a discriminação, estratificação e privação de liberdade pessoal a partir do tratamento de dados pessoais.

O tratamento de dados de saúde é um caso emblemático para o acompanhamento desta trajetória que impulsionou a proteção de dados pessoais e consolidou a presença, em diversos ordenamentos jurídicos, de um direito fundamental autônomo referente à proteção de dados pessoais. Os dados de saúde refletem de forma concreta a ligação direta da personalidade aos dados pessoais e a sua utilização hoje chama para a necessidade de uma nova pactuação que permita tanto a proteção da pessoa para que não seja discriminada pelo mau uso de seus dados pessoais, como, na maior medida possível, a uso compartilhado destes dados de forma que não seja capaz de causar danos e discriminação ao seu titular. E, ainda, nesta equação deve haver espaço para que a pessoa decida de forma autônoma e livre sobre suas próprias opções em relação à proteção e uso de seus dados de saúde.

Referências

ASIA-Pacific Economic Cooperation-APEC. **Privacy Framework**. Singapura, 2005. Disponível em: <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>. Acesso em: 28 abr. 2015.

BENNET, C.; RAAB, C. **The Governance of privacy:** Policy Instruments in Global Perspective. 2.ed. Cambridge, MA: MIT Press. 2006.

BENNETT, C. **Regulating privacy. Data protection and public policy in Europe and United States**. Itahaca: Cornell University, 1992.

BRASIL. Constituição (1988a) Art. 5º, XIV; art. 220; incluindo o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos (art. 5º, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5º, XXXIV). Brasília, D.F.: Senado Federal, 2015. Disponivel em: <http://www.senado.gov.br/legislacao/const/con1988/CON1988_07.05.2015/CON1988.pdf> Acesso em: 28 abr. 2015.

BRASIL. Constituição (1988b) Art. 5º, IX; art. 220. Dispõe sobre livre expressão da atividade intelectual. Brasília, D.F.: Senado Federal, 2015. Disponível em: <http://www.senado.gov.br/legislacao/const/con1988/CON1988_07.05.2015/CON1988.pdf> Acesso em: 29 abr. 2015.

BRASIL. Constituição (1988c) Art. 5º, LXXII Dispõe sobre o Habeas Data. Brasília, D.F.: Senado Federal, 2015. Disponivel em: <http://www.senado.gov.br/legislacao/const/con1988/CON1988_07.05.2015/CON1988.pdf> Acesso em: 28 abr. 2015.

CARVALHO, A.P.G. O consumidor e o direito à autodeterminação informacional. **Revista de Direito do Consumidor**, n. 46, p. 77-119, abril-junho 2003.

CASTELLS, M. **A sociedade em rede. A era da informação, economia, sociedade e cultura.** São Paulo: Paz e Terra, 1999. V.1.

CATALA, P. Ebauche d'une théorie juridique de l'information. **Rivista Informatica e Diritto**, Firenze, v.9, p. 15-31, jan-apr. 1983.

CONSELHO DA EUROPA. **Convenção Europeia nº 108, de 28 de Janeiro de 1981**. **Para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal.** Estrasburg, 1981. Disponível em: <http://conventions.coe.int/Treaty/ITA/Treaties/Html/108.htm>. Acesso em: 8 abr. 2015.

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

ESTADOS UNIDOS DA AMERICA. U.S. Department of Health, Education & Welfare. Records, computers and the rights of citizens. **Report of the Secretary's Advisory Committee on Automated Personal Data Systems.** Washington, DC, 1973. Disponível em: <http://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 29 abr. 2015.

ESPANHA. CONSTITUIÇÃO (1978) **Dispõe sobre a utilização da Informática.** Madrid, 1978. Disponivel em: <http://www.congreso.es/consti/constitucion/indice/index.htm>. Acesso em: 29 abr. 2015.

GARFINKEL, S. **Database nation.** Sebastopol: O'Reillly, 2000.

GREENLEAF, G. Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. **Journal of Law, Information & Science**, v.23, n.1, 2014. Disponível em: <http://ssrn.com/abstract=2280877>.

KUNER, C. **Regulation of transborder data flows under data protection and privacy law: past, present and future**". Paris, OCDE, 2011. 40 p. (OECD Digital Economy Papers, 187). Disponível em: <http://dx.doi.org/10.1787/5kg0s2fk315f-en>. Acesso em: 29 abr.2015

LYON, D. The roots of the information society idea. In: O'SULLIVAN, T.; JEWKES. I. (Ed.). **The media studies reader**. London: Arnold, 1998. p. 384-402.

MACARIO, F. La protezione dei dati personali nel diritto privato europeo. In: CUFFARO, V.; RICCIUTO, V. **La disciplina del trattamento dei dati personali**. Torino: Giappechelli, 1997.

MAÑAS, J.L.P. El derecho fundamental a la protección de datos personales (LOPD). In: PIÑAR MAÑAS, J. L. **Protección de datos de carácter personal en Iberoamérica**. Valencia: Tirant Lo Blanch, 2005. p. 19-36.

MANDIL, S. e-Health is health care transformation, not "an IT project". **Eastern Mediterranean Health Journal**, Cairo v. 21, n. 2, p 81-82, 2015, Disponível em: <http://www.emro.who.int/emhj-volume-21-2015/volume-21-issue-2/ehealth-is-health-care-transformation--not-an-it-project.html>. Acesso em: 28 abr. 2015

MAYER-SCÖNBERGER, V. General development of data protection in Europe. In: AGRE, P.: ROTENBERG, M. (Org) **Technology and privacy:** the new landscape. Cambridge: MIT Press, 1997. p. 219-242.

MILLER, A. **Assault on privacy**. Ann Arbor: University of Michigan, 1971.

ORGANIZAÇÃO PARA COOPERAÇÃO ECONÔMICA E O DESENVOLVIMENTO-OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Paris, 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 28 abr. 2015.

PARLAMENTO EUROPEU. **Diretiva 95/46/CE DE 24 de Outubro de 1995. Dispõe sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Estrasburg, 1995. Disponível em: < http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 28 abr. 2015

PORTUGAL. Constituição (2005). Art 35. Dispõe sobre a utilização da Informática. Lisboa, Assembleia da República, 2005. Disponível em: <http://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf>. Acesso em: 28 abr. 2015.

PUCCINELLI, O. **El habeas data en Indoiberoamérica**. Bogotá: Temis, 1999.

RODOTÀ, S. **Repertorio di fine secolo**. Bari: Laterza, 1999.

PINHO, J.A.G; SACRAMENTO, A.R.S. Accountability: já podemos traduzi-la para o português? **Revista de Administração Pública (RAP)**. Rio de Janeiro, v.43, n.6, p.1343-1368, nov./dez. 2009. Disponível em: <http://www.scielo.br/pdf/rap/v43n6/06.pdf>. Acesso em: 7 Mar 2013.

SAMPAIO, J.A.L. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1997.

SIMITIS, S. Il contesto giuridico e politico della tutela della privacy. **Rivista Critica del Diritto Privato**, Napoli, v.15, n.4, p. 563-581, 1997.

TAN, J.G. A Comparative Study of de APEC Privacy Framework – A New Voice in The Data Protection Dialogue. **Asian Journal of Comparative Law,** v.3, n.1,2008 DOI:10.2202/1932-0205.1071.

UNIÃO EUROPEIA. Versão Consolidada do Tratado que institui a Comunidade Europeia – Artigo 286. **Jornal Oficial da União Europeia,** Bruxelas, 29 dez. 2006. Disponível em: <https://www.ecb.europa.eu/ecb/legal/pdf/ce32120061229pt00010331.pdf>. Acesso em: 29abr. 2015.

WUERMELING, U. Harmonization of European Union Privacy Law. **John Marshall Journal of Computer & Information Law,** Chicago, v. 14, n. 3, p. 411- 460, 1996.

7

Direitos da Personalidade, sigilo e confidencialidade das informações em saúde

Ana Carla Bliacheriene[1]

Conceito e natureza jurídica do Direito da Personalidade

Ao se propor escrever sobre privacidade, sigilo e confidencialidade da informação sob o olhar jurídico, torna-se absolutamente indispensável tratar dos Direitos da Personalidade, ou seja, daqueles direitos afeitos à condição do "ser", aqueles direitos afeitos à condição de ser "pessoa".

No Direito, a pessoa pode adquirir o sentido intuitivo e até normal como aquele ser humano que é portador da vida, mas também pode ter um sentido dado exclusivamente pela lei como o é o da personalidade jurídica (a das empresas).

Assim, para o Direito, pessoas físicas ou jurídicas são "pessoas" e, portanto, detentoras de personalidade. Os animais não são detentores de tal designação. Isto significa que aqueles que são detentores do título de "pessoa" e, portanto, têm personalidade para a lei, serão protegidos por um conjunto de garantias de seus Direitos de Personalidade, dentre os quais os que trataremos neste artigo.

1 Ana Carla Bliacheriene (acb@usp.br) é Doutora em Direito Social pela PUCSP, livre-docente em Direito Financeiro pela Faculdade de Direito-USP e Professora Associada de Finanças Públicas e Orçamento e de Direito Econômico da Faculdade de Direito de Ribeirão Preto.

Às pessoas físicas garante-se o exercício de todos os direitos da personalidade às jurídicas alguns deles.

A divisão do mundo entre ser ou não considerado pessoa foi um marco histórico nas relações humanas. Índios e negros não eram considerados pessoas ao tempo em que eram "legalmente" escravizados e negociados. A mulher, embora considerada pessoa, teve por muito tempo seus direitos restringidos, como alguém que necessitava da curatela masculina. Os portadores de necessidades especiais, as crianças, os portadores de quadros psiquiátricos, embora sejam pessoas que ainda não exercem, em plenitude, sua capacidade jurídica, têm adquirido cada vez mais algumas concessões, no sentido do exercício de uma autonomia possível, em respeito à integralidade dos seus Direitos da Personalidade.

Mas que seria esse Direito da Personalidade? É um direito, *subjetivo* (que se refere à pessoa que o detém), *inato (*que já nasce com o detentor, independentemente de ser declarado ou reconhecido por alguém é inerente à condição humana e sem o qual a pessoa não subsiste dignamente). É um complexo (material e espiritual).

Embora seja um plexo de direitos privados (regulado pelo Código Civil) não perde seu caráter público, uma vez que, em sua grande maioria, tem natureza de Direito Fundamental e, portanto, Direito Constitucional.

Assim, a violação ao Direito da Personalidade implica ferir a dignidade humana. Não obstante isto, sua proteção não é ilimitada, pois não se trata de "direitos dos egoísmos individuais".

Direitos da Personalidade em Espécie

Considerando o entendimento que os direitos da personalidade são aqueles que compõem a identidade da pessoa, poderá se dividir em grandes grupos. Listamos abaixo os principais:

- Direito à Vida
- Direito à Integridade Física
- Direito ao Corpo
- Direito a partes separadas do Corpo
- Direito ao Cadáver

- Direito à Imagem
- Direito à Voz
- Direito à Intimidade
- Direito à Integridade Psíquica
- Direito ao Segredo
- Direito à Identidade
- Direito à Honra
- Direito ao Respeito
- Direito às Criações Intelectuais (Direito Autoral)

Na relação do paciente com os profissionais de saúde, bem como na adoção de PEP´s por organizações de saúde, alguns destes direitos podem, eventualmente, ser violados. A leitura subliminar desta assertiva é a de que os profissionais de saúde, bem como os empregados das organizações de saúde são responsáveis pela preservação destes direitos, quando haja alguma possibilidade de violação, decorrente da relação de prestação de serviços de saúde ou de guarda e manipulação de dados do paciente.

Não é sem razão que os conselhos de classe têm, cada vez mais, editado normas protetivas dos pacientes nas relações com instituições e profissionais de saúde.

Fundamento Legal

A base normativa dos direitos da personalidade tem fundamento constitucional no art. 5º, que trata dos Direitos Fundamentais.

Já no art. 1º da CF/88 alça como fundamento do Estado Democrático de Direito, dentre outros, a dignidade da pessoa humana.

O princípio da isonomia estampado no caput do art. 5º, que se segue dos direitos fundamentais, aponta para aquilo que teremos como Direitos da Personalidade, que podem impactar diretamente na adoção dos PEP´s em organizações de saúde, tais quais:

> I - homens e mulheres são iguais em direitos e obrigações, nos termos desta Constituição;
>
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias;

VIII - ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei;

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

XXVII - aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar;

XXVIII - são assegurados, nos termos da lei:

a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;

b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas;

XXIX - a lei assegurará aos autores de inventos industriais privilégio temporário para sua utilização, bem como proteção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e econômico do País;

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo

ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

XXXIV - são a todos assegurados, independentemente do pagamento de taxas:

a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder;

b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal;

LXVIII - conceder-se-á *habeas-corpus* sempre que alguém sofrer ou se achar ameaçado de sofrer violência ou coação em sua liberdade de locomoção, por ilegalidade ou abuso de poder;

LXIX - conceder-se-á mandado de segurança para proteger direito líquido e certo, não amparado por *habeas-corpus* ou *habeas-data*, quando o responsável pela ilegalidade ou abuso de poder for autoridade pública ou agente de pessoa jurídica no exercício de atribuições do Poder Público;

LXXII - conceder-se-á *habeas-data*:

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

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

Esses direitos têm aplicação imediata, independentemente de que qualquer tipo de lei ou norma ordinária (não constitucional) seja publicada. Assim, ainda que não houvesse capítulo próprio no Código Civil, a parte constitucional dos direitos de personalidade já estariam garantidos.

No entanto, o art. 12 do Código Civil assevera que "pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei".

Atributos do Direito da Personalidade

Não obstante sua essência pública, dentre os atributos do Direito da Personalidade está o fato de ser um direito: privado; inato; vitalício; absoluto; extrapatrimonial; indisponível; intransmissível; irrenunciável; impenhorável; inexpropriável; e imprescritível.

Para melhor compreender os atributos do direito da personalidade da pessoa física, utilizemos um exemplo prático do direito ao nome.

É um direito privado, ou seja, regulado pelas leis civis.

É inato, ao nascer com vida já tenho direito a ele, ainda que morra momentos depois do parto.

É vitalício, pois durante toda a vida me será garantido. É absoluto, não cabe ressalvas.

É extrapatrimonial, ou seja, independe de valor comercial e nos casos em que o nome também tenha valor comercial, este será um efeito econômico deste e não sua essência. Não se pode dispor (doar, vender, alugar) deste como essência, embora se possa usufruir de seus benefícios econômicos, sem lhe retirar o caráter personalíssimo.

É intransmissível, embora seus efeitos econômicos possam sê-lo, ou seja, posso ceder o direito da exploração econômica de um nome reconhecido, mas não seu atributo personalíssimo.

Irrenunciável em termos de que nem que por desgosto com um pai ou uma mãe se pode renunciar ao direito de ter um nome.

Impenhorável e inexpropriável, pois dívidas ou processos não podem me retirar qualquer esfera dos meus direitos das personalidades, embora possa atingir os efeitos patrimoniais destes.

Imprescritível, já que sua violação gera, a qualquer tempo, o direito de ação reparadora ou inibitária, por parte de seu detentor, e de reparação por parte do violador.

Elementos dos Direitos da Personalidade

Os direitos da personalidade têm elementos físicos, materiais e os atinentes ao desenvolvimento da personalidade.

Dentre os elementos físicos estão a proteção da pessoa enquanto organismo vivo, como a garantia ao direito à vida (afastar comportamento que coloquem em risco a vida, como aborto, eutanásia, pena de morte, suicídio, experimentação em humanos) e o direito ao corpo (integridade física e psíquica do corpo e de suas partes).

Os elementos morais partem do pressuposto de que cada pessoa é única e irrepetível; assim, protege-se a identidade pessoal como seu nome e sinais distintivos, o direito à imagem, direito à honra, direito à vida privada.

Por fim, os elementos atinentes ao desenvolvimento da personalidade têm forte aproximação com o direito à liberdade e seus princípios balizadores (legalidade, liberdade contratual, liberdade matrimonial e liberdade laboral.)

Limitações do Direito da Personalidade

Não obstante tantas garantias e tanta proteção jurídica, os Direitos da Personalidade não são ilimitados. Gozam de limites que devem ser balizados a partir de três óticas.

Há as chamadas limitações voluntárias nas quais o detentor do direito mitiga sua aplicação plena, respeitados os limites da lei. Como quando um paciente assina, num procedimento eletivo, um termo de consentimento informado dos riscos do procedimento médico ao qual se submeterá. Ali está muito claro que mesmo ocorrendo qualquer evento adverso, numa situação técnica sob controle, que possa gerar dano ao seu corpo ou sobre parte dele, o detentor do direito (o paciente) está disposto a correr o risco na busca da melhor qualidade de vida ou da saúde integral.

Outra limitação é o abuso de direito o que impede, por exemplo, que o detentor de um direito autoral o seja pela eternidade. O direito à informação e à universalização do conhecimento faz com que direitos autorais tenham limitação temporal para sua exploração econômica. Embora o direito à autoria do conhecimento seja imprescritível, o direito à sua exploração econômica tem limitação estabelecida na lei.

Outro tipo de limitação é a colisão de direitos que não é protegida pelo ordenamento jurídico. Em tempos sobre a polêmica do parto vaginal (normal) ou cirúrgico (cesariana) uma mãe poderia se negar a se submeter a uma cesariana quando a indicação médica[2] aponta claramente como sendo a via segura de parto para mãe e filho, alegando direito ao corpo e às suas partes e colocando em risco a vida da criança ou de ambos? Certamente a resposta é negativa. Vê-se claramente uma colisão de direitos.

Proteção dos Direitos da Personalidade

A proteção de direitos, também conhecida como tutela no direito, pode ser dar de maneira preventiva ou de maneira repressiva. A preventiva tenta inibir a lesão ao direito protegido, a repressiva pode visar estabelecer o status anterior à lesão, quando possível, ou indenizar uma lesão irreparável. Pode haver também tutela repressiva que vise às duas medidas reparadoras.

Há também a possibilidade de reparação dos chamados danos (morais e matérias) que sofram o detentor do direito violado e todo aquele que concorra ao dano – por ato próprio ou de terceiro a este subordinado – tem o dever jurídico da reparação.

Assim, a proteção do dano pode se dar por tutela preventiva ou tutela inibitória que pode ser acionada, a depender do caso por mandatos de segurança, liminares em ações judiciais de obrigação de fazer ou de ações de obrigação de não fazer algo.

As tutelas ressarcitórias podem apontar para uma reparação pecuniária (em dinheiro), tais quais: ressarcimento de despesas; incapacidade física; prejuízo dos que dependiam economicamente; danos morais e materiais devido a dano à integridade física; danos morais devido a aspectos da personalidade; danos que afetam ao livre desenvolvimento da personalidade.

Pode-se também requerer uma tutela ressarcitória não pecuniária (em dinheiro), mas *in natura* entregando o bem desejado em lugar do valor equivalente ao mesmo.

2 Considere, neste exemplo, que a indicação medica é tecnicamente a mais adequada.

Conclusão

A adoção de PEP´s por profissionais e organizações de saúde, certamente traz vantagens comparativas positivas quanto à manutenção do histórico do paciente e à garantia da segurança dos mesmos nos sistemas de saúde, com destaque para o SUS.

Não obstante isto, sua adoção requer uma série de preocupações de ordem técnica, ética e também jurídicas.

A finalidade deste texto foi discutir as implicações jurídicas que esta opção poderia causar no confronto com os direitos à privacidade, sigilo e confidencialidade das informações dos pacientes, tidos duplamente como direitos da personalidade e como direitos fundamentais do ser humano.

Observa-se, a partir da análise da proteção jurídica destes direitos, que a responsabilidade dos profissionais de saúde, dos prepostos das organizações de saúde e, principalmente, destas é relevante para a proteção dos direitos de todos os envolvidos no atendimento assistencial.

Defende-se a necessidade do estabelecimento do maior nível de proteção possível das informações do (e sobre o) paciente (sem comprometer a operacionalidade do modelo eletrônico), a fim de proteger seus direitos fundamentais e evitar eventuais condenações dos prestadores e seus prepostos ou inibir a utilização absolutamente essencial para o atendimento em saúde pública na era da tecnologia da informação.

Embora seja um desafio importante, deve ser enfrentado com coragem para atingir os objetivos de uma prestação de serviços de saúde ágil, segura e de qualidade no SUS.

Referências

BITTAR, C.A. **Os direitos da personalidade**. 7.ed. Rio de Janeiro: Forense Universitária, 2008.

BORGES, R.C.B.. **Direitos de personalidade e autonomia privada**. 2.ed. São Paulo: Saraiva, 2007.

GONÇALVES, D.C. **Pessoa e direitos da personalidade: Fundamentação ontológica da tutela.** Lisboa: Almedina, 2008.

HOGEMANN, E.R. Danos morais e direitos da personalidade: Uma questão de dignidade. In: KLEVENHUSEN, R.B**. Direito público e evolução social**. 2.ed. Rio de Janeiro:Lumen Juris, 2008.

LEMBO, C**. A pessoa e seus direitos.** São Paulo: Manole, 2007.

OLIVEIRA, N.M.P. **O direito geral de personalidade e a "solução do dissentimento". Ensaio sobre um caso de "constitucionalização" do direito civil**. Coimbra: Coimbra Editora, 2002.

III

Segurança das informações, privacidade e informática em saúde

8

Epistemologia em informática em saúde

Eliane Colepícolo[1],
Alex Esteves Jaccoud Falcão[2],
Fabio Oliveira Teixeira[3]
Ivan Torres Pisa[4]

A informática em saúde surgiu como uma aplicação da informática à medicina. Shortliffe (1995) explica que o surgimento da área ocorreu por 3 motivos principais: 1) devido aos avanços da computação e das tecnologias de informação e comunicação; 2) à consciência crescente de que a base de conhecimento da medicina e das demais áreas da saúde não pode ser gerenciada apenas em suporte papel; 3) à convicção de que o processo de tomada de decisão é tão importante para a medicina quanto a coleção de fatos nos quais estas decisões são baseadas, e que ambos podem ser otimizados com o auxílio da informática. Shortliffe (1995) descreveu uma necessidade da implantação de setores de tecnologia nas escolas médicas, ação que tem se tornado uma realidade cada vez mais comum em todo o mundo. Nas últimas décadas a informática médica foi ampliando seu escopo para além da medicina, atrelando-se à necessidade de organização

1 Eliane Colepícolo (ecolepicolo@hotmail.com) é graduada em Ciência da Informação e Biblioteconomia, Doutora em Psicologia e Chefe da Seção de Acesso a Bases de Dados da Biblioteca Comunitária da Universidade Federal de São Carlos (UFSCar).
2 Alex Esteves Jaccoud Falcão é Pesquisador do Grupo Saúde 360º da Universidade Federal de São Paulo (UNIFESP).
3 Fabio Oliveira Teixeira é Mestre e Doutorando do Programa de Pós-gradução em Gestão e Informática em Saúde, Universidade Federal de São Paulo (UNIFESP).
4 Ivan Torres Pisa (ivanpisa@gmail.com) é Bacharel em matemática, Professor-adjunto do Departamento de Informática em Saúde, Escola Paulista de Medicina, UNIFESP e Vice-coordenador do Curso de Especialização em Informática em Saúde, UAB/UNIFESP, 3ª edição.

do conhecimento e da pesquisa em ciências da saúde. Mais que isso, seu escopo inclui a ideia de otimizar processos relacionados às práticas dessas ciências, por meio das tecnologias da informação e comunicação, fomentando projetos multidisciplinares envolvendo informática e ciências da saúde. Tais fatos justificaram denominá-la informática em saúde.

Nos dias de hoje o processamento de informação e de comunicação tornou-se essencial para muitas atividades em ciências da saúde, incluindo: registro e recuperação de informação sobre pacientes; comunicação entre profissionais de saúde; acesso à literatura médica; seleção de procedimentos diagnósticos; interpretação de resultados de laboratório e coleção de dados clínicos (Georgiou, 2002). A área vem se tornando essencial na pesquisa em ciências da saúde e, mais recentemente, nas pesquisas biológicas. Com isto, a informática em saúde vem se estabelecendo e se consolidando como uma área de conhecimento independente.

A informática em saúde é uma disciplina que envolve diversas áreas do conhecimento, tanto científicas quanto tecnológicas e até mesmo artísticas, e vem sendo considerada de importância primordial para os avanços das ciências da saúde e da informática em todo o mundo. Esta importância foi enfatizada por Parent et al. (2001) ao afirmar, na década passada, que a globalização efetiva ainda estava em curso de se concretizar porque ainda não existia uma distribuição equitativa do uso das tecnologias da informação. Essa realidade é válida nos dias de hoje. Parent et al. (2001) propuseram ações para melhorar essa realidade no âmbito da saúde global que envolvem essencialmente a informática em saúde, tais como a implantação cada vez mais ampla de sistemas de informação em saúde na internet, a descentralização da avaliação de dados em saúde e o treinamento em informática em saúde.

Este capítulo apresenta um estudo epistemológico da informática em saúde que inclui uma análise estatística de termos em artigos publicados no PubMed (ncbi.nlm.nih.gov/pubmed), um estudo epistemológico e uma pesquisa de opinião com especialistas. Nosso objetivo ao realizar este estudo foi buscar compreender as nomenclaturas que são utilizadas na literatura ou em reuniões científicas e propor um mecanismo de classificação de revistas e indexação de artigos que respeite tais nomenclaturas.

Terminologia em Informática em Saúde

A evolução da área da informática em saúde promove fenômenos similares aos que ocorrem em outras áreas de ciências mais maduras. Uma delas é sobre sua própria natureza, não havendo um consenso a respeito do que ela é como disciplina: uma ciência, uma tecnologia, uma arte, uma tecnociência? Talvez uma integração de tudo isso ou talvez não. As discussões ocorrem concomitantemente ao crescimento da própria área, mas poucas respostas são conclusivas, por serem em geral baseadas mais em opiniões do que em pesquisas propriamente ditas. Portanto, parece importante termos avaliações panorâmicas do campo para colaborar com a formação de estudantes, profissionais e pesquisadores das ciências da saúde para esta nova realidade, na qual os computadores são amplamente utilizados no apoio ao cuidado do paciente, na avaliação da qualidade do cuidado em saúde, na tomada de decisão, administração, planejamento e pesquisa em saúde (Van Bemmel 1999).

A área que se ocupa da análise panorâmica de uma disciplina do conhecimento é a epistemologia, que é um dos ramos da filosofia da ciência. Logo, estudar a epistemologia da informática em saúde é buscar compreender de forma ampla o seu arcabouço de conceitos, métodos, técnicas e seu comportamento como arte, ciência, tecnologia ou tecnociência. Na literatura científico-tecnológica relativa à informática em saúde encontram-se poucos estudos epistemológicos sobre a área que apresentem um corpo sólido de conhecimento e que possibilite qualificá-la como uma ciência com teoria, métodos e técnicas estabelecidos, seja ela básica ou aplicada. Mais que estudos epistemológicos, poucos são os estudos baseados em técnicas estatísticas que comprovem ou refutem a natureza epistemológica da informática em saúde. Ainda, um estudo teórico e prático sobre a epistemologia da informática em saúde torna-se útil para que instituições de ensino e pesquisa em informática em saúde tenham mais subsídios e critérios para elaborar seus planos curriculares, para desenvolver suas pesquisas e para publicar seus resultados.

O estudo e uso de terminologias têm trazido importantes avanços para áreas interdisciplinares à informática em saúde, tais como inteli-

gência artificial, mineração de dados, mineração de textos, busca e recuperação de informação, entre outras áreas da computação, amplamente utilizadas em aplicações para as ciências (Ebecken 2003). Como tipos de terminologias podemos citar vocabulários controlados, cabeçalhos de assuntos, ontologias e tesauros, que têm por objetivo a indexação, classificação, busca e recuperação de documentos, a partir de processos de análise e síntese. Os tesauros, mais sofisticados que vocabulários controlados e cabeçalhos de assuntos, apresentam controle persistente e relações de vários tipos entre os termos. Por este motivo, os tesauros vêm ganhando cada vez mais espaço como instrumento de indexação e classificação de informação, em substituição aos vocabulários controlados e cabeçalhos de assunto. Isto porque apresentam, além das relações hierárquicas entre os termos, relações de equivalência e de associação, definições conceituais e uma série de outras informações importantes sobre os termos que o compõem. Com isto, a rede de relacionamentos entre os termos se torna mais rica e sofisticada, o que pode ser útil nas estratégias de formulação da pesquisa e também nos resultados da busca por informação a partir de um termo do tesauro.

Um tesauro pode ser definido como um vocabulário controlado que representa hierarquias, relações de equivalência, pertinência e associações entre os termos, com objetivo de auxiliar o usuário potencial a encontrar a informação de que necessita com a menor margem de erro possível (Ebecken, 2003). Os termos de um tesauro podem ser construídos por uma única palavra ou por várias palavras, formando um termo composto. Os termos de um tesauro são comumente denominados termos descritores, que Lancaster (1972) define como termos atribuídos por um indexador a um documento para descrever seu assunto. As relações hierárquicas de um tesauro são as relações de ordenação entre os termos, ou seja, a superordenação (acima de), a subordinação (abaixo de) e a coordenação (na mesma ordem, igual a). As relações de equivalência envolvem o estudo e delimitação de termos diferentes com um mesmo significado e termos idênticos com significados diferentes, entre outras relações de equivalência entre termos já estabelecidos pela gramática das línguas, ou seja, sinônimos, antônimos, parônimos e homônimos. Junto às relações de equivalência são estabelecidas as relações de pertinência,

que envolvem o estabelecimento de um termo padrão, com conceito e escopo bem definidos. Desta forma fica instituído que o termo padrão será pertinente e seus sinônimos proibidos. Isto não impede a pesquisa por sinônimos, porque remete o usuário, ao utilizar um termo proibido, ao termo permitido. As relações associativas entre termos de um tesauro são aquelas que não se enquadram nas relações hierárquicas, nem nas de pertinência ou equivalência e, ainda assim, permanecem e são importantes para a recuperação da informação.

Tesauro para Modelagem de Domínios

O tesauro surge como uma alternativa para resolver estes problemas característicos do uso da linguagem natural, mapeando, por exemplo, os termos que representam o mesmo conceito, selecionando um termo apenas como padrão e os restantes como sinônimos, além de estabelecer relações entre estes termos e outros a estes relacionados. O tesauro pode ainda representar a riqueza dos relacionamentos associativos e hierárquicos de tal maneira que usuários possam limitar suas pesquisas a níveis de especificidade mais restritos ou mais amplos, melhorando os resultados da busca. Além disso, técnicas e ferramentas da mineração de textos em estudo na inteligência artificial e na linguística computacional vêm utilizando tesauros como instrumentos para modelagem de domínios específicos e para extração automática de informação, a partir de conjuntos de textos (corpus) que resultam numa série de aplicações, por exemplo, para indexação.

Um tesauro pode ser considerado como uma linguagem para modelagem de domínio, ou seja, uma linguagem especializada que abrange a maioria dos conceitos e relações conceituais de uma área específica, podendo ser utilizada como instrumento para uma série de aplicações na área. Um dos principais objetivos de uma linguagem especializada é estabelecer limites de abrangência conceitual do domínio, assim como eliminar a ambiguidade dos conceitos, dando maior coerência e consistência ao conhecimento do domínio. Tanto o desenvolvimento de linguagens especializadas contribui para a redução da ambiguidade, quanto a redu-

ção da ambiguidade promove o desenvolvimento de linguagens especializadas e ambas contribuem para a formalização do conhecimento de um domínio. Maas et al. (2001) afirmam que o caminho para a maturidade científica da informática em saúde (medical informatics) é a formalização do conhecimento pertinente ao domínio. Ressaltam que o desenvolvimento de linguagens para modelagem de domínios específicos das ciências da saúde é essencial ao desenvolvimento da Informática em Saúde, tal como ocorre em áreas como a de sistemas de informação, na qual as linguagens de modelagem de domínios são utilizadas como fundamento do sistema de informação daquele domínio. Se a Informática em Saúde é considerada um tema do escopo da ciência da informação, questões relacionadas a remover a ambiguidade da informação médica fazem parte de seus assuntos centrais. Logo, a informática em saúde como ciência deve buscar respostas não ambíguas às questões do seu domínio, do contrário faltará a esta disciplina uma fundamentação teórica adequada que a eleve ao status de uma ciência (Maas et al., 2001).

Pesquisas realizadas

Considerando a importância na realização de pesquisas teóricas sobre a epistemologia da informática em saúde, tivemos interesse em compreender a área sob abordagens teórica e prática, a partir de três estudos complementares: um estudo epistemológico, um estudo terminológico e um estudo estatístico. O objetivo desta pesquisa foi aplicar um conjunto de métodos e técnicas integrados para efetuar um estudo epistemológico da Informática em Saúde e analisar a tendência desta área do conhecimento para a ciência, tecnologia, tecnociência ou arte, a partir de um referencial teórico embasado na epistemologia de Bunge (1969). Considerando o tesauro como instrumento de sistematização de um domínio do conhecimento pode-se compreender o motivo pelo qual o tesauro vem sendo tão valorizado e utilizado em detrimento de terminologias mais simples como os cabeçalhos de assuntos. Por isto decidimos neste trabalho transformar o Medical Subject Headings (MeSH) (NLM, 2005) (nlm.nih.gov/mesh) em um tesauro e, a partir deste, desenvolver

um tesauro especializado em informática em saúde, o qual denominamos EpistemIS (Colepícolo, 2008), disponível na web (telemedicina6.unifesp.br/epistemis).

Este estudo foi realizado no grupo de pesquisa Saúde 360 junto ao Programa de Pós-graduação em Informática em Saúde, EPM, UNIFESP. A pesquisa foi conduzida como um projeto de mestrado por Eliane Colepícolo, intitulado "Epistemologia da Informática em Saúde: entre a teoria e a prática", cujo foco concentrou-se na integração das análises epistemológica, estatística e de opinião. Contou com o apoio de Alex Esteves Jaccoud Falcão, Fábio Oliveira Teixeira e Felipe Mancini. Este trabalho contou também com apoio de Adalberto Tardelli, BIREME. Foi realizado no período de 2006 a 2008.

O MeSH é um instrumento terminológico largamente utilizado, cujo domínio de estudo e atuação está delimitado às ciências da saúde. O MeSH é um cabeçalho de assunto especializado, desenvolvido, publicado e disponível online na internet pela U.S. National Library of Medicine (nlm.nih.gov), EUA, tendo como idioma principal o inglês. É atualizado dinamicamente por especialistas de várias áreas do conhecimento. No MeSH um descritor representa uma classe de conceitos, enquanto um conceito representa uma classe de sinônimos. A sua organização se dá em 19 categorias de assuntos (ncbi.nlm.nih.gov/mesh/1000048), sendo que cada uma se divide em subcategorias, nas quais os descritores subordinados são organizados hierarquicamente numa relação do mais genérico para o mais específico.

Os principais usos do MeSH são a indexação de artigos, a classificação de itens de informação e a pesquisa em bancos de dados de literatura científica em saúde, que tenham sido indexados pelo MeSH. A terminologia MeSH oferece um modo consistente para recuperar informação permitindo o uso de diferentes terminologias para os mesmos conceitos. Possivelmente a maior aplicação do MeSH reside na base de dados de literatura em saúde MEDLINE (NLM/NIH/NBCI, 2007), indexada pelo MeSH, que contém mais de 16 milhões de registros indexados com taxa de crescimento de 500.000 artigos/ano, cobrindo aproximadamente 4.600 revistas biomédicas internacionais.

Estatística de termos de artigos PubMed

O processo como um todo se iniciou com um estudo estatístico, cujo objetivo foi analisar o corpus composto de metadados de 437.289 artigos científicos provenientes da literatura científico-tecnológica em informática em saúde, extraídos da base PubMed. Utilizando técnicas de mineração de textos e o software PreText (Matsubara, 2005) foram extraídos os n-gramas dos resumos dos artigos. Após os estudos terminológico e epistemológico, os metadados dos artigos foram utilizados para o cálculo de estatísticas relativas à epistemologia da informática em saúde.

Em seguida, o estudo terminológico envolveu a modelagem dos dados e a transformação do cabeçalho de assunto MeSH em tesauro. A extração de conceitos a partir da literatura científico-tecnológica associada aos termos MeSH relativos à informática em saúde formaram as bases para o desenvolvimento do tesauro EpistemIS. A criação de n-gramas dos termos do tesauro EpistemIS, usando algoritmo stemming de Porter (2006), possibilitou o relacionamento entre termos do corpus e termos EpistemIS.

Por fim, o estudo epistemológico se iniciou na revisão de literatura em epistemologia para caracterização e distinção entre os metaconceitos da ação e pensamento humanos (MAPHs), que são arte, técnica, ciência, tecnologia e tecnociência. O estudo continuou com a apresentação do referencial teórico-metodológico, baseado nas obras de Mário Bunge (Bunge 1969, 1980, 1987). A partir deste referencial foi criado um método para classificação epistemológica dos termos EpistemIS. O estudo foi finalizado com a revisão de literatura em informática em saúde para apresentação de um estudo teórico e epistemológico da área, que contribuiu com a sistematização do conhecimento (mapa de conhecimento) da informática em saúde e com a classificação de suas subáreas em MAPHs.

Por meio deste estudo foi possível inferir as principais áreas que compõem a informática em saúde. Fundamentalmente a área abrange dois tipos de conhecimento:

- a base específica, formada por conhecimento obtido de outras áreas:
  - ciências comportamentais;

  - ciências naturais;
  - ciências biológicas;
  - ciências da informação.
- o corpo de conhecimento, formado por conhecimento obtido na própria área:
  - informática biomédica, que é aplicada tanto às ciências da saúde quanto às ciências da vida ou ciências biológicas;
  - informática médica aplicada à medicina;
  - informática em enfermagem aplicada à enfermagem;
  - informática odontológica aplicada à odontologia;
  - informática aplicada a todas as outras ciências da saúde não especificadas.

Tesauro EpistemIS

O tesauro EpistemIS (Colepícolo, 2008; telemedicina6.unifesp.br/epistemis) construído contém 730 termos, sendo 110 provenientes do MeSH e 620 obtidos da literatura científico-tecnológica em informática em saúde. Os termos contidos (Tabela 1) fazem parte, em sua maioria, da área de ciências da informação (76%), seguido por ciências biológicas (8%) e ciências comportamentais (8%), havendo uma pequena minoria da área de ciências humanas (2%). A pequena porcentagem de termos na área de cuidado em saúde (categoria N) se justifica por ser uma área MeSH que abrange os seus aspectos organizacionais, educacionais e econômicos, enquanto aspectos relativos à prática do cuidado em saúde estão alocados em ciências biológicas. Em relação aos MAPHs, os termos do tesauro EpistemIS obteve uma distribuição equitativa entre tecnociência (35%), tecnologia (28%) e ciência (31%). Também consideramos lógico que seja mínima a quantidade de termos classificados como arte (6%), já que há um esforço da informática em saúde em comportar-se como ciência e tecnologia, afastando-se da subjetividade, sendo o mais objetiva possível.

Classe	Área	Categ MeSH	Qtd termos	% termos
12	Information Science	Information Science [L]	563	76%
07	Biological Sciences	Biological Sciences [G]	58	8%
08	Natural Sciences	Natural Sciences [H]	58	8%
06	Behavioral Sciences	Psychiatry and Psychology [F]	29	4%
14	Health Care	Health Care [N]	16	2%
09	Human Sciences	Anthropology, Education, Sociology and Social Phenomena [I]	13	2%
TOTAL			737	100%

Tabela 1 – Tesauro EpistemIS. Distribuição de termos nas áreas de conhecimento e categoria MeSH (Colepicolo, 2008).

Publicações no PubMed

De um total de 437.289 artigos analisados, somente 231.416 (53%) estavam relacionados aos MAPHs. Entre estes, apenas 5.200 (2%) têm relação com o tesauro EpistemIS. Identificamos os autores individuais que mais publicaram artigos que contêm n-gramas do tesauro EpistemIS, ou seja, os mais representativos em informática em saúde. Esta contagem foi realizada por autor individual com repetição na base indexada. Foi possível observar que o aspecto científico dos registros de artigos publicados pelos autores individuais é dominante (2.292.569), seguido pelo tecnológico (430.906) e tecnocientífico (218.008), com uma pequena quantidade de artigos sobre o aspecto artístico (110.543).

Ao analisar o top 20 do ranking gerado dos autores que mais publicam em informática em saúde, incluindo origem, vínculo institucional e perfil desses autores, foi possível observar as áreas de atuação e inferir interesse e motivos que os levam a publicar em informática em saúde. Observamos que a maioria destes autores, em 2008, atuava no Channing Laboratory, que é uma divisão de pesquisa multidisciplinar do Brigham and Women's Hospital e da Harvard Medical School (brighamandwomens.org). As áreas principais de pesquisa desta instituição, na época, eram bacteriologia, epidemiologia de doenças crônicas e virologia. A integração de uma das mais notórias universidades do mundo com uma instituição de cuidado em saúde no desenvolvimento de pesquisas científicas e tecnológicas para aplicação na saúde denota mais uma vez o caráter tecnocientífico da informática em saúde. O autor Walter C. Willett, o primeiro do ranking, um importante cientista e docente do Departamento de Nutrição da Harvard School of Public Health nas áreas de nutrição e epidemiologia também atuava no Channing

Laboratory, sendo apontado inclusive como um dos autores mais citados do ISI (Thomson ISI 2002), na época, com mais de 600 artigos publicados, sendo mais de 400 destes indexados na base PubMed. Outros autores do ranking, tais como Graham A. Colditz, Meir J. Stampfer, Susan E. Hankinson, Frank B. Hu, Eric B. Rimm, Nader Rifai e David J. Hunter têm perfil semelhante ao de Willet como membros de alguma divisão da Harvard School. O autor Lex M Bouter atuava no EMGO Institute for Health and Care Research (EMGO+) (emgo.nl), um instituto de pesquisa da VU University Medical Center Amsterdam, especializado em atenção primária e saúde pública, com ênfase em doenças crônicas. Ronald Klein integra o Department of Ophthalmology and Visual Sciences da University of Wisconsin-Madison, EUA (ophth.wisc.edu) e desenvolve pesquisas relacionadas à epidemiologia em doenças oftálmicas, tais como catarata e retinopatia por diabete.

Observando o ranking das 20 instituições que mais publicam como autor coletivo temos que a maioria é de grupos de pesquisa ou de trabalho das áreas de controle e prevenção de doenças (1.519), ciências da saúde e farmacêuticas em geral (241), oncologia (107), cardiologia (103), saúde materno-infantil (100), cuidado em saúde (93). O Centro de Controle e Prevenção de Doenças (CDC), EUA, publicou mais artigos em ciência (1.099), mas também em tecnociência (125), tecnologia (107) e em arte (46).

Quanto aos periódicos, a maioria dos registros relacionados à informática em saúde privilegia artigos científicos (407.231; 76%), e com muito menos ênfase também publicam artigos tecnológicos (71.360; 13%), tecnocientíficos (38.758; 7%) e artísticos (19.004; 4%). O ranking geral nos permite observar que o periódico que mais publicava artigos relativos à informática em saúde, na época, é o The Journal of Biological Chemistry (jbc.org), especializado em bioquímica, seguido por uma série de periódicos especializados em radiologia, microbiologia, neurociências, controle e prevenção de doenças e genética. É marcante a presença de periódicos de especialidades médicas tais como oncologia, pediatria, endocrinologia, cardiologia e gastroenterologia publicando artigos classificados como informática em saúde. Entre os periódicos especializados temos o Bioinformatics (Oxford, England) e o BMC Bioinformatics, ambos com foco em bioinformática, que constaram como mais representativos do corpo de conhecimento da informática em saúde no ranking gerado.

A Figura 1 apresenta dados parciais das publicações da área de informática em saúde, mostrando um incremento na publicação de artigos classificados como científicos por meio do EpistemIS. Em 1999, os Proceedings do AMIA Annual Symposium eram os mais representativos (590) com publicações relativas ao aspecto científico da informática em saúde. Porém, de maneira geral, a maioria dos artigos publicados neste ano é relativa à pesquisa em informática em saúde para especialidades médicas (2.732), tais como oncologia, cardiologia, endocrinologia e pneumologia. Outros temas importantes já em 1999 são bioquímica (911), neurociências (605), epidemiologia (552), microbiologia (351), medicina nuclear (284) e radiologia (260). Nos anos de 2003 e 2004 mantêm a 1ª e 2ª posições do ranking os periódicos The Journal of Biological Chemistry e Pediatrics, respectivamente. Também ocorre um crescimento de publicações especializadas em informática em saúde em 2003 devido ao AMIA Annual Symposium (921) e ao Bioinformatics (Oxford, England) (968), que expandiu sua produção científica em 2004 (1.310), chegando ao seu ápice em 2005 com 2.301 artigos em ciência. Até então foi o periódico mais representativo em informática em saúde, no período estudado.

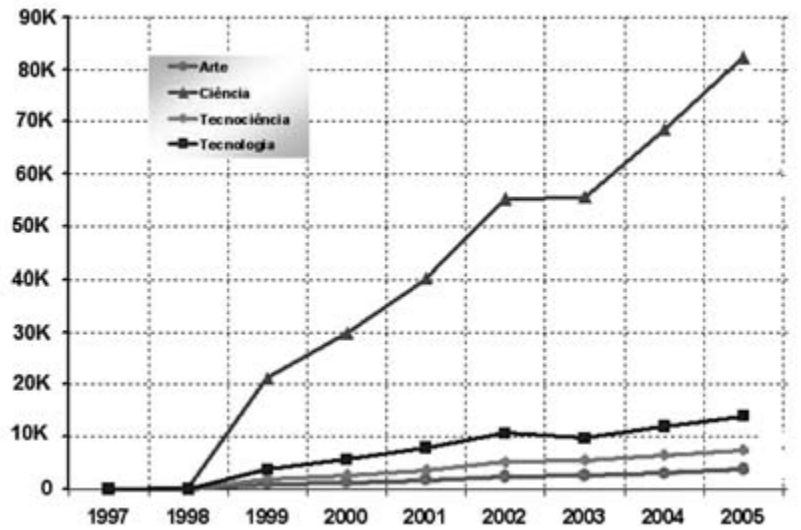


Figura 1 – Contagem de artigos PubMed da área de informática em saúde publicados no período 1998-2005 de acordo com classificação EpistemIS (Colepícolo, 2008).

A partir dos resultados obtidos foi possível observar que a evolução da literatura em informática em saúde privilegia o seu aspecto científico, ainda que a origem do conhecimento científico da área seja proveniente de outras ciências e que a aplicação desses conhecimentos também se destina a outras áreas. A produção científica da informática em saúde esteve voltada, para o período analisado, para 6 áreas principais: bioquímica, microbiologia, especialidades médicas, radiologia, genética e, mais recentemente, saúde pública. A tendência para a aplicação da informática às ciências biológicas vem crescendo nos últimos anos, levando a uma consolidação da bioinformática, sem, no entanto, afastar-se das ciências da saúde e especialidades médicas.

Pesquisa de opinião

Uma pesquisa de opinião (Colepícolo, 2008) com 32 especialistas da área apontou que mais da metade considera a informática em saúde derivada tanto da informática (58%) quanto das ciências da saúde (63%). Apenas 50% consideram a informática em saúde uma tecnologia, enquanto 75% a consideram uma ciência e 83% observam uma integração entre ciência e tecnologia, ou seja, uma tecnociência, o que vai ao encontro aos resultados do estudo epistemológico. Ainda, quanto à atuação em informática em saúde, 83% consideram-se pesquisadores, 65% consideram-se desenvolvedores, enquanto 55% são educadores, havendo sobreposição de papéis, o que reflete mais uma vez o caráter tecnocientífico da área.

Em relação à nomenclatura da área, poucos (10%) entendem informática em saúde como sinônimo de informática médica ou de telemedicina/telessaúde (15%). Um dos respondentes afirma, tal como observamos no estudo epistemológico, que a informática em saúde (health informatics) é o termo mais inclusivo, mas o termo informática biomédica (biomedical informatics) vem ganhando atenção; a telessaúde é mais ampla que a telemedicina e ambas fazem parte da informática em saúde. Alguns respondentes apontaram outros sinônimos para a informática em saúde, tais como bioinformática, ciência da computação aplicada a saúde, biotecnologia, e-Saúde, informática no cuidado em saúde (healthcare

informatics), informática biomédica (biomedical informatics) ou informática em biomedicina, e tecnologia de informação em saúde.

Foi solicitado aos respondentes que definissem a informática em saúde com suas próprias palavras e foi interessante observar que boa parte deles se refere à informática em saúde como uma aplicação (32,5%) ou uso de ferramentas da informática (17,5%), ou de recursos da computação (15%) à área da saúde (22,5%) ou aos serviços em saúde (15%), o que poderia denotá-la como uma tecnologia (5%). Entretanto, 22,5% dos respondentes definem a informática em saúde como uma ciência baseada na ciência da computação (10%) que lida com a pesquisa e desenvolvimento em medicina (10%). Alguns citaram ainda a relação da informática em saúde com a educação e pesquisa em saúde (7,5%). Poucos respondentes (2,5%) citaram aspectos da área relacionados à promoção da saúde, à prática médica e ao auxílio aos profissionais em saúde para melhorar sua eficiência, eficácia e produtividade, contribuindo com a redução de custos.

A maioria das definições pareceu tratar a informática em saúde como integração entre ciência e tecnologia, ou seja, tecnociência, valendo-se de pesquisa, desenvolvimento, aplicações, ferramentas e recursos da informática e ciência da computação para auxílio à pesquisa, desenvolvimento e prática das ciências da saúde.

Tecnociência Interdisciplinar

A partir de estudo comparativo entre aspectos teóricos e práticos, considerando como etapas os estudos estatístico, terminológico e epistemológico, concluímos que a área da informática em saúde é uma tecnociência interdisciplinar que se ocupa da solução de problemas de um amplo leque de domínios e fatos das ciências da vida, das ciências da saúde e da prática do cuidado em saúde, por meio da pesquisa científica proveniente de outras áreas do conhecimento e do desenvolvimento de suas próprias tecnologias para uso na sociedade (Colepicolo 2008).

Vale destacar que há 20 anos Greenes e Shortliffe (1990) já defendiam argumentos de que a informática médica seria tanto ciência quanto tecnologia, lidando com uma série de atividades, como pesquisa básica,

pesquisa aplicada, engenharia, desenvolvimento e planejamento. Yuval Shahar defendeu que a informática médica é mais íntima da engenharia, enquanto Van Bemmel apoiou que era uma ciência (Maojo et al., 2002). Maas et al. (2001) afirmavam em 2001 que a informática médica não poderia ser considerada só como uma extensão da informática aplicada às ciências da saúde, sem comprometimento com seu avanço científico. Também não poderia ser vista apenas como forma de solucionar problemas tecnológicos do cuidado à saúde e tornar o trabalho dos profissionais em saúde mais efetivo. Ele considerava que a criação, desenvolvimento e aperfeiçoamento de métodos e técnicas da informática médica havia se tornado premente, como ocorre em qualquer disciplina jovem, e que a aceitação deste fato deveria conduzir ao reconhecimento de informática médica como um campo de estudo por seu próprio direito. Mais que isso, que a pesquisa em informática médica deve contribuir com os avanços tecnológicos do cuidado em saúde, mas o foco está muito mais no longo que no curto prazo. No ano seguinte, Georgiou (2002) definiu a informática médica como a disciplina que integra ciências biomédicas, informática e políticas de administração e organização das ciências da saúde. Disse ainda que, assim como a medicina, a informática é essencialmente heterogênea e não pode escapar de estudos metodológicos e epistemológicos que envolvam a prática da medicina. Nota-se nos dizeres de Maas et al. e Georgiou uma preocupação em estabelecer princípios e fundamentos científicos para a consolidação da informática em saúde.

Diferentes Nomenclaturas para Informática em Saúde

A nomenclatura utilizada para definir uma área do conhecimento pode nos dizer muito a respeito da sua abrangência. No caso da informática médica, não há ainda um nome consolidado mundialmente para designar a área. Uma compreensão da evolução da área pode nos fornecer algumas pistas da melhor nomenclatura para a área, de acordo com sua abrangência. Shortliffe & Cimino (2006) apresentam um interessante estudo evolutivo dos termos utilizados para denominar a área de informática médica, que norteou a elaboração desta seção.

Desde os anos 1960, quando se inicia a informática em saúde - denominação utilizada neste trabalho –, as pessoas têm dúvidas em relação ao nome que devem dar a conceitos de informática aplicada às ciências da saúde e ciências da vida. O próprio termo ciência da computação era novo nos anos 1960 e tinha uma definição vaga. O termo ciência da computação médica (medical computer science) se refere à subdivisão da ciência da computação que aplica seus métodos à medicina. O termo computação médica (medical computing) inclui tópicos de estatística médica, manutenção de registros e estudo da natureza da informação médica (Shortliffe; Cimino, 2006). O termo originalmente introduzido na Europa para a área como um todo foi informática médica (medical informatics), que tira a ênfase do computador, enfatizando o campo no qual a computação é aplicada, ou seja, a medicina. O termo ciências da informação médica (medical information science) tem sido bastante usado nos EUA, mas pode ser confundido com a biblioteconomia (library science) e não diz respeito à abrangência total da área. Além disso, o termo informática (informatics) foi bem aceito nos EUA a partir dos anos 1990, tendo como consequência a ampla aceitação do termo informática médica (medical informatics) a partir do ano 2000, embora algumas pessoas repelem o seu uso, por considerarem como um neologismo ambíguo (Shortliffe; Cimino, 2006). Na última década em regiões do mundo como a Ásia, Europa e EUA tornou-se mais comum o uso do termo informática médica (medical informatics), porque o adjetivo medical é utilizado em sentido tão amplo quanto health (Sigulem, 1997).

Informática médica (medical informatics) também é o nome do campo usado por Shortliffe e Cimino (2006) nas duas primeiras edições do seu livro didático Biomedical Informatics: Computer Applications in Health Care. O nome do livro foi mudado de informática médica (medical informatics), na 1ª e 2ª edições, para informática biomédica (biomedical informatics), na 3ª e atual edição por duas razões: devido à expansão da aplicação da informática não só nas ciências da saúde, mas também para as ciências biológicas, e devido ao uso do novo termo em unidades acadêmicas, sociedades, programas de pesquisa e publicações da área.

Porém, desde a ascensão do termo bioinformática (bioinformatics), muitos observadores expressaram preocupação com o adjetivo médico, focado em médicos e desconsiderando a relevância desta disciplina para outros profissionais em saúde e em ciências da vida (Shortliffe; Cimino, 2006). Assim, o termo informática em saúde (health informatics) ganhou mais popularidade, embora com a tendência de excluir aplicações em biologia.

No Brasil, por exemplo, utiliza-se mais o termo informática em saúde (health informatics) devido à abrangência da área que não lida apenas com a medicina, mas também com a enfermagem, a nutrição, a veterinária e odontologia, entre outras, que são consideradas pelo Ministério da Educação como ciências da saúde. A Sociedade Brasileira de Informática em Saúde (SBIS) (sbis.org.br) utiliza o termo mais amplo saúde ao invés de médica.

Apesar da prevalência do termo informática médica (medical informatics), nos anos 1990 surgiram iniciativas que agregavam a aplicação da informática nas ciências da saúde e nas ciências da vida, o que abriu espaço para o uso da expressão informática biomédica (biomedical informatics). Em 1999, no National Institutes of Health (NIH) (nih.gov), EUA, foram criados dois grupos de trabalho, o de computação biomédica e o de bioinformática, que deram maior visibilidade e expansão às aplicações da informática em biologia. Desde então, o termo informática biomédica (biomedical informatics) tem sido largamente aceito e pode ser entendido como o campo que abrange todas as áreas subjacentes à aplicação em saúde, prática clínica e pesquisa biomédica. Para se referir ao uso de computadores nas atividades de informática biomédica, usa-se para tópicos metodológicos o termo ciência da computação biomédica (biomedical computer science) e para descrever a atividade em si, o termo computação biomédica (biomedical computing). Entretanto, a informática biomédica, que abrange as duas áreas anteriores, tem outros componentes além da ciência da computação, que são as ciências da decisão, estatística, ciências cognitivas, ciências da informação e ciências da administração.

Apesar de suas considerações, a obra de Shortliffe & Cimino (2006) faz parte da série que contém pelo menos mais 12 volumes dedicados à

informática em saúde (health informatics) sob vários aspectos, inclusive, informática odontológica e informática em enfermagem. A série começou em 1988 com o nome Computers in Health Care, mas em 1998 teve o nome alterado para Health Informatics Series, o que parece indicar que existe não só uma distinção entre a informática em saúde e a informática biomédica, mas também uma subordinação da informática biomédica à informática em saúde.

Também existe alguma confusão entre a informática em saúde e a e-Saúde ou saúde eletrônica (e-Health ou electronic health) (Eysenbach, 2001). Pouco utilizado antes das 1999, o termo e-Saúde vem sendo largamente utilizado para caracterizar tudo que está virtualmente relacionado a computadores e medicina. O termo aparentemente começou a ser usado por líderes de indústria e comércio e não por acadêmicos. Eles criaram e usaram este termo em analogia a outras e-palavras, tais como e-comércio (e-commerce) e e-negócio (e-business), numa tentativa de levar as promessas, princípios e o entusiasmo do comércio eletrônico para a área de saúde, e dar conta das novas possibilidades que a internet está abrindo à área de cuidado médico. Como a internet criou novas oportunidades e desafios à indústria de informática em saúde tradicional, o uso de um termo novo para tratar estes assuntos parecia apropriado. Estes desafios ditos novos para a indústria de informática em saúde eram principalmente: a capacidade de consumidores interagirem com seus sistemas comerciais on-line (B2C); melhoria das possibilidades de transmissões de dados de instituição para instituição (B2B); novas possibilidades para comunicação entre consumidores (C2C).

A e-Saúde (e-Health) surgiu em substituição à telemedicina. A Declaração de Tel-aviv (WMA, 2006) oferece uma série de princípios e recomendações éticas para o uso da telemedicina pela classe médica. Neste documento, a telemedicina é definida como o exercício da medicina à distância, cujas intervenções, diagnósticos, decisões de tratamentos e recomendações estão baseadas em dados, documentos e outras informações transmitidas por sistemas de telecomunicação. Considerando uma ampla disponibilidade de sistemas de informação médicos que podem interconectar e comunicar, o termo e-Saúde po-

deria substituir o termo telemedicina apenas como um nome de moda para algo que já existia, mas que com outro termo, antigo, era difícil de se evidenciar. Em dezembro de 1999, o subtítulo do Telemedicine Today (telemedtoday.com), um periódico sem revisão por pares, mudou de Where Healthcare + Telecommunications Converge para e-Health Newsmagazine, e alguns meses depois, o Telemedicine Journal, um periódico científico revisado por pares, adicionou um e-Health ao seu título (liebertpub.com/TMJ). Apesar disso, quando pesquisadores escrevem seus trabalhos não utilizam e-Saúde, mas os termos clássicos telemedicina e informática médica.

A despeito disto, muitos continuam pesquisando, utilizando e tentando definir o conceito de e-Saúde. A definição de e-Saúde feita por Mitchell (1999) parece abrangente: um termo novo, necessário para descrever o uso combinado de comunicação eletrônica e informática no setor da saúde, ou seja, a transmissão, armazenamento, recuperação e uso de dados digitais no setor saúde para propósitos clínicos, educacionais e administrativos, tanto localmente quanto a distância. Pode-se considerar o equivalente de e-comércio para a indústria de saúde.

Para Eysenbach (2001), definir e-Saúde é como definir a internet: só pode ser definido em um momento específico, a definição não pode ser fixa, já que se trata de um ambiente dinâmico, em constante movimento. Assim, e-Saúde é considerada por ele como um campo emergente na interseção da informática em saúde, saúde pública e negócios, referindo-se à melhoria dos serviços em saúde e da distribuição de informação pela internet e tecnologias relacionadas. Em um sentido mais amplo, o termo caracteriza não só um desenvolvimento técnico, mas também um paradigma, um modo de pensar, uma atitude e um compromisso para transmissão em rede, pensamento global, melhoria da saúde local, regional e global, usando tecnologias de informação e comunicação. Para Ivanitskaya et al. (2006), a e-Saúde vem causando um impacto cultural crescente tanto na pesquisa quanto nas profissões de saúde, afetando a relação entre profissional da saúde e paciente e abrindo possibilidades de novos papéis profissionais na prestação de serviços em saúde. O uso crescente da internet chama a atenção de cientistas para a modelagem do comportamento individu-

al como contribuição ao desenvolvimento e refinamento de teorias e modelos de saúde.

Um estudo extenso sobre definições de e-Saúde foi realizado por Oh et al. (2005), no qual apresenta 51 definições distintas do termo, as quais foram analisadas qualitativamente. A análise mostra que o termo e-Saúde apresenta conceitos diversificados, envolvendo áreas como saúde, tecnologia e comércio e que o termo, apesar das definições imprecisas, é bem compreendido pela comunidade que faz uso dele. Contudo, Oh et al. (2005) não apresentam uma compilação das definições do termo.

Informática em Saúde como Melhor Nomenclatura

Em nossos estudos foi possível compilar o conceito de e-Saúde definindo-o como um campo emergente na interseção da informática em saúde, saúde pública e negócios, que representa o uso combinado de informática e da comunicação eletrônica no setor da saúde, ou seja, a transmissão, armazenamento, recuperação e uso de dados digitais para propósitos clínicos, educacionais e administrativos, tanto localmente quanto à distância. A e-Saúde representa um esforço empreendido por líderes em saúde e indústrias de alta tecnologia, visando o máximo aproveitamento dos benefícios disponíveis pela convergência da internet com a saúde, assim como a melhoria da saúde local, regional e global, por meio de tecnologias de informação e comunicação.

O termo e-Saúde parece ser mais amplo que telemedicina porque não se restringe a interação médico-paciente. A telemedicina parece ser um dos temas da e-Saúde, mesmo porque o termo medicina é mais específico do que saúde, mais adequado para designar uma série de ações envolvidas no cuidado em saúde que vão além do âmbito da medicina. Já o termo telessaúde (telehealth) por vezes é utilizado como sinônimo de telemedicina, o que parece mais adequado para representar o cuidado em saúde por meio de redes de comunicação como a internet. O prefixo tele significa à distância, assim telessaúde seria adequado para o cuidado

em saúde à distância, assim como telemedicina bem traduz o cuidado médico à distância. Nenhum dos dois termos, entretanto, representaria bem o uso da informática em ciências da saúde e da vida, porque não necessariamente esta integração é feita para uso à distância. Assim, parece mais coerente considerar que a telemedicina e telessaúde tratem apenas de um dos aspectos da e-Saúde.

Portanto, o termo e-Saúde parece inviável para representar a interdisciplinaridade da informática com as ciências da saúde e da vida, dada a sua abrangência que ultrapassa os limites de uma área científica e tecnológica. A e-Saúde envolve muito mais aspectos mercadológicos do uso da informática na saúde e do consumo de produtos e serviços em saúde, tendo, muitas vezes, mas nem sempre, como pano de fundo a informática médica e a telemedicina. É como confundir o comércio com as ciências econômicas ou confundir o uso de redes de telecomunicação com a engenharia de telecomunicações. O MeSH classifica telemedicina (telemedicine) como uma subárea da medicina que emprega a tecnologia de redes de comunicação na relação médico-paciente à distância.

A e-Saúde pode ser compreendida como uma das subáreas da informática médica, atrelada às redes de informação e comunicação (networking) em saúde, que contém a telessaúde, a qual representa o cuidado em saúde à distância. O termo e-Saúde pode até vir a substituir os termos informática médica, informática em saúde e informática biomédica em algum momento futuro, devido à abrangência do conceito e sua facilidade mnemônica. No momento, pode ser considerada como parte da informática médica e até caracterizada como uma tecnociência, somente quando de fato emprega métodos e técnicas provenientes da ciência e tecnologia na saúde, no âmbito da sociedade, o que nem sempre ocorre.

De outro lado, o termo informática biomédica (biomedical informatics) parece considerar somente o desenvolvimento e aplicação da informática (informatics) em ciências biológicas (bio) e em medicina (medicine), excluindo outras ciências da saúde a qual a área se aplica. O termo informática médica (medical informatics) parece considerar

somente o desenvolvimento e aplicação da informática (informatics) em medicina (medicine), excluindo outras ciências da saúde e as ciências biológicas. O termo informática em saúde (health informatics) parece considerar somente o desenvolvimento e aplicação da informática (informatics) nas ciências da saúde, ficando de fora as ciências biológicas. Nenhum dos termos parece representar integralmente o conceito de desenvolvimento e aplicação da informática nas ciências da saúde e da vida.

Portanto, o termo informática em saúde (health informatics) parece ser o mais apropriado, entre as denominações citadas, por três razões: 1) por ser um termo já utilizado pela comunidade científico-tecnológica no mundo inteiro até então, ainda que em menor escala; 2) por abranger todas as ciências da saúde e não só a medicina; 3) parece continuar sendo mais representativo na literatura científico-tecnológica disponível nos mecanismos de busca do que o termo informática biomédica.

Mesmo não havendo intenção em definir uma nova nomenclatura para a área, em nosso estudo epistemológico foi possível constatar os valores de uma comunidade científico-tecnológica em relação ao seu próprio campo de pesquisa. Um neologismo foi explicitado (Colepícolo, 2008) como um termo capaz de abranger toda a gama de conhecimento da área. A informática em biossaúde (biohealth informatics) seria a pesquisa (ciência), desenvolvimento (tecnologia) e aplicação (tecnociência) da informática e suas subáreas às ciências da saúde e às ciências biológicas (da vida).

Nomenclaturas na Web

A título de curiosidade vale a pena observar o número total (aproximado) de ocorrências na web das nomenclaturas mais comuns utilizadas para representar a área da informática em saúde a partir de alguns mecanismos populares de indexação de conteúdo, apresentado no Quadro 1.

Nomenclaturas***	Google	Google Acadêmico	Bing	PubMed	ACM	Wikipedia	YouTube
e-Health	177.000K	52K	2.700K	17K	1K	Sim	14K
Biomedical Informatics	77.000K	40K	464K	3K	5K	Sim*	1K
Health Informatics	22.900K	50K	1.490K	3K	3K	Sim	5K
Medical Informatics	21.700K	356K	1.360K	16K	8K	Sim*	2K
Informática Biomédica	2.630K	1K	60K	0,027K	0,007K	Sim	0,816K
Informática Médica	2.300K	8K	261K	0,067K	0,018K	Sim	2K
Informática em Saúde	684K	3K	49K	0,017K	0,013K	Não	0,238K
e-Saúde	93K	0,168K	10.300K	0	0	Não	0,020K
BioHealth Informatics	22K	0,5K	6K	0,004K	0,005K	Não	0
Informática em Biossaúde**	0,005K	0,001K	0,002K	0,043K	0	Não	0

Dados obtidos em 28 de setembro de 2013.
* Pela nomenclatura Health Informatics ** Utilizado com a escrita informática em biossaúde
*** Quando possível foi realizada busca exata do termo, sem permitir variações.
Quadro 1 - Número aproximado de ocorrências na web das principais nomenclaturas associadas à área da informática em saúde.

Subáreas da informática em saúde

A definição de subáreas da informática em saúde pode colaborar com uma melhor organização das pesquisas realizadas na área, contribuindo também para auxiliar a seleção de apresentações em eventos científicos de forma a enfatizar os métodos e técnicas. Desta forma, foram selecionadas algumas visões de subáreas que são utilizadas frequentemente nas atividades científicas em informática em saúde.

Na visão dos membros American Medical Informatics Association (AMIA) as subáreas a enfatizar são (AMIA, 2013): (1) bioinformáti-

ca translacional; (2) pesquisa clínica; (3) aplicações; (4) consumidor em saúde; (5) saúde pública.

A classificação em subáreas estabelecida pela International Medical Informatics Association (IMIA), para fins de organização dos estudos, considera as 5 subáreas utilizadas pela AMIA e adicionalmente 2 outras subáreas (IMIA 2013): (1) bioinformática translacional; (2) pesquisa clínica; (3) aplicações; (4) consumidor em saúde; (5) saúde pública; (6) informática em enfermagem; (7) informática para ambientes de recursos limitados.

A proposta de Shortiliffe (2006) consta de uma classificação em termos das aplicações em informática biomédica, a saber: (1) sistemas de registro eletrônico em saúde; (2) gerenciamento da informação em organizações de saúde; (3) consumidor em saúde e telessaúde; (4) saúde pública e infraestrutura em informação em saúde; (5) sistemas de cuidados com o paciente; (6) sistemas de monitoramento do paciente; (7) sistemas de imagem em radiologia; (8) recuperação da informação e bibliotecas digitais; (9) sistemas de apoio à decisão clínica; (10) computadores em educação médica; (11) bioinformática.

Outro exemplo de visão das subáreas da informática em saúde pode ser obtida a partir da lista utilizada pelo Congresso Brasileiro de Informática em Saúde (CBIS´2012) (sbis.org.br), que ofereceu, em 2012, palestras, minicursos e recebeu trabalhos a serem apresentados considerandos 19 temas/sub-áreas: (1) aplicações móveis em saúde; (2) avaliação de tecnologias de informação e comunicação em saúde; (3) educação e capacitação em informática em saúde; (4) gestão do conhecimento e mineração de dados; (5) informática em saúde e o paciente; (6) informática translacional; (7) modelos e padrões para representação de conhecimento, ontologias e terminologias; (8) organização, política, economia e gestão em saúde; (9) padrões de interoperabilidade entre sistemas; (10) políticas de informação e informática em saúde e aspectos éticos; (11) processamento e análise de sinais biológicos e imagens médicas; (12) projeto e arquitetura de sistemas de informação em saúde; (13) recuperação de informações e processamento de linguagem natural; (14) registro eletrônico de saúde / prontuário eletrônico do paciente; (15) segurança, privacidade e confidencialidade; (16) sistema de apoio à decisão e inteligência artifi-

cial; (17) tecnologias emergentes (TV digital, realidade virtual, computação ubíqua, redes virtuais); (18) telessaúde; e (19) usabilidade, interação e fatores humanos em sistemas de informação em saúde.

O Departamento de Informática em Saúde, da Escola Paulista de Medicina, UNIFESP, tem utilizado um quadro conceitual que considera 20 subáreas de interesse dentro da informática em saúde, para efeito de concursos, sendo: (1) princípios e história; (2) representação de conceitos: ontologias, vocabulários e terminologias; (3) padrões; (4) bioinformática; (5) processamento de sinais biológicos e imagens; (6) aplicações clínicas baseadas em imagens médicas; (7) sistemas de cuidado ao paciente; (8) registro eletrônico de saúde (RES); (9) sistemas de gerenciamento da informação em saúde; (10) sistemas para monitoração de pacientes; (11) sistemas de apoio à decisão clínica; (12) sistemas para armazenamento, processamento, transmissão e visualização de imagens médicas (PACS); (13) prontuário eletrônico do paciente (PEP); (14) segurança, privacidade e confidencialidade em sistemas de informação em saúde; (15) mineração de dados e textos em saúde; (16) telemedicina e telessaúde; (17) educação a distância em saúde; (18) internet e a saúde; (19) prática digital da saúde; e (20) sistemas de informação em saúde pública.

Na visão de Sigulem (1997) sobre uma prática médica digital, a visão descrita sobre as subáreas consta dos itens: (1) telemedicina; (2) informação digital; (3) educação; (4) comunicação; (5) registro eletrônico do paciente; (6) sistemas de apoio à decisão; (7) diretrizes médicas (guidelines).

Por fim, uma outra visão de subáreas da informática em saúde pode ser exemplificada a partir da lista construída junto ao grupo de pesquisa Saúde 360, UNIFESP (saude360.com.br), para identificação das atividades de pesquisa dos programas de graduação e pós-graduação disponíveis no país. Esta ação foi realizada com apoio da SBIS antes do CBIS'2010 e por algum tempo esteve disponível oficialmente na página web da sociedade. A lista criada foi utilizada neste projeto de identificação de escopo de programas de pós-graduação, a partir da análise de trabalhos publicados nos últimos eventos da SBIS. A partir da página web disponibilizada, coordenadores e orientadores de programas de pós-graduação foram convidados a ajudar na descrição de seus programas usando esta

lista de subáreas. A lista das subáreas da informática em saúde deste projeto, versão 2013, segue:

1. aplicações móveis em saúde, m-Saúde;
2. aquisição e armazenamento de dados em saúde;
3. armazenamento, processamento, transmissão e visualização de imagens médicas;
4. automação e robótica aplicadas à saúde;
5. avaliação de tecnologia de informação e comunicação em saúde;
6. bioengenharia;
7. bioinformática;
8. cientometria em saúde;
9. computação distribuída aplicada à saúde;
10. computação gráfica em saúde;
11. computação ubíqua e pervasiva aplicadas à saúde;
12. comunicação em saúde;
13. descoberta de conhecimento e mineração de dados em saúde;
14. econometria em tecnologia da informação e comunicação em saúde;
15. educação à distância em saúde;
16. educação e capacitação em informática em saúde;
17. educação em saúde mediada por computador;
18. equipamentos informatizados em saúde;
19. ética, legislação e políticas em informática em saúde;
20. fundamentos e epistemologia em informática em saúde;
21. história da informática em saúde;
22. informática em saúde pública;
23. informática para a gestão em saúde;
24. informática para a saúde do consumidor;
25. informática translacional;
26. inteligência artificial em saúde;
27. interação humano-computador para aplicações em saúde;
28. interoperabilidade e comunicação de sistemas em saúde;
29. métodos e técnicas informatizados de ensino em saúde;
30. metodologia e técnicas da informática em saúde;

31. modelagem e simulação computacional em saúde;
32. monitorização informatizada em saúde;
33. padrões em informática em saúde;
34. processamento e análise de sinais e imagens médicas;
35. prontuário eletrônico do paciente (PEP);
36. realidade virtual em saúde;
37. recuperação de informação em saúde;
38. redes avançadas e de alto desempenho para aplicações em saúde;
39. registro eletrônico em saúde (RES);
40. registro eletrônico pessoal em saúde;
41. representação de conhecimento, vocabulários, ontologias e terminologias em saúde;
42. saúde digital, e-Saúde;
43. segurança do paciente;
44. segurança, privacidade e confidencialidade em saúde;
45. sistemas colaborativos em saúde;
46. sistemas de apoio à decisão em saúde;
47. sistemas de informação em pesquisa clínica;
48. sistemas de informação em saúde;
49. sistemas de informação hospitalar;
50. software aplicado à saúde;
51. telemedicina;
52. telessaúde.

Considerações finais

Inicialmente nossos estudos sobre a área da informática em saúde concentraram-se apenas no esforço na compreensão das nomenclaturas que são utilizadas na literatura e em reuniões científicas. Há literatura disponível (Shortliffe; Cimino, 2006) que discute, em relação à tecnologia da informação e comunicação, os conceitos, aplicações, práticas, métodos e impactos na sociedade em geral, nos sistemas de saúde, na assistência diretamente e também para benefício individual do consumidor em saúde. No entanto, nosso interesse em conhecer o que se publicava na

área, como essas nomenclaturas se relacionavam e qual era a opinião de profissionais-chave no país expandiram nossos horizontes. Pela curiosidade científica continuamos a avançar em tais investigações para outros campos de representação da área da informática em saúde.

Do ponto de vista epistemológico foi possível constatar que a informática em saúde é, de fato, uma ciência aplicada interdisciplinar – denominada tecnociência –, a qual se ocupa da solução de problemas de um amplo leque de domínios e fatos das ciências da saúde e da vida e da prática do cuidado em saúde, por meio da pesquisa científica interdisciplinar e do desenvolvimento de tecnologias próprias para uso na sociedade (Colepícolo, 2008). A ciência contida na informática em saúde se mostrou proveniente de sua base interdisciplinar e o seu corpo de conhecimento é composto por objetos e fatos de domínio tecnológico. A sua problemática concentra-se na 61ª resolução de problemas das ciências da saúde e da vida, portanto, tecnocientífica. Seu aspecto de ciência/tecnologia aplicada tem fundamentação lógica e racional, e pauta-se em um conjunto de padrões, modelos, regras, normas e convenções que norteiam sua pesquisa e desenvolvimento. Há um grande esforço da área em consolidar-se como uma ciência independente; porém, é fortemente composta por conceitos interdisciplinares provenientes de outras ciências. O conjunto dos conceitos científicos da área que têm função na formação de suas teorias é pequeno, sendo a maioria de origem interdisciplinar. Seu aspecto artístico é mínimo e também interdisciplinar.

Os principais objetos do domínio da informática em saúde são a aquisição, transferência, armazenamento, processamento automático e análise de dados, informação e de conhecimento em ciências da saúde e da vida. Os problemas concentram-se no desenvolvimento de tecnologias e sistemas que contribuam com a gestão, aquisição, armazenamento, organização, recuperação e distribuição de dados, informação e conhecimento em saúde em qualquer suporte, seja texto, imagens, sons ou sinais, para o apoio à tomada de decisão na administração, educação e cuidado em saúde. Assim, a nomenclatura que melhor se adequa para a área, embora não utilizada, é o termo informática em biossaúde, que dá conta da aplicação da informática às ciências da vida ou biológicas e às ciências da saúde (Colepícolo, 2008).

Nossa investigação sobre os processos de classificação e indexação de artigos científicos na área de informática em saúde teve início a partir da análise realizada de 430 mil artigos disponibilizados no PubMed (Colepícolo, 2008). Foi possível avaliar a ligação de termos sendo usados por estes artigos em comparação com uma árvore padronizada de termos, EpistemIS, em contraste com a opinião de profissionais-chave. Nossa intenção, em continuar estes estudos, foi buscar expandir estes conhecimentos adquiridos no grupo de pesquisa para uma aplicação prática. Assim, decidimos focar na classificação e indexação de artigos científicos, por meio do Portal ISI Web of Knowledge, o que nos levou a conhecer um método automatizado utilizado pela *National Library of Medicina* (NLM), EUA, denominado Journal Descriptor Indexing (JDI). Estes aprendizados influenciaram a maneira como considerávamos, dentro do grupo de pesquisa, a aplicação de métodos quantitativos para classificação e indexação de conteúdos textuais. Neste caso, aplicamos com sucesso esta metodologia para realizar uma proposição de expansão na maneira como os artigos da nossa área são classificados e indexados no portal (Teixeira, 2011). Também conseguimos adaptar o mesmo método para classificação e indexação de conteúdos sobre saúde de páginas web usando 19 categorias padronizadas pela DMOZ *The Open Directory Project* (Sousa, 2011) e para análise de sentimento de opiniões relativas a temas de saúde publicados por consumidores em mídias sociais (Araujo, 2012).

Ao trabalhar com a opinião de profissionais-chave sobre nomenclaturas e conceitos da área da informática em saúde tivemos nossa curiosidade despertada para explicitar como estes profissionais se relacionavam. Ficou claro, a partir das respostas que tivemos, que os profissionais apresentam conceituação por agrupamentos a partir de suas formações e ligações. Mesmo a região e o tipo de instituição do profissional geravam diferenças de visão sobre a área. Naturalmente o tema rede social entrou em nossa agenda. Inicialmente como um exercício científico foi possível mapear a ligação do Prof. Dr. Daniel Sigulem, professor titular, com demais pesquisadores no país para uma homenagem a ele realizada no XIII Congresso Brasileiro de Informática em Saúde (CBIS'2008), em Campos de Jordão. Também foi possível calcular um nível de relacionamento entre os pesquisadores (orientadores de pós-graduação) da própria UNIFESP, na época.

A aplicação de técnicas e algoritmos da análise de rede social tomou conta do interesse de muitos pesquisadores a partir dos fenômenos populares de redes sociais eletrônicas. Após uma fase inicial de experimentações foi possível iniciar estudos formais que possibilitaram em 2012 uma descrição mais robusta da ligação entre os profissionais (Santo et al., 2012). Em 2013 refizemos as análises com dados atualizados e ampliação da rede social, o que nos possibilitou observar fenômenos de ligação entre as principais áreas que compõem a interdisciplinaridade da informática em saúde a partir da autodeclaração das pessoas em seus currículos da Plataforma Lattes CNPq. Estes resultados, que serão submetidos para publicação, identificam indivíduos e relacionamentos que podem colaborar com a construção de um sistema de recomendação acadêmica (Herlocker et al., 1999) na área da informática em saúde, que será nosso próximo passo de estudo.

Acreditamos que a área da informática em saúde se beneficia da aplicação de processos e técnicas da descoberta de conhecimento e mineração de dados para sua própria análise e evolução epistemológica. Os resultados de pesquisas qualitativas na área, o esforço de acadêmicos e profissionais em conduzir um progresso na área por meio de congressos e discussões científicas, e sistemas de avaliação dos órgãos de fomento podem se beneficiar com os resultados que a aplicação de mineração de dados e texto geram. A exposição de fenômenos epistemológicos, estatísticos e de rede social podem colaborar para definição dos rumos da área da informática em saúde no Brasil e, consequentemente, influenciar a evolução do uso das tecnologias de informação e comunicação na saúde.

Referências

AMERICAN MEDICAL INFORMATICS ASSOCIATION-AMIA. The science of informatics. Bethesda: AMIA, 2013. Disponível em: <http://www.amia.org/about-amia/science-informatics>. Acesso em: 20 out. 2013.

ARAUJO, G.D.; SOUSA, F.S.; TEIXEIRA, F. et al. Análise de sentimentos sobre temas de saúde em mídia social. **Journal of Health Informatics**, v. 4, n. 3, 2012.

BUNGE, M. **Ciência e desenvolvimento**. Belo Horizonte/São Paulo: Itatiaia/EDUSP; 1980.

_____. **Epistemologia**: curso de atualização, trad. Claudio Navarra. 2.ed.São Paulo: T.A.Queiroz; 1987.

_____. **La investigación científica**. Barcelona: Ariel; 1969.

COLEPÍCOLO, E.; MATSUBARA, E.T.; FALCÃO, A.E.J. et al. Uso da ferramenta PreText para mineração de textos extraídos do NCBI para estudo epistemológico da Informática em Saúde. **Revista de Informática Teórica e Aplicada**, v. 16, p. 9-24, 2009.

COLEPÍCOLO, E. **Epistemologia da Informática em Saúde: entre a teoria e a prática**. São Paulo. 2008. Dissertação [Mestrado em Informática em Saúde] – Universidade Federal de São Paulo, São Paulo, 2008.

EBECKEN, N.F.; LOPES, M.C.S.; COSTA, M..C.A. Mineração de textos. In: REZENDE, S.O. (Org.). **Sistemas inteligentes**. Barueri: Manole; 2003. p. 337-70.

EYSENBACH, G. What is e-health? **J Med Internet Res**., v.18, n.3(2), p.20, 2001.

GEORGIOU, A. Data, information and knowledge: the health informatics model and its role in evidence-based medicine. **J Eval Clin Pract.,** v.8, n.2, p.127-30, 2002.

GREENES, R.A.; SHORTLIFFE, E.H. Medical informatics. An emerging academic discipline and institutional priority. **JAMA,** v.263, n.8, p.1114–20, 1990.

HERLOCKER, J.L;KONSTAN, J.A.; BORCHERS, A. An algorithmic framework for collaborative filtering. In: ANNUAL INTERNATIONAL ACM SIGIR CONFERENCE ON RESEARCH AND DEVELOPMENT IN INFORMATION RETRIEVAL, 22., New York, 1999. **Proceedings**... New York, 1999.

INTERNATIONAL MEDICAL INFORMATICS ASSOCIATION-IMIA. MedInfo 2013. Last updated: 2012. Disponível em: <http://www.medinfo2013.dk/node/13>. Acesso em: 20 out. 2013.

IVANITSKAYA, L.; O'BOYLE, I.; CASEY, A.M. Health information literacy and competencies of information age students: results from the interactive online Research Readiness Self-Assessment (RRSA). **J Med Internet Res**., v.8, n.2, p.e6, 2006.

LANCASTER, F.W. **Vocabulary control for information retrieval**. Washington, D.C.: Information Resources Press; 1972.

MAAS, A.A.F.; HOOPEN, A.J.; HOFSTEDE, A.H.M. Progress with formalization in medical informatics? **J Am Med Inform Assoc**., v.8, n.2, p. 126–130, 2001. Disponível em: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=134552>. Acesso em: 29 out. 2007.

MAOJO, V.; MARTÍN, F.; CRESPO, J. Theory, abstraction and design in medical informatics. **Methods Inf Med.,** v.41, n.1, p.44-50**,** 2002.

MATSUBARA, E.T. PreText: an environment for pre-processing text for Text Mining. Disponível em: <http://www.icmc. usp.br/~edsontm/PreText/PreText.html>. Acesso em: 13 dez. 2006.

MITCHELL, J.G. **From Telehealth to E-health: the unstoppable rise of E-health** Canberra: Commonwealth Department of Communications, Information Technology and the Arts, 1999. Disponível em: < http://www.archive.dcita.gov.au/1999/09/rise#foreword>. Acesso em: 29 out. 2007.

NATIONAL LIBRARY OF MEDECINE-NLM. Medical Subject Headings: files available to download. Disponível em: <http://www.nlm.nih.gov/mesh/filelist.html>. Acesso em: 2 jun. 2006.

NLM/NIH/NBCI. PubMed: a service of the National Library of Medicine and the National Institutes of Health. Disponível em: <http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?db=PubMed>. Acesso em: 3 out. 2007.

OH, H.; RIZO, C.; ENKIN, M., et al. What Is e-Health (3): A Systematic Review of Published Definitions. **J Med Internet Res.,** v.7, n.1, 2005. Disponível em: <http://www.jmir.org/2005/1/e1/>. Acesso em: 27 out. 2013.

PARENT, F.; COPPIETERS, Y.; PARENT, M. Information technologies, health, and globalization: anyone excluded? **J Med Internet Res**., v.3, n.1, p.e11, 2001.

PORTER, M. The Porter Stemming Algorithm. Disponível em: <http://tartarus.org/~martin/PorterStemmer>. Acesso em: 21 out. 2007.

SANTO, C.C.; BONOME, K.S.; TEIXEIRA, F. et al. Rede Social de Currículos Lattes da Informática em Saúde Brasileira. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, 13., Curitiba,19-23 2012. Curitiba, 2012. p.1-2.

SHORTLIFFE, E.H.; CIMINO, J.J. **Biomedical Informatics:** computer applications in health care and biomedicine. London:Springer, 2006.

SHORTLIFFE, E.H. Medical informatics meets medical education. **JAMA,** v.273, n.13, p.1061, 1064-5,1995.

SIGULEM, D. **Um novo paradigma de aprendizado na prática médica da UNIFESP/EPM.** 1997. Tese (livre-docência) – Escola Paulista de Medicina, Universidade de São Paulo. São Paulo, 1997.

SOUSA, F.S. **Análise comparativa de métodos de recuperação de informação para categorização de conteúdos web relacionados à saúde**. 2011. Dissertação (Mestrado em Ciências – Gestão e Informática em Saúde) – Universidade de São Paulo. São Paulo, 2011.

TEIXEIRA, F.O. **Classificação e indexação de artigos científicos internacionais de informática em saúde**. 2011. Dissertação (Mestrado em Ciências - Gestão e Informática em Saúde) – Universidade Federal de São Paulo. São Paulo, 2011.

THOMSON ISI. ISI HighlyCited.com: Willett, Walter C. Last update: 2002 Nov 22. Disponível em: < http://goo.gl/rtixET>. Acesso em: 20 out. 2013.

VAN BEMMEL, J.H. (Ed.). **Handbook of Medical Informatics**. Rotterdam: Erasmus University, 1999. Disponível em: http://www.mieur.nl/mihandbook/r_3_3/ handbook/home.htm>. Acesso em: 20 out. 2013.

WORLD MEDICAL ASSEMBLY- WMA. Responsibilities and ethical guidelines in the practice of telemedicine. [Declaração de Telaviv]. Adopted by the 51st World Medical Assembly Tel Aviv, Israel, October 1999 and rescinded at the WMA General Assembly, Pilanesberg, South Africa, 2006. Disponível em: <http://www.wma.net/e/policy/a7.htm>. Acesso em: 16 out. 2013.

9

Sobre privacidade e anonimato na internet[1]

Pedro A. D. Rezende [2]

Introdução

O processo legislativo que culminou na promulgação do chamado Marco Civil da Internet (Lei 12.965, de 2014) ensejou várias discussões e debates públicos sobre o papel dos provedores de acesso à internet no teatro e no combate ao cibercrime. Diante da relevância atual do assunto, este artigo apresenta algumas considerações referentes a uma corrente de opinião que se manifestou nesse debate, frequentemente defendida em listas de discussões de cunho jurídico[3], que podemos chamar de anti-anonimista. Ao longo deste artigo, desenvolvemos algumas considerações sobre essas opiniões, com algumas reflexões gerais pertinentes ao contexto desta publicação.

Tal corrente presume, às vezes explicitamente, a existência de um "mito da incompatibilidade entre a privacidade, o anonimato e a responsabilização". O anonimato é incompatível com a responsabilização no âmbito jurídico, isto é fato. Mas também é fato que o âmbito jurídico não existe no vácuo; ele existe num espaço de valores sociais que muitas vezes

1 Adaptado de um artigo com mesmo título publicado no portal do autor (http://www.cic.unb.br/~rezende/trabs/anonimato.html)

2 Pedro A. D. Rezende (prezende@unb.br) é matemático e professor concursado no Departamento de Ciência da Computação da Universidade de Brasília (UnB).

3 Como expressa, por exemplo, no artigo disponível em: http://www.verbojuridico.com/doutrina/tecnologia/isp.pdf

conflitam entre si. Antes de se precipitar em justificativas ancoradas no primeiro fato, ou em mitos que dele germinam, para uma defesa moral ou política do fim do anonimato na esfera ou na era digital, convém melhor compreender a relação entre a eficácia histórica das normas jurídicas em exame, e as condições semiológicas inéditas do contexto ao qual se pretende estender esta eficácia.

Numa rede digital aberta, como a internet, a comunicação funciona por acordo tácito, através de adesão a protocolos digitais que se organizam – e se complementam – em camadas. Como por exemplo a camada de conexão para transmissão e recepção de sinal digital, operada por um provedor de acesso, e a camada de aplicação, operada por navegadores e servidores de conteúdo web. Uma escolha de protocolos que preenche todas as camadas necessárias para uma certa forma de comunicação é chamada, no jargão técnico das redes digitais, uma "pilha" de protocolos. Assim como no mundo da vida, o anonimato – e o pseudonimia *(*uso de pseudônimo*)* – numa rede digital aberta pode ser reversível, possibilidade esta que dependerá, via de regra, da participação de intermediadores que operam os meios, a lógica negocial e as tecnologias de informação e comunicação (TIC) envolvidas.

Numa rede digital aberta esta reversão dependerá, pelo ângulo técnico, da composição da pilha de protocolos aos quais os interlocutores aderem para se comunicar. Dependerá, mais precisamente, da execução de procedimentos ou da disponibilização de recursos da dita pilha – geralmente referidos como "dados de conexão" – acessíveis em princípio aos intermediadores da comunicação em foco. Quando um interlocutor busca, na esfera jurídica, reparar danos decorrentes de uma comunicação digital em rede aberta, componentes para a identificação dos interlocutores estará a depender da participação de intermediadores dessa comunicação, para reversão do anonimato (ou pseudoanonimato) do autor da ofensa.

Simplificação perigosa

Porém, esta possível reversão estará sempre sujeita aos limites cognitivos – isto é, à capacidade e ao interesse de conhecer – inerentes à

menor esfera social que seja comum aos participantes da comunicação em foco. Numa rede aberta, onde o alcance da comunicação é em tese ilimitado, esta esfera raramente é suficiente para a reversão completa do anonimato do autor da ofensa. Um endereço IP num registro de dados de conexão, por exemplo, pode identificar o uso de algum computador em algum contexto, mas não necessariamente a pessoa que deliberou, comandou ou controlou esse uso. O mesmo, para a chave privada que corresponde a um certificado digital de chave pública, usada para lavrar assinaturas digitais sobre documentos eletrônicos.

Doutro lado, a prática de *profiling*[4], cada vez mais comum entre intermediadores, pode identificar unicamente um interlocutor colhendo elementos do contexto digital onde se opera, e atribuir-lhe um pseudônimo, associado ou não a um ou mais nomes ou pseudônimos que esse suposto interlocutor atribui a si mesmo nessas e noutras interlocuções. Tal prática pode violar a privacidade deste indivíduo sem ferir seu anonimato, quando a prática for de fato eficaz para selecionar suas ações na internet, enquanto acumula elementos úteis à sua identificação positiva – por exemplo, a identidade civil do mesmo – mediante cruzamento com outras bases de dados.

Quando interessa ao intermediador, tal reversão do anonimato é potencializada e realizada em caráter privado, para conversão em ativo rentável (comércio de dados pessoais), mesmo em possível afronta a leis que buscam proteger a privacidade dos internautas. E quando não interessa, ela é burocratizada ou sabotada, imprecisa e custosa para o ofendido, pois tal capacidade de reversão, se admitida, poderia imputar ao intermediador responsabilidades jurídicas além do seu interesse.

Em sua defesa, a corrente antianonimista tende a se valer de questionáveis argumentos, via de regra reducionistas. O artigo citado na primeira nota de rodapé, por exemplo[1], afirma que "a Internet é caracterizada por ser um meio de comunicação onde não há intermediários", o que é uma miragem ou simplificação perigosa. Tal miragem decorre, a meu ver, da conjunção de dois fatores:

4 Ver http://en.wikipedia.org/wiki/Profiling_(information_science)

1. da possibilidade – quase sempre realizada – dos intermediadores necessários à comunicação digital em rede aberta se fazerem "invisíveis" (pense na operadora de telefonia celular, no provedor de conexão, no fornecedor do sistema operacional, etc.) ou transparentes (exceto quando mandam a fatura ou quando o serviço falha); e
2. do desconhecimento, por parte do usuário médio, de como as necessidades de intermediação precisam ser atendidas para que a comunicação digital aparentemente "direta" em rede aberta funcione a contento, e de como essas necessidades dispõem, para intermediadores, dados úteis à identificação de interlocutores, que pensam estar se comunicando anonimamente.

Embora o restante do citado artigo contenha análise competente e equilibrada, tal simplificação se torna – nele e em qualquer artigo que pretenda estabelecer doutrina jurídica antianonimista – perigosa por vários motivos. Tal simplificação ignora, oculta ou camufla o poder semiológico – conversível em poder econômico e político – que esses intermediadores já concentram na necessidade dessas intermediações. Poder tanto maior quanto mais a sociedade depende de comunicação digital em rede aberta, e tanto maior quanto mais o controle de suas intermediações se concentra em poucos negócios, em grandes empresas fornecedoras de tecnologias subjacentes, serviços de conexão ou de agregação ou classificação de conteúdo em escala global.

As revelações de Edward Snowden deixam evidentes a existência e a convergência de interesses que empoderam politicamente essas grandes empresas em alianças espúrias, camufladas ou não de legalismo, consentidas ou cooptadas, com os de Estados cuja pretensão hegemônica os impele a se armarem para as novas formas de conflito geopolítico na esfera digital. Tal simplificação sobre a natureza da internet traz a marca do ponto cego da ideologia neoliberal dominante, instalada na falácia dos mercados perfeitos. Repisada como senso comum, a miragem dessa simplificação se transforma em mito, que é perigoso como base para doutrina jurídica.

Anonimato e tecnologia

Trata-se de um mito perigoso, pois induz a sociedade a conceder, no plano normativo, a esses agentes intermediadores mais poderes do que eles já detêm, à guisa de lhes habilitar o exercício de funções técnicas necessárias à identificação positiva de quem pratique ofensas por meio digital, em troca de uma almejada eficácia jurídica perante a migração de atividades criminosas ao ciberespaço, mas desconsiderando as responsabilidades que tais agentes deveriam cumprir em virtude do poder semiológico já amealhado, e os limites práticos do Estado para coagir tal cumprimento.

Ou, o que é pior, quando essas desconsiderações se imbricam, porque tal imbricação induz a sociedade a condescender com o Estado, permitindo que este coopte agentes intermediadores para agirem também como mediadores do exercício de poderes até aqui ilegítimos para ambos, estratégia que rompe o equilíbrio normativo na divisão do poder político em democracias modernas.

Em defesa da doutrina antianonimista, num debate suscitado pelo artigo já citado[1], um debatedor[5] comenta:

> *"Não há prejuízo nenhum causado às iniciativas de extirpação do solo e exposição da raiz do sistema à luz (em outras palavras, as revoluções não armadas) pela vedação ao anonimato, eis que as mesmas sempre se valeram de tecnologias simples e do contato pessoal direto para atuarem; a vedação ao anonimato é um direito fundamental a ser defendido. As iniciativas anônimas, quando não são podres em seu objetivo, o são em seus meios, e todo o trabalho para neutralizá-las é digno. Quem tem algo a esconder não é obrigado a produzir prova contra si mesmo, e tem seus segredos constitucionalmente guardados pelo direito à privacidade; ...*

5 Aqui anonimizado em respeito ao seu direito à privacidade, e citado sob abrigo do inciso III, art. 46 da Lei 9.610/98

> *A defesa do anonimato no judiciário e no legislativo favorece única e exclusivamente quem detém os meios técnicos de invasão da privacidade no que diz respeito ao privilégio da informação. Um critério exclusivamente técnico acaba por prevalecer com a positivação de tal perversidade. E o império da técnica, assim como o império das armas, concentra o poder no indivíduo mais "habilidoso", ou mais "esperto", mas sempre o indivíduo. Para ilustrar melhor a similitude entre os dois tipos de critério de tomada de decisões, basta recordarmos que a maioria das tecnologias surgiu em função da guerra.*
>
> *Caso o anonimato venha a ser abraçado pelo ordenamento jurídico, os detentores de conhecimento avançado em informática poderão, sempre que quiserem, expressar-se anonimamente frente aos excluídos digitalmente, mas o contrário jamais. Defender o anonimato é defender um critério técnico, em detrimento de um critério humano, de inclusão, de integração; para selecionar quem participa e quem não participa efetivamente nas tomadas de decisão sobre o curso da sociedade, quem tem voz ativa e quem não tem; não há nada de revolucionário nisso. "*

Essa pungente defesa da tese antianonimista merece algumas reflexões.

Sobre revoluções não armadas, o que a História nos mostra é bem o contrário do que se argumenta acima. As revoluções que mais triunfaram, valeram-se de tecnologias que hoje nos parecem simples, mas que eram revolucionárias na ocasião. Revolucionárias, justamente, por propiciarem novas formas de comunicação que, aos costumes anteriores, pareciam pessoais e diretas ou desintermediadas – portanto, de credibilidade admissível –, mas que permitiam iniciativas anônimas de alcance inusitado, no vazio ou mesmo ao arrepio do ordenamento jurídico a respeito.

O anonimato pode, aqui, ser entendido como fundamento semiológico da privacidade, como uma forma de "última garantia" social em contextos de hipossuficiência jurídica para sua defesa. Não se deve aqui desnudar um mito apenas para encobrir outro: a eficácia da proteção ju-

rídica à privacidade não emana da respectiva norma jurídica *em si*, seja civil, processual ou constitucional, mas antes flutua pelos interesses políticos e econômicos que estiverem ativos no contexto. A título de exemplo desta flutuação, basta lembrar de algemas nos punhos de um certo banqueiro corruptor[6] diante de uma câmara de TV, e seus desdobramentos[7]. Em situações críticas, a proteção à privacidade terá de vir por outros meios, como ilustram eloquentes exemplos na História moderna.

Para exemplificar o funcionamento dessa "última garantia" como defensável pelos resultados socialmente benéficos, lembramos inicialmente que a revolução científica se valeu de traduções de clássicos de civilizações passadas, editadas sob pseudônimos e disseminadas (mais agilmente que as fogueiras) por meio da recém-inventada imprensa de tipo móvel, para beber e filtrar sua energia de fontes interditadas pelo poder semiológico da vez, o eclesiástico que vigia sobre o conhecimento "legítimo", evadindo seus controles anteriormente eficazes (antes dessa tecnologia gráfica).

E das revoluções francesa e americana, as quais se valeram, em sua origem, de desobediência civil. Nelas a panfletagem anônima foi usada para antes derrubar o dogma da origem divina do poder absoluto da realeza, com atuação "desregulada" dessa inovação tecnológica de Gutenberg. Revoluções das quais emergiu, no arcabouço jurídico dos freios e contrapesos da democracia moderna, justamente o instituto da proteção ao anonimato, para resguardar o indivíduo enfraquecido ante abusos do poder político ou econômico: como uma forma de autodefesa imunológica da sociedade ante a inclinação natural do Estado à tirania, em oposição ao direito à sua vedação, este necessário à eficácia do Estado Democrático de Direito.

A História é eloquente

Tal proteção ao anonimato foi depois estendida ao próprio processo democrático, no instituto do sigilo do voto, na legalização de denúncias anônimas, na proteção a testemunhas e, em alguns casos, à liberdade

6 Ver http://www1.folha.uol.com.br/fsp/dinheiro/fi1908200022.htm
7 Ver http://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Satiagraha

de expressão. Essa autodefesa se expressa, com ajuda do "império da técnica" que sempre se adianta ao Direito, em revoluções locais desarmadas que vêm triunfando par e passo com a revolução digital: nos desmanches do império soviético, das ditaduras de Suharto na Indonésia e de Marcos nas Filipinas, operados com a velocidade e capilaridade do e-mail, explorada pela esperteza semiesteganográfica de indivíduos que dominavam essa novidade tecnológica do final dos anos 1980[8]; nos contragolpes às conspirações midiáticas que tentaram plantar "a renúncia" do presidente sequestrado na Venezuela em 2002[9], e "a autoria do ataque" terrorista ao metrô de Madrid em véspera das eleições de 2004[10], expostas pela esperteza autoinvestigativa de indivíduos que concentraram sua cidadania em câmeras e SMS de celulares de última geração. E, por último, na recente sequência de levantes contra regimes autocráticos no Oriente Médio, acuados pela esperteza auto-organizada em redes sociais virtuais, de indivíduos que concentraram sua coragem e determinação cívica em praças públicas diante de filmadoras e fuzis. Agora às portas da Europa.

Se ainda havia alguma dúvida, empírica ou sofista que seja, de que as chances de iniciativas endógenas para extirpar a raiz tirânica de um sistema dependem, em essência, do fator "surpresa tecnológica", onde o anonimato serve de trincheira fundamental, a reação dos regimes recentemente acuados deveria honestamente sepultá-la. A reação imediata foi de desplugar toda a sociedade de suas mais novas, sofisticadas e "desreguladas" TIC, quando possível, e quando não, de catraquizar seus fluxos. A verdade essencial aqui é que as iniciativas anônimas, quando não são individualmente podres em seu objetivo, em seus meios trabalham dignamente para neutralizar o que lhes parece podre no coletivo. Por meio da desobediência civil, se o "podre" coletivo está na norma legal ou em sua aplicação.

Em nossas democracias, votos são comprados, mas tal podridão não parece motivo digno para se abolir o sigilo dos mesmos, ou seja, para se vedar o anonimato da autoria dos que são apurados. Em disque-denúncias, trotes são recebidos, mas tal podridão não parece motivo dig-

8 Ver, por exemplo, http://e-repository.tecminho.uminho.pt/poaw/SPIRIT04web
9 http://pt.wikipedia.org/wiki/Golpe_de_Estado_na_Venezuela_de_2002
10 http://pt.wikipedia.org/wiki/Atentados_de_11_de_mar%C3%A7o_de_2004_em_Madrid

no para se exigir do denunciante CPF e cadastro na operadora, para se verificar a identidade do denunciante antes de despachar a polícia. Em programas de proteção a testemunhas, quem busca o pseudoanonimato numa "nova identidade" é geralmente cúmplice indultado por delação premiada, mas tal podridão não parece motivo digno para se banir da lei esta opção processual, reconhecida como instrumento essencial no combate ao núcleo duro do crime organizado.

Esses casos não parecem dignos de exceção, no direito ao anonimato, porque suas consequentes podridões abusivas são efeitos colaterais ou custos sociais tolerados para os benefícios almejados. Mas então por que, quando se trata de liberdade de expressão, onde a podridão de abusos sempre serviu de trincheira individual contra a eficácia processual, a percepção de doutas mentes jurídicas se revela, na avaliação de custos e benefícios da sua proteção e de sua vedação, cada vez mais ideologicamente deslocada?

Esconder e vigiar

Das possíveis explicações para esse crescente deslocamento, algumas me parecem sintomáticas. Os sinais reveladores começam num surrado e tosco reducionismo, em retórica insinuante que desvia o debate para antes denunciar a fé alheia, que seria intrinsecamente má, e assim já tisnar aquelas outras fés que em si não forem: "...quem tem algo a esconder..." Qualquer resposta racional a insinuações desse tipo teria que ser relativa e especulativa: algo a esconder *de quem*, por q*uais razões*, e sob *quais circunstâncias*?

No escuro do abstrato, todas as fés são pardas. Mas no escuro das farisaicas intenções ocultáveis nesse tipo de argumento ("quem não tem o que esconder..."), quem se engaja nessa retórica tacitamente abraça um duvidoso princípio, o de um pretenso direito do Estado de prejulgar moralmente seus cidadãos. Com a óbvia contraface da questão – quem tem algo a bisbilhotar... – absolutizada no implícito dever do Estado em combater "o crime", onde qualquer resposta digna (do tipo: quais condutas serão tipificadas, por quais métodos, sob quais circunstâncias indiciantes

e probantes, e com quais prioridades e rigores persecutórios) soterrada ou manipulada por medos irracionais do desconhecido, insuflados pelo sofisma desse tipo de questionamento.

Tal direito implícito do Estado, exercido como querem os antianonimistas, constitui-se em convite ao empoderamento absolutista para os detentores da capacidade de monitorar, bastando que ambos ajam em conjunto, amplificando seu poder semiológico para isso, cooptando também os meios institucionais que poderiam coibir seus abusos (os quais também dependem das TIC). Esta é exatamente a definição, em forma de receita, que Mussolini dá para fascismo. Um Estado com capacidade absoluta de monitorar pode assim abusá-la, impunemente, de todas as formas tecnologicamente imagináveis.

Em alguma etapa desse empoderamento, a cooptação dos meios sociais de coibição de abusos se estende sobre o quarto poder, o da mídia corporativa (que também depende das TIC), para indução e manutenção de uma percepção coletiva orwelliana da "realidade dos fatos." E, por consequência lógica, na etapa seguinte esse empoderamento será ampliado sobre a mídia alternativa[11], por outros meios coercitivos, para controle da "liberdade de expressão" digitalmente intermediada: seremos livres para expressar o que for permitido, isto é, o que não for "indigno", no sentido hoje atinente à liberdade de expressão rotulado de "extremismo".

Essa é a função das TIC como arsenal no decisivo *front* psicológico da guerra cibernética e da guerra de amplo espectro. Nele, a capacidade total de monitoramento digital pode ser aplicada para se implantar na psique coletiva modos de percepção e de entendimento da "realidade oficial", inclusive nos mercados, através da manipulação opaca dos mecanismos cambiais e de precificação de ativos, atrelados a moedas cujo lastro é hoje tão somente o poderio militar. E para controle social, através da manipulação opaca dos mecanismos de documentação das práticas sociais, para se forjar ou se apagar provas documentais conforme os interesses assim coludidos.

A informatização capilarizada sob um tal controle abre um leque ilimitado para a possibilidade de se forjar provas falsas e irrefutáveis –

11 http://www.infowars.com/fcc-to-seize-cable-tv-broadband-regulations-for-internet-takeover/

mas legalmente válidas – contra qualquer um, e para o planejamento e execução de ataques de bandeira falsa, que tem sido estopins para toda guerra global. Isto significa, num mundo hiperconectado com o que vivemos hoje, um convite à transição para um Estado tirânico e global, de ideologia fascista, contra o qual as únicas defesas da cidadania serão limitadas ou paliativas.

Nesse tempo de turbulência política, com claras tendências à desintegração disseminada da ordem democrática e à instalação de uma tirania global, a informatização na gestão dos serviços de saúde pública se torna fonte de cobiça para o comércio estratégico de dados pessoais, que alimenta a corrida armamentista cibernética correspondente. Não só pelo valor que os dados pessoais sobre saúde representam para as técnicas de *profiling*, mas também para um Estado fascista restringir liberdades sob pretexto de forjadas condições sanitárias ou mentais. Nesse contexto, as medidas técnicas mais relevantes para defesa da privacidade, ao alcance de quem responde pela gestão de bases de dados na área da saúde, consistem em defesa política da autonomia dessa gestão, e em resistência às iniciativas de integração com outras bases sem motivo justificado como imperativo.

Crítica ao vigilantismo

O exemplo de argumento antianonimista – ou pró-vigilantismo – citado acima, de que "a defesa do anonimato no judiciário e no legislativo favorece única e exclusivamente quem detém os meios técnicos de invasão da privacidade no que diz respeito ao privilégio da informação ... o império da técnica, assim como o império das armas, concentra o poder no indivíduo mais habilidoso, ou mais esperto, mas sempre o indivíduo", merece análise mais detalhada devido a suas falácias.

- É fato que as armas, quando empregadas na guerra, o serão antes pelo Estado que por indivíduos, servindo tanto para a defesa quanto para o ataque. As armas de ataque, por exemplo, servem à defesa quando ostentadas para efeito dissuasivo.

- É fato que o privilégio da informação é gozado por quem detém meios de acessá-la, e que numa sociedade informatizada esse privilégio é supremo para quem controla a intermediação propiciada pelas TIC. Mas não é o indivíduo em si que controla quais tecnologias se tornam padrões, pois suas habilidades e espertezas agem pontualmente, para explorar padrões em seu favor. O papel de padronizar e controlar as práticas sociais digitalmente intermediadas é exercido, com brutal competitividade, por empresas monopolizantes do setor, as quais naquele argumento não aparecem.
- Sugerir que são sempre indivíduos – e não empresas globais como google, facebook, verizon e microsoft – que concentram maior poder em meios técnicos para invasão à privacidade soa no mínimo ridículo. Tampouco são indivíduos, por mais espertos ou habilidosos que sejam, que promovem corridas armamentistas, convencionais, nucleares e cibernéticas, em simbiose com o complexo cibernético-industrial-militar.

Escondido por essa retórica está a tendência evolutiva do papel do Estado, que vai se reorganizando em ente supranacional, cuja emergência se imbrica a interesses convergentes de megacorporações, sob o guante das financeiras, em um mundo sob vertiginosa transformação. Mundo onde só caberá ao indivíduo exercer papéis sociais quase sempre amorais, que fazem girar as grandes engrenagens do sistema e da vida terrena. Será que para nos situarmos nesse tipo de debate teríamos de fingir complacência com esse rumo? Tal complacência revela tibieza de princípios morais subjetivos e desprezo a lições trágicas do passado, e deixa o pêndulo da História reverter outra vez seu curso, de volta ao absolutismo.

O que é privacidade, ontem e hoje?

Defendo que a privacidade seja entendida como separabilidade de papéis sociais, controlada por quem exerce esses papéis. Por exemplo, um cidadão, que exerce o papel civil de indivíduo, de consumidor, de pai

ou mãe (se for o caso), de paciente (perante os serviços de saúde) ou de trabalhador (mesmo em atividades criminosas), decidindo o que nesses papéis é público, ou quando e como se misturam. O desejo individual por privacidade pode ser entendido, então, como manifestação social do instinto de defesa. Mas como tal inconsciente em situações de equilíbrio hobbesiano, ou seja, enquanto o "pacto social" implícito na aceitação do papel do Estado como guardião coletivo dessa defesa é respeitado. Em situações de acentuado desequilíbrio ou ruptura institucional, esse pacto tácito (que legitima o papel social do Estado) é posto em cheque, e a defesa de direitos individuais considerados fundamentais ou naturais por cada um fica à deriva.

Doutro lado, quando esse pacto tácito entra em crise, o Estado precisa manter sua legitimidade enquanto tenta reorganizar novos papéis sociais, os quais deseja impor aos indivíduos em sua nova forma de exercer o poder. Para isto o Estado precisa antes dar dois passos, que subtraiam do indivíduo a possibilidade destes seguir em escolhendo e controlando seus papéis sociais. O primeiro passo é o de convencer indivíduos de que eles não desejam, não necessitam, ou não devem exercer tais papéis de forma anônima, ou mesmo autônoma (o papel de condenado à prisão, por exemplo). De que o anonimato seria uma "perversidade" social, tão perverso quanto turbulenta for a crise. O segundo passo é o de impedir que possam exercer seus papéis de forma anônima perante o Estado.

Para completar o primeiro passo com sucesso, convém que do *front* psicológico se projetem gigantescos espantalhos intangíveis e inimigos invisíveis, tal como são vistos hoje o cibercrime, o terrorismo, o fundamentalismo religioso, etc. O estímulo ao voyeurismo (em redes sociais) serve então de arma psicológica para minar resistências, para que a renúncia à privacidade seja rotulada como necessária ao combate a esses inimigos postiços. Para o segundo passo, o arsenal está no controle das intermediações, ou seja, no controle do uso das TIC, para se evitar reveses com o fator "surpresa tecnológica", tal como estão tentando as grandes potências[12].

12 http:// lauren.vortex.com/ archive/000856.html, smeira.blog.terra.com.br/2011/06/01

Nessa marcha, o Estado se torna por dentro policialesco e totalitário, rumo à tirania, à revelia de como esteja organizado por fora (seja em república ou monarquia, democracia ou autocracia, federação ou império). Até que as forças sociais em ebulição se acomodem em um novo pacto, em outro regime que as estabilize, até a próxima crise. E assim, seguindo o pêndulo da História não faltarão arautos, com suas espertezas envernizadas de moralidade, buscando convencer outros disso ou daquilo, para locupletar-se ao final duma ou doutra coisa.

A internet pode ser neutra?

Num regime policialesco, o braço judiciário do Estado se hipertrofia, e sua estabilização demanda um mercado de serviços expandido; plausível razão para bacharéis em Direito, em qualquer função, tenderem ideologicamente a se opor às proteções legais ao anonimato, em períodos de crise do Estado. A revolução digital também abala o pacto implícito na divisão de direitos e deveres entre Estado, indivíduo e empreendimento privado. Nesse abalo, intuem aqueles, o custo de se fazer prova em juízo "precisa ser controlado, senão a impunidade acaba vencendo!"

Mas ocorre que a impunidade pode ser sinal, e não causa, de turbulências revolucionárias, inclusive da revolução digital ora em curso. Doutro lado, se esta revolução causar o abate do anonimato, os detentores do controle avançado sobre os fluxos informacionais, necessário para este abate, poderão, sempre que quiserem, expressar ocultamente seus interesses frente aos excluídos desse novo poder, mas o contrário, jamais (até à crise seguinte). Seria o estopim para mazelas que começam pela autoimplosão ou autofagia da ordem democrática, cujo sinal mais palpável são sistemas de votação eletrônica infiscalizáveis.

Defender o anonimato é defender um critério histórico, que se vale da técnica, em detrimento de critérios pseudo-humanistas, de cooptação pelo medo insuflado frente a incertezas crescentes. Um critério para habilitar quem queira participar, de maneiras ao seu alcance, nas tomadas de decisão sobre o curso da sociedade em momentos de crise. Para habilitar quem quer ter voz ativa na revolução digital, sem detrimento de quem

não queira, sem se expor a perseguições ideológicas e políticas. Há tudo de contrarrevolucionário na atitude contrária, de se atacar o anonimato num momento desses, habilitando os dois passos essenciais ao sucesso das contrarrevoluções políticas.

É inegável que o Estado contemporâneo se encontra sob enorme pressão para radicalizar seu ordenamento normativo e suas prioridades, no que tange à esfera digital e seus fluxos de bens simbólicos. Que nesses tempos a eficácia do seu poder depende do fim anonimato e do fim da neutralidade na internet. Daí podemos concluir que a contrarrevolução digital, também conhecida como ciberguerra, agora explicitamente declarada[13,14] está em pleno curso.

Mas que neutralidade é esta, sob ataque na ciberguerra? Se estendermos a noção de papel social para incluir o das organizações e empresas com suas plataformas de TIC, desempenhados através de serviços e protocolos implementáveis por software, o que se entende por neutralidade "da rede" corresponderia a uma generalização do conceito de privacidade, acima citado. Ou seja, essa neutralidade seria uma generalização do conceito de privacidade aplicado a serviços e processos que ocorrem na Internet. Uma generalização de cunho semiológico mas não jurídico, pois para o Direito a privacidade é um conceito cujo objeto é a pessoa humana.

Essa visão da neutralidade da rede é útil porque existe uma certa confusão ingênua, filha do mito da comunicabilidade global desintermediada, que surge quando o tema é abordado apenas em sua dimensão técnica, e que convém dissipar. Podemos observar que a independência de camadas numa pilha TCP/IP dá ensejo a que cada uma delas possa ser implementada e operada, em qualquer ponto ou segmento da rede, de forma autônoma, isto é, por agentes que não saibam, nem precisem saber, como estão operando outros intermediadores em outras camadas.

A arquitetura TCP/IP permite que tal acoplagem entre camadas funcione a contento, propiciando não só comunicações que parecem "diretas", mas também inovações que parecem não ter limites na Internet. Noutras palavras, o TCP/IP oferece por *design* o que se pode chamar

13 http://www.businessinsider.com/pentagon-says-it-will-respond-to-cyber-attacks-with-military-force-2011-5
14 http:/taosecurity.blogspot.com/2011/06/chinas-view-is-more-important-than.html

de neutralidade (ou "privacidade", no sentido de controle autônomo de processos) a nível sintático. Esta característica é por vezes qualificada de neutralidade técnica, ou embutida, da Internet. Porém, isso não impede que os agentes implementadores e operadores de serviços e processos numa camada possam ou queiram saber como outros estão operando em outras camadas, para quem, para quê, etc.

Esses agentes que oferecem intermediação digital (companhias telefônicas, fornecedores de hardware ou software, de serviço agregado, etc) podem muito bem, por canais outros que não o da acoplagem com as camadas acima e abaixo da sua, se intrometer no que fazem e como fazem outros intermediadores noutras camadas. E os maiores inevitavelmente querem. E para isso fazem alianças estratégicas, nem sempre reveladas ou legais, com outros que atuam noutras camadas. Muitas vezes "alianças" forçadas, como em casos de órgãos estatais que regulamentam a produção de dispositivos de telecomunicação, obrigando fornecedores a embutirem, em todo dispositivo vendido, portas de fundo ocultas que podem ser operadas secretamente por agências de três letras[15].

Sapos e pirâmides

Pelo que foi explicado acima, podemos concluir que a "linguagem" TCP/IP não pode oferecer neutralidade ou privacidade a rede digitais abertas, como a Internet, nem em nível semântico nem em nível pragmático. Ou seja, não pode oferecê-las aos demais níveis da comunicação humana (apenas ao nível sintático). Quem poderia oferecê-las seria o Direito, mas apenas sob condições de eficácia: se os poderes legislativos instrumentarem para isso a Justiça; se os Judiciários priorizarem esses instrumentos ante outros que já protegem interesses negociais opostos de intermediadores; e se os Executivos cumprirem com eficácia seus papéis de fiscalizar e coibir violações

Mas o que já seria difícil pela natureza do bem tutelado, e pela natureza dos meios de prova de violações, no contexto atual se torna uma

15 Por exemplo, nos EUA, através da lei CALEA: http://pt.wikipedia.org/wiki/CALEA

quimera. Com agências reguladoras de fachada, com a bússola neoliberal dando o norte da evolução tecnológica, e a contrarrevolução digital de vento em popa, a neutralidade que de fato existe na Internet (apenas em nível sintático) subsiste por inércia, no legado de uma idílica era pré-contrarrevolucionária. Na era da contrarrevolução digital, que estamos vivendo, tal legado se torna o cavalo de batalha pelo controle do que virá a ser a mais formidável infraestrutura de controle social já vista pela humanidade.

Sobre o contexto geopolítico em que isto está ocorrendo, parafraseamos a perspectiva do economista Wilfred Hahn[16]: A ideologia neoliberal, que acredita em mercados eficientes, capazes de engendrar um capitalismo de livre mercado, hoje não mais produz o que possa ser visto como algo que faça "o bolo crescer". Que permita a populações do planeta depois receber dele uma fatia maior. Ao contrário, o sistema econômico dominante está em desarranjo, como que anunciando um "fim de linha" para tal doutrina. As políticas de estímulo à demanda via endividamento estão cada vez mais impotentes e destrutivas, apenas concentrando cada vez mais capital em cada vez menos mãos.

Nesse contexto, atitudes e estratégias também vão mudando. Ultrapassar limites de prudência nas "regras do jogo" está se tornando tática comum em estratégias financeiras e políticas. A mudança de perspectiva de analistas e estadistas independentes é visível em todo o mundo. Nosso planeta é cada vez mais claramente, e pela primeira vez na História, visto por eles como finito, superpovoado e escasso em recursos de energia, terra arável e água potável, pelo que tais estratégias passam então a priorizar garantias de reservas e estoques, mesmo à custa de bolhas especulativas.

Uma cultura de acumulação predatória vai assim se formando. Para uns prosperarem, outros terão que pagar. A transição para esse padrão de comportamento leva Estados a tolerar, instituir e depois instilar práticas sociais de inspiração canibalista. Começando por esquemas de pirâmide financeiras, alimentadas pelo consumo supérfluo e pela destruição criativa[17], as quais, no fim da linha, se transformarão em pirâmides de sobrevivência.

16 http://www.eternalvalue.com/adownload/EVR_06_2011.pdf
17 http://en.wikipedia.org/wiki/Creative_destruction

O papel das TIC em evolução nesse processo foi, durante dez anos, objeto de uma série de artigos e palestras sob o título "Sapos Piramidais", em alusão à limitada sensibilidade térmica dos batráquios (restrita a choques bruscos de temperatura) que os fazem vulneráveis, sob lento aquecimento, até a fervura em vivo[18]. Mas os treze episódios da série nunca esclareceram as nuances e detalhes da metáfora. Agora, com o ponto de fervura se aproximando, cabe esclarecer.

A espécie de sapo que inspirou a metáfora é a *Notaden nichollsi*, da família *Myobatrachidae*, conhecido como pé-de-espada (*spadefoot*)[19]. É um anfíbio de reprodução explosiva, que habita os desertos do norte da Austrália, onde pode ficar enterrado na areia durante anos aguardando uma chuva ou inundação ocasional. Quando esse "evento de liquidez" ocorre, as poças viram cenário de um desbragado surto de atividade sexual, cujo barulho pode ser ouvido a quilômetros de distância. Em apenas um mês um ovo posto passa pelo estágio de girino e à fase adulta; a metamorfose precisa ser rápida, antes que as poças sequem.

18 http://www.cic.unb.br/~rezende/trabs/sapos.htm

19 http://bie.ala.org.au/species/Notaden%20nichollsi,http://blogs.scientificamerican.com/tetrapod-zoology/2015/01/02/north-american-spadefoot-toads/

E o que é mais fascinante: quando as poças se tornam turvas e rasas, os girinos passam a desenvolver dentes... até três fileiras deles. Começam então a comer uns aos outros, para acelerar seu crescimento e a seleção dos sobreviventes. Até que estes, os que galgarem o topo da pirâmide da sobrevivência, tenham que se enterrar novamente na areia, para sobreviver à seca seguinte. O título da série está inspirado na função desses dentes. A radicalização normativa em curso, que irradiará os efeitos da ciberguerra a toda a poça humana, tem função semelhante.

Ciberguerra contrarrevolucionária

A autonomização da esfera tecnológica, manifesta no perigoso mito da comunicabiliade global desintermediada, produz uma hiperconectividade que trará, como contrapartida ou efeito colateral no plano geopolítico, aquilo que alguns juristas chamam de erosão do Direito (e de sua implícita base moral). Essa autonomização tensiona aquilo que o filósofo Jurgen Habermas chama de juridificação do mundo vivido (*lebenswelt*), sob colonização pelo sistema político-econômico. Em nossa analogia batraquiana, tal colonização corresponde a um turvamento e rasamento do espaço de auto-organização biossocial (que entre os *Notaden nichollsi* induz a dentição nos girinos).

Na corrida global pela radicalização normativa, a rodada anterior à declaração multilateral de ciberguerra revela metaforicamente sua função, digamos, dentário canibalista, em propostas como a do ACTA[20]. Literalmente uma proposta de tratado para comércio internacional que busca combater a falsificação de marcas, na prática o ACTA é uma iniciativa de grandes cartéis do capitalismo pós-industrial, em aliança com o Departamento de Comércio dos EUA e o braço executivo de mais doze governos ideologicamente próximos, para demarcar novas fronteiras. Fronteiras institucionais para a mais nova forma de colonialismo, baseado em controle utilitário do conhecimento pelo capital.

20 http://www.cic.unb.br/~rezende/trabs/acta.html

Esse controle utilitário do conhecimento se realiza através do controle de fluxos de bens simbólicos – que incluem bases de dados pessoais –, controle este que se torna potencialmente ilimitado com a Internet e a convergência digital. Geopoliticamente, o ACTA é uma armadilha jurídica para limitar o braço legislativo de estados democráticos que forem legislar nacionalmente sobre esse tema (fluxo de bens simbólicos). Essa armadilha é montada com ambiguidades sobre as divisões funcionais na tripartição de poderes dos estados nacionais que aderirem ao tratado.

Tratados nesse molde (i.e., o ACTA e seus sucedâneos, como o TTP com a Ásia[21] e TTIP com a Europa[22]) servem também para estabelecer, a partir desse espaço político evacuado, e em conjunto com iniciativas similares noutros *fronts* da ciberguerra, bases funcionais para o braço armado de um governo supranacional, totalitário e global, que emerge da convergência de interesses entre esses cartéis e a inclinação natural de Estados dominantes à tirania, impulsionada pela hiperconectividade que as TIC propiciam. Porém, a riqueza virtual assim acumulada irá secar no deserto da escassez material vindoura, quando então a utilidade dessa "dentição normativa" se revelará canibalesca.

A sociedade brasileira pode encontrar dificuldades para entender esse contexto, em decorrência da forma como nosso legado cultural acolhe os conceitos de soberania, nação, cidadania e guerra. Opiniões como as aqui lavradas podem parecer, à primeira vista, puro devaneio ou idealismo, mas vale a pena insistir que devemos nos esforçar para entender um pouco mais a geopolítica do nosso tempo. Pois nossa terra e seus recursos são cobiçados do alto das pirâmides da *realpolitk*.

Já que o Brasil está sendo, com o ACTA e seus sucedâneos, encurralado junto com os demais países do grupo BRICS, convém tentar superar esse desconhecimento e observar como o governo do maior dentro do grupo encara publicamente a questão. Remeto o leitor a um artigo escrito por dois professores da Academia Militar do Exército Chinês, em um jornal oficial do Partido[23].

21 https://www.eff.org/issues/tpp
22 https://www.eff.org/pt-br/deeplinks/2013/07/tafta-us-eus-trojan-trade-agreement-talks-and-leaks-begin.
23 http://taosecurity.blogspot.com/2011/06/chinas-view-is-more-important-than.html

> *"...Assim como a guerra nuclear era a guerra estratégica da era industrial, a ciberguerra é a guerra estratégica da era da informação, e esta se tornou uma forma de batalha massivamente destrutiva, que diz respeito à vida e morte de nações... A ciberguerra é uma forma inteiramente nova que é invisível e silenciosa, e está ativa não apenas em conflitos e guerras convencionais, como também se deflagra em atividades diárias de natureza política, econômica, militar, cultural e científica... Recentemente, um furacão varreu a Internet pelo mundo ... Os alvos da guerra psicológica na Internet se expandiram da esfera militar para a esfera pública... Confrontadas com esse aquecimento para a ciberguerra na Internet, nenhuma nação ou força armada pode ficar passiva e está se preparando para lutar a guerra da Internet."*

Uma metáfora pode ser útil, no que é capaz de explicar por analogia, mas também enganosa, no que pode ocultar onde as diferenças estão. Não somos sapos com pés de espada, e por isso não podemos nos enterrar de cabeça na areia, em busca de sobrevida quando a água da nossa poça se esvai. Mas somos animais com vida no espírito, e por isso podemos nos entregar à promessa de vida eterna, quando a esperança neste mundo nos trai. Sem precisar nos enterrarmos vivos.

Falo de uma promessa com fiança em palavra profética que vem se cumprindo há mais de três mil anos, nos mínimos detalhes. Proferidas e registradas antes mesmo de existirem os contextos que poderiam lhe dar sentido, e reveladas a quem as quiser aceitar em seu coração contrito. A alternativa é sucumbir, por anfíbia soberba, nas guerras que se sucederão até o fim da linha.

10

Segurança da informação eletrônica em saúde: aspectos físicos, lógicos, éticos e legais

Cintia Ribeiro Vivanco[1]
Heimar de Fátima Marin[2]
Antonio Carlos Onofre de Lira[3]

Introdução

Este capítulo trata a questão da segurança da informação eletrônica em saúde através da análise histórica da sociedade sob o ponto de vista do compartilhamento de informações e sua progressiva evolução social em busca da individualização e do direito à privacidade. Com o objetivo de oferecer ao leitor, usuário de sistemas informatizados de saúde, uma leitura que possibilite a compreensão sobre os principais conceitos relacionados à segurança da informação eletrônica, sua relação com o direito à privacidade, e a disponibilização de dados como dever do Estado para manutenção do processo de controle social democrático sobre informações relacionadas à administração e gestão de recursos públicos.

1 Cintia Ribeiro Vivanco (crvivancoadv@gmail.com) é advogada, enfermeira, especialista em Informática em Saúde e Professora da Universidade Nove de Julho.
2 Heimar de Fátima Marin é enfermeira, Pós-doutora em Informática Clínica no Center for Clinical Computing na Harvard Medical School, Harvard University e Professora Titular da Universidade Federal de São Paulo – UNIFESP.
3 Antonio Carlos Onofre de Lira é médico, Doutor em Informática Médica – Universidade de São Paulo – USP e Superintendente Técnico Hospitalar do Hospital Sírio-Libanês.

Dada a relevância do tema e sua inegável complexidade técnica, selecionou-se conceitos basilares que sustentam reflexão a respeito do direito à privacidade no âmbito profissional, ético e legal destacando as principais normas regulamentadoras relacionadas ao tema.

Com relação à proteção física e lógica da informação, os conceitos apresentam as possibilidades utilizadas em sistemas de big data e, ao final, algumas questões relacionadas ao controle do indivíduo através da monitorização eletrônica de seus dados são apresentadas para provocar a reflexão e o debate entre Estado e instituições de saúde sobre a evolução tecnológica através dos sistemas de informação eletrônica público e privado, sua integração e o uso de medidas protetivas necessárias para a busca da melhoria na qualidade dos serviços, através da segurança da informação.

Breve digressão histórica

Ao longo de sua evolução, o homem caminhou da associação coletiva primitiva, onde os indivíduos para sobreviver ao ambiente hostil que os cercava, reuniam-se em pequenos grupos, para comunidades politicamente organizadas, como na Grécia, onde Aristóteles afirmava ser o direito e a lei, essenciais para a estruturação da "polis" (cidade). (MAGALHÃES, 2007).

O intuito não era apenas sobreviver, mas viver de forma organizada, estabelecendo regras de conduta, comando decisório e supremo através da delegação do poder natural do povo ao Estado. Sob o aspecto social de integração e valoração do coletivo, podemos observar que nossos ancestrais evoluíram da convivência coletiva para uma sociedade dividida em castas, como na Idade Média, época caracterizada pela concentração de riqueza e poder compartilhados entre clero e nobreza.

Durante séculos, a profunda desigualdade social que imperava na Europa estimulou movimentos que combatiam o regime monárquico e em 1789, a Revolução Francesa obteve sucesso como movimento político de desconstrução do poder instituído. O Iluminismo e sua visão antropo-

cêntrica, alçou o homem ao centro de todas as manifestações culturais, políticas e sociais como senhor de sua própria história.

A ascensão da burguesia definiu o pensamento comercial como movimento de organização contratual das relações comerciais. A sociedade é então organizada a partir das relações entre proprietários livres e a proteção oferecida pelo Estado está relacionada a pessoa e seus bens. (BONAVIDES, 2000). É a ascensão do Estado Liberal que institui como Direitos Fundamentais os Direitos Individuais relativos à liberdade, propriedade e igualdade; traduzido no pensamento: "laissez faire, laissez passer" (deixar fazer, deixar passar) e praticado através da livre concorrência. (LABRADBURY, 2006).

O século XIX caracterizou-se pela agudização do processo de omissão dos Estados frente aos problemas sociais e econômicos resultantes do capitalismo liberal praticado na Europa e América. Porém, após a Primeira Guerra Mundial, e a devastação de muitos países, as novas Constituições tomaram para si a responsabilidade sobre os Direitos Sociais como parte integrante dos Direitos Fundamentais do indivíduo, na tentativa de restabelecer o equilíbrio social. (PFAFFENSELLER, 2007).

Portanto, a análise evolutiva da sociedade denota um movimento que desloca-se do conviver coletivo até a supervalorização do indivíduo; culminando, em nosso presente momento histórico, em uma realidade dualista.

Sociedade digital e segurança da informação privada

Sob a ótica dualista, os direitos sociais definem conquistas de uma sociedade individualista de massa, onde observamos normas contraditórias como a valorização do indivíduo em um regime liberal e a valorização do grande número em defesa da igualdade e do consumo de massa, onde também se observa a escolha do individuo, porém, esta se dá em um contexto de convívio coletivo (LOWY, 1995).

Atualmente, a sociedade está conectada e interligada digitalmente e o desafio desta contradição social encontra-se na busca pelo equilíbrio

entre o que pode ser compartilhado socialmente e o que deve permanecer sob sigilo, na esfera privada. Neste sentido, a privacidade e a segurança da informação eletrônica de saúde que alimentam os sistemas de organizações públicas e privadas objeto deste estudo, devem ser definidas quanto aos seus limites, de acordo com a autodeterminação do indivíduo, respeitados os ditames legais que caracterizam o Estado de direito. (FORTES, 1998).

Neste momento, algumas questões sociolegais emergem para reflexão:

- Em um sistema eletrônico utilizado pelas instituições de saúde para oferecer uma melhor qualidade assistencial, que tipo de informação do indivíduo será coletada?
- Como se fará o uso desta informação?
- Quem usará esta informação?
- Como será o acesso a esta informação?
- Como se garantirá a integridade, a confiabilidade e a atualização desta informação?
- Como selecionar a informação essencial à prestação da assistência?
- Como detectar o mau uso desta informação?
- Existe um modelo ideal de software que alie o compartilhamento de dados com a garantia da segurança da informação?
- As respostas para todas estas questões estão relacionadas à segurança da informação, que objetiva, através de mecanismos diversos, a proteção necessária sobre dados e informações que possuem valor para o indivíduo proprietário destas informações e também para a organização que as coletou, armazenou e que detêm sua posse.

Existem três conceitos relacionados à segurança da informação que devem ser entendidos (HAUGHN & GIBILISCO, 2014):

1. ***Integridade de dados e/ou informações e programas***: propriedade que garante que a informação manipulada mantenha

todas as características originais estabelecidas pelo proprietário da informação incluindo o controle de alterações e garantindo o ciclo de vida da informação (inserção no sistema, manutenção e destruição).

2. ***Integridade de uso ou confidencialidade***: propriedade que limita o acesso à informação tão somente às entidades legítimas, autorizadas pelo proprietário da informação.
3. ***Disponibilidade de dados e/ou informações***: propriedade que garante que a informação esteja sempre disponível para seu uso legítimo.

Através desta tríade C.I.A. (*Confidentiality, Integrity, Availability*), pode-se orientar a análise, planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outras propriedades como: Legitimidade e Autenticidade complementam as características que um sistema deve apresentar para definição de uma Política de Segurança da Informação adequada, à medida que transações eletrônicas são realizadas através da comunicação e do compartilhamento de informações entre sistemas. (ALBUQUERQUE JUNIOR & SANTOS, 2011).

Os mecanismos de segurança da informação podem ser físicos e lógicos, merecendo destaque as barreiras lógicas que impedem ou limitam o acesso à informação contida em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada.

O controle físico de segurança da informação está relacionado à estrutura do local onde estão armazenados os equipamentos que contêm informações sigilosas – portas, trancas, paredes, blindagem, seguranças pessoais capacitados para controlar acesso de pessoas não autorizadas, sistema de monitoramento de imagem 24 horas, sistemas de detecção de movimento e calor para acionamento de alarmes. Estas barreiras limitam o contato ou acesso direto a estes equipamentos e compõem a primeira barreira impeditiva de controle para proteção digital.

Mecanismos lógicos de segurança das informações

Dentre os mecanismos lógicos de segurança, considera-se todas as soluções relacionadas à guarda de dados e informações de instituições de saúde que possuam *software e hardware* direcionados ao uso destas informações em prol da qualidade assistencial. A quantidade de dados armazenados e compartilhados por estas organizações tem aumentado exponencialmente graças aos avanços dos programas utilizados e, atualmente, o uso do ***Big Data*** se faz pela maioria das instituições de grande porte.

O ***Big Data*** pode ser entendido como uma grande quantidade de dados, estruturados e não estruturados, medidos em *terabytes* ou *petabytes,* que as organizações podem acessar para uso imediato ou posterior, de acordo com seus objetivos. Portanto, existem sistemas de segurança tradicionais que ordenam e gerenciam uma quantidade de dados controlada e aqueles direcionados para manipulação do ***Big Data***.

Dentre os sistemas de segurança lógica da informação, destaca-se a criptografia, ou sistema de encriptação, muito utilizado para segurança na transmissão de dados e informações. Cripto (grego *kryptos*) que significa esconder, ocultar. Grafia (grego *graphein)* significa escrever, portanto, a Criptografia pode ser entendida como escrita oculta ou secreta. (TKOTZ, 2005). Consiste em um sistema de cifragem que oculta a informação contida na mensagem, permitindo a transformação reversível da informação de forma a torná-la ininteligível a terceiros. A criptografia pode ser simétrica ou assimétrica. O modelo simétrico caracteriza-se pelo compartilhamento entre emissor e receptor da mensagem com a mesma chave de acesso. A criptografia assimétrica, mais utilizada, por tratar-se de um modelo mais seguro, caracteriza-se pelo uso de uma senha pública pelo emissor da mensagem, e outra senha privada conhecida somente por ele. Em uma infraestrutura de chaves públicas, usa-se o sistema de criptografia assimétrica, combinada com a função de *hash* (resumo de mensagem) (TREVISAN, 2004).

Outra barreira lógica de segurança é a assinatura digital, que pode ser entendida como um conjunto de dados cifrados, associados a um documento que garante a integridade do documento associado, mas não sua confidencialidade. A verificação da assinatura é realizada "decifrando-se" o criptograma

(assinatura) com a suposta chave-pública correspondente, sendo válido o resultado, é autêntica a assinatura, uma vez que só o detentor da chave privada, par da chave pública utilizada, poderia ter gerado aquela assinatura.

A garantia da autenticidade, integridade e confidencialidade das informações pode ser alcançada através do processo de certificação digital, que atesta a validade de um sistema informatizado que guarda e manuseia informações. Os sistemas de Registro Eletrônico de Saúde (SRES), podem obter a certificação eletrônica, pelo processo voluntário de certificação oferecido através da parceria firmada entre a Sociedade Brasileira de Informática em Saúde (SBIS) e o Conselho Federal de Medicina (CFM), autoridades certificadoras, assim reconhecidas na Resolução CFM nº 1821/2007 que aprova o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde versão 3.0. (CFM & SBIS, 2012)

Sob a análise dos componentes de segurança lógica dos sistemas, outro mecanismo de controle de acesso é o sistema de firewall, em tradução livre: parede de fogo, que consiste em um dispositivo de rede que protege os dados de um determinado ponto da rede de computadores. Ele pode se apresentar em software ou hardware e também combinado, quando é designado "*appliance*". Sua complexidade e alcance é definida pelo tamanho da rede, fluxo de entrada e saída de informações, a política de segurança da organização e finalmente pelo nível de segurança necessário.

Com relação ao desenvolvimento de *softwares* (suporte lógico desenvolvido para uso em computadores ou equipamento similar), é indispensável que haja respeito às normas técnicas de segurança. Atualmente, a Norma ISO/IEC 27.002 define os critérios para gestão da segurança da informação, no desenvolvimento destes programas (ISO-IEC, 2009).

O uso de senhas, palavras-chaves, sistemas biométricos e cartões inteligentes completam os mecanismos de controle de acesso (acessibilidade) a dados e informações armazenados nos sistemas eletrônicos das organizações de saúde.

Com relação à proteção do **Big Data,** as organizações de saúde elaboram e supervisionam os sistemas de segurança, bem como respondem sobre eventuais eventos adversos que comprometam a segurança das informações coletadas. Dentre as funcionalidades do sistema de segurança do ***Big Data***, deve-se assegurar:

- **Agregação dos dados** de todos os servidores, redes, base de dados, utilizadores, *cloud* (nuvem de dados);
- **Organização / normalização** de dados estruturados para facilitar análise e tratamento;
- **Indexação e categorização de dados**, as quais facilitarão a correlação e identificação de padrões para propiciar a criação de alertas em tempo real na detecção de incidentes.
- **Monitorização de atividade maliciosa em curso**, a qual permite envio de avisos, como e-mails ao responsável e equipe notificando-os sobre risco operacional, assim, alertas de segurança são disparados cientificando a todos os usuários sobre o risco operacional.

Concluindo, pode-se entender que o nível de segurança desejado para proteção dos dados e informações de um sistema eletrônico de saúde materializa-se através da confluência entre os sistemas de segurança lógico e físico, e estes são complementados pela Política de Segurança da Instituição, definida e respeitada por todos os colaboradores diretos e terceirizados, bem como os usuários internos e externos. A Política de Segurança deve garantir que, uma vez estabelecidos seus princípios e normas, o nível de segurança desejado será perseguido e mantido.

A análise dos riscos associados à falta de segurança, auditorias de processos, benefícios de sua implementação e custos de implementação dos mecanismos devem ser apresentados a todos os colaboradores e usuários do sistema, para fomentar a cultura da segurança da informação eletrônica de saúde institucional, através de um programa de capacitação bem estruturado que deverá ser aplicado periodicamente.

Implementação da Política de Segurança da Informação Institucional

A Política de Segurança da Informação consiste num conjunto formal de regras que devem ser respeitadas e seguidas pelos usuários dos recursos disponibilizados no sistema de registro eletrônico de saúde de

uma organização. Dentre suas características, há atribuição de direitos e responsabilidades na manipulação das informações armazenadas no sistema, além das atribuições de cada um em relação à segurança dos recursos com os quais trabalham (VITORINO & COSTA & KENCHIAN, 2011).

Esta política deve basear-se em critérios que norteiam o acesso de indivíduos que procuram informações a respeito da instituição ou atendidos por ela, profissionais de saúde, outras instituições que compartilham dados e informações e também pelos auditores internos e externos. As regras e mecanismos que autorizam pessoas ao acesso de informações devem considerar a relevância da informação contida e a necessidade de uso desta informação pelo usuário solicitante, além de mecanismos que permitam o registro de acesso para rastreamento do usuário sempre que necessário.

A primeira questão que deve ser considerada na elaboração de uma Política de Segurança reside no entendimento sobre a propriedade e posse da informação de saúde. Em instituições privadas, a concorrência faz parte do jogo comercial, e a busca incessante pela diferenciação no mercado se dá através dos serviços oferecidos, qualificação de profissionais, disponibilização de equipamentos de última geração para diagnóstico e tratamento, ambiente agradável e atendimento personalizado. São os detalhes em cada um destes segmentos que podem conquistar e manter novos usuários dos serviços de saúde. A individualização no atendimento, por vezes se faz através de informações pessoais destes usuários. Questões relacionadas à licitude sobre o acesso e uso destas informações podem gerar desconforto aos gestores e consequências negativas à instituição.

O uso de dados relacionados ao usuário do serviço, que agregam elementos diferenciais qualificando e individualizando a assistência, pode variar quanto a relevância, porém todos eles são de propriedade do usuário e não devem ser utilizados sem a devida autorização; por exemplo, o uso de informações como: perfil epidemiológico, uso contínuo de medicamentos, alergias, doenças pregressas, histórico familiar para doenças genéticas, procedimentos cirúrgicos realizados, tempo de internação anterior, causas de internação e reinternação, restrições quanto a visitas, passatempos, preferências gastronômicas, crenças religiosas, etc., oferecem à instituição a oportunidade de customizar seus serviços conquistando, assim, a fidelização deste usuário.

Questiona-se:

- Qual o limite para que não haja violação do direito à privacidade e sigilo de dados e informações dos usuários do serviço de saúde?
- Como a Política de Segurança Institucional pode proteger estas informações quanto ao acesso e uso?

Deve-se considerar neste contexto o uso inadequado e não autorizado com a violação dos limites de segurança para uso indevido de dados e informações, como, por exemplo, a interceptação e venda de banco de dados, que caracterizam um dos inúmeros delitos definidos como crime cibernético, onde a conduta criminosa se materializa através do uso de um computador, uma rede ou um dispositivo de hardware. (CAVALCANTE, 2013).

Para que a Política de Segurança proteja adequadamente todas as informações contidas em seu sistema, é necessário que o sigilo e a privacidade sejam definidos a partir da cientificação de todos os usuários do serviço de saúde para que estes possam autorizar o acesso de seus dados, considerando, para tanto, o respeito à sua Autonomia. Assim, ao admitir um novo usuário, a instituição de saúde deve oferecer orientação adequada a ele, ou a seu representante legal, quanto à Política de Segurança eletrônica, destacando como elementos essenciais desta norma institucional – a manutenção do sigilo de todos seus dados e informações pessoais e de saúde, o uso exclusivo pelos colaboradores da instituição das informações para prestação de serviços assistenciais de saúde, e que qualquer compartilhamento de dados se efetivará após devida autorização do usuário ou de seu representante.

Tornando-o consciente quanto ao uso de suas informações, a instituição estará se resguardando legalmente de qualquer prestação jurisdicional pleiteada "*a posteriori*" pelo uso indevido destas, descaracterizando o eventual expectativa de privacidade conforme artigo 5º, X, da Constituição Federal de 1988 (BRASIL, 1988).

As Políticas de Segurança devem definir ainda as áreas de responsabilidade dos usuários/clientes, dos colaboradores assistenciais, dos profissionais terceirizados, do pessoal de gestão de sistemas de redes e da

cúpula diretiva institucional. Suas diretrizes devem adaptar-se a alterações organizacionais e avanços de sistemas, para fornecerem um enquadramento de implementação de mecanismos de segurança com adequação tecnológica.

Os procedimentos de segurança devem compor as normas da política de segurança institucional e sua descrição seguirá modelo objetivo e claro para ciência e concordância tácita de todos submetidos a ela, colaboradores diretos e indiretos legitimamente autorizados ou não. Dentre eles, processos de auditoria, rastreabilidade de dados do sistema e procedimentos internos de responsabilização com definição de punições administrativas, que devem ser graduais e suplementares de acordo com o tipo de evento e sua gravidade, podendo culminar com a dispensa por justa causa.

Com relação aos aspectos técnicos de implementação dos mecanismos de segurança, é desnecessário que sejam explicitados no corpo deste documento, podendo, no entanto, comporem anexo de informações técnicas, haja vista suas características específicas e a necessidade de atualizações constantes, o que obrigaria a reestruturação de todo o documento periodicamente, não agregando maior entendimento ao usuário comum sobre as normas estabelecidas. Deve ser um documento de fácil leitura e compreensão, permanecendo disponível em local acessível tanto aos colaboradores quanto aos usuários do serviço de saúde.

Portanto, a premissa que norteia a elaboração da Política de Segurança Institucional deve ser: "tudo que não é expressamente proibido, é permitido", assim, a definição de toda estrutura normativa do uso do sistema institucional é primordial para a efetividade de sua aplicação, importante destacar que estas normas internas estejam em consonância com as práticas da segurança da informação de cada ambiente da organização, alcançando, assim, eficácia e eficiência no processo de tomada de decisão sobre os recursos de TI. Este documento deve ser considerado como parte da filosofia e da cultura organizacional, através da educação permanente dos colaboradores para que todos estejam cientes sobre os limites de suas ações de acesso, manipulação e uso de dados e informações dos usuários, bem como as implicações e punições administrativas resultantes do mau uso do sistema. O respeito a esta norma interna deve ser estimulado e garantido a todos os colaboradores.

Aspectos éticos e legais da segurança da informação

Em um passado não muito distante, apenas a algumas décadas, as informações das organizações eram armazenadas apenas em papel e seu patrimônio era mensurado pela quantificação de seus bens materiais. Atualmente, um grande número de instituições de saúde armazena suas informações em meio eletrônico, substituindo definitivamente documentos em papel. Com isso, otimiza-se a eficiência de processos e o espaço físico anteriormente ocupado por um volume sem fim de documentos em papel, poderá ter seu uso diversificado e qualificado. O patrimônio mais precioso das instituições de saúde é o conhecimento contido e armazenado em seus sistemas de registro eletrônico em saúde e enriquecido continuamente por seus colaboradores. As redes e sistemas de intranet cada vez mais se interconectam para o compartilhamento de dados, muitos deles armazenados em "cloud" (nuvem digital). Esta realidade oferece inúmeros benefícios, principalmente no quesito gestão da qualidade assistencial, porém, há que se considerar os limites éticos e legais no uso destas informações.

Podemos entender ética como um mecanismo de regulação das relações sociais, que implica uma opção individual, filtrada pelos valores e vivências de cada um na busca pela resposta "do que deve ser feito" e não "do que pode ser feito". (COHEN & SEGRE, 1995).

A ética contemporânea considera que os limites a serem estabelecidos no convivio social, devam garantir o respeito à dignidade humana. Instrumentalizando o cidadão cada vez mais empoderado e conhecedor de seus direitos para que ele acione os mecanismos de defesa e proteção jurisdicional quando sentir-se ameaçado com relação ao respeito à privacidade e sigilo de seus dados e informações eletrônicas.

A privacidade de um indivíduo consagra a liberdade e a segurança das relações íntimas garantidas na conquista da cidadania (BASTOS, 1999) e o direito de privacidade é parte dos direitos personalíssimos do indivíduo, constitucionalmente assegurados, no artigo 5º, X, da Constituição Federal de 1988. A guarida da intimidade, assim como da vida privada, consiste na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhe o

acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano (BASTOS, 1999).

Segundo a Declaração Universal dos Direitos Humanos, é assegurado: "o direito de cada pessoa ao respeito de sua vida privada." (UNESCO, 1998). Mas é um direito relativo, pois comporta exceções, constituindo-se em uma forma de instrumento social em favor do bem comum e da ordem pública, prevalecendo o interesse coletivo sobre o particular. Em serviços de saúde, principalmente hospitais (GOLDIN E FRANCISCONI, 2004), afirmam que durante uma internação, até 75 pessoas diferentes, incluindo-se os profissionais de saúde, chegam a lidar com o prontuário de um paciente, ampliando as chances de violação da privacidade e sigilo destes dados. Para coibir esta prática, há um arcabouço de normas e legislação pertinente à proteção da informação eletrônica de saúde, incluindo-se os Códigos de Ética dos Profissionais de Saúde.

Relaciona-se com o direito à privacidade o dever de segredo/sigilo do profissional de saúde. Segundo o Juramento de Hipócrates: "O que no exercício ou fora do exercício e no comércio da vida eu vir ou ouvir, que não seja necessário revelar, conservarei como segredo." (CREMESP, 2015). A violação do sigilo profissional é uma circunstância que compromete a liberdade individual.

O Código de Ética Médica, conforme Resolução CFM nº 1.997/2012, proíbe ao médico revelar fato de que tenha conhecimento em virtude do exercício de sua profissão. Esta obrigação é um direito do paciente e uma conquista da sociedade organizada, que permite a quebra do sigilo apenas por autorização expressa do usuário do sistema de saúde ou de seu representante legal, por justa causa ou por dever legal.

Da mesma forma, o Código de Ética dos Profissionais de Enfermagem de acordo com a Resolução COFEN nº 311/2007, em seu capítulo II, artigo 82, define (COFEN,2007):

> "Manter segredo sobre fato sigiloso de que tenha conhecimento em razão de sua atividade profissional, exceto casos previstos em lei, ordem judicial, ou com o consentimento escrito da pessoa envolvida ou de seu representante legal."

O mesmo diploma legal, em seu artigo 84, proíbe acesso a informações ou a documentos de pessoas que não estejam diretamente envolvidas na prestação da assistência, exceto nos casos previstos na legislação ou por ordem judicial. Entende-se que apenas a equipe de saúde diretamente envolvida na assistência do paciente tem o direito de conhecer os fatos sigilosos, resguardada a hierarquia das informações, para definição de acesso e a necessidade de uso, para o exercício profissional adequado.

Coadunam-se a estas normas éticas profissionais, a previsão do direito à privacidade estabelecido em nossa Constituição Federal de 1988 (BRASIL,1988) que, em seu artigo 5º, assegura a todos os brasileiros a inviolabilidade do direito à segurança, abrangendo entre outros os seguintes itens:

1. é inviolável o sigilo de dados;
2. é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
3. são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;
4. todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
5. conceder-se-á "habeas-data" para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público para a retificação de dados quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

O artigo 21 do mesmo diploma legal estabelece que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Em normas infraconstitucionais, como o Código Civil e Código Penal, há o estabelecimento da responsabilização do indivíduo violador do

direito à privacidade. O Código Civil (BRASIL, 2002), em seus artigos 20 e 21 estabelece:

- Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
- Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Havendo dano, há lugar para a reparação civil, a menos que o acusado prove que existe alguma condição excludente de ilicitude. Este dever persiste não apenas durante o tratamento, mas mesmo depois de extinto o vínculo entre profissional de saúde e cliente, respeitada a prescrição do direito de requerer reparação.

Assim, será responsabilizado aquele que por culpa ou dolo violar direito a privacidade causando prejuízo a outrem, conforme previsão nos artigos: 159, 1056 e 1545 do Código Civil (BRASIL,2002).

O Código Penal, instituído pelo Decreto Lei nº 2848/1940, tipifica em seus artigos 153 e 154, ato lesivo à liberdade individual, a violação de sigilo de documentos ou de informações contidas em sistemas de informação, com previsão de pena de detenção de 3 meses a um ano ou multa (BRASIL,1940). Atualizando a norma supracitada, a Lei nº 12.737, de 30 de novembro de 2012 (BRASIL,2012c), define a redação do artigo 154-A estabelecendo:

> "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou des-

truir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: pena de detenção de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Ação penal

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Caracteriza-se crime tipificado no artigo 305 do mesmo diploma legal, a ocultação, destruição, supressão de documentos públicos ou particulares, com previsão de pena de 02 a 06 anos e multa.

O crime de inserção de dados falsos, previsto no artigo 313A, estabelece pena de 2 a 12 meses e multa, e o crime de modificação ou alteração não autorizada de sistema de informação, artigo 313B, estabelece pena de 03 meses a 02 anos e multa.

O Código de Processo Civil (BRASIL,1973), em seus artigos 347, 363 e 406, diz respeito, entre outros itens, ao depoimento e apresentação de documentos nas situações onde o depoente apresenta o dever profissional de manter sigilo:

> Art. 347. A parte não é obrigada a depor de fatos: II - a cujo respeito, por estado ou profissão, deva guardar sigilo. Parágrafo único. Esta disposição não se aplica às ações de filiação, de desquite e de anulação de casamento.
>
> Art. 363. A parte e o terceiro se escusam de exibir, em juízo, o documento ou a coisa: (Redação dada pela Lei nº 5.925, de 1º.10.1973)
>
> Art. 406. A testemunha não é obrigada a depor de fatos: II - a cujo respeito, por estado ou profissão, deva guardar sigilo.

No mesmo sentido, o Código de Defesa do Consumidor instituído pela Lei nº 8078/1990 (BRASIL,1990) em seu artigo 43, §§ 1, 2, 3, 4 e 5 tratam sobre os dados cadastrais do consumidor em bancos de dados e seu acesso, e o artigo 44, § 1 trata sobre a disponibilidade e acesso pelo consumidor a informações de fornecedores de produtos e serviços.

A Carta dos Direitos dos Usuários da Saúde, em todo o País (BRASIL, 2006), estabelece em seu quarto princípio que o sigilo e a confidencialidade de todas as informações pessoais, mesmo após a morte, salvo quando houver expressa autorização do usuário ou em caso de imposição legal, como situações de risco de terceiro ou por ele autorizado deve ser resguardado, bem como deve ser facilitado a qualquer tempo o acesso pelo indivíduo ou por terceiro autorizado por ele a dados registrados em prontuário, bem como ter garantido encaminhamento de cópia em caso de transferência.

Marco Civil Regulatório da Internet no Brasil: Aspectos de segurança

Recentemente, foi publicada a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil Regulatório da Internet que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (BRASIL, 2014). Sua análise se faz relevante neste contexto, pois se entende que a questão da segurança da informação extrapola o âmbito das organizações que lidam com dados de saúde, mas não as exclui; abarcando toda a sociedade na utilização dos meios de comunicação eletrônico, e obrigando a todos os cidadãos e organizações a se adequarem a norma, pois o uso da internet é parte integrante do sistema eletrônico mantido por estas organizações.

Com relação à privacidade dos usuários da rede, é garantia estabelecida pela nova lei, ficando proibido o repasse de informações de usuários para terceiros sem o consentimento expresso e livre do proprietário da informação.

A proteção dos dados de internautas é garantida e só poderá ser quebrada mediante ordem judicial. A garantia é estendida à privacidade das comunicações, incluindo e-mails. Há também a garantia de liberdade de expressão e retirada de conteúdo do ar, que só poderá ser realizada mediante ordem judicial, com exceção dos casos de pornografia de vingança, onde a vítima poderá solicitar diretamente aos sites que hospedam o conteúdo sua retirada.

Tratando também sobre o acesso à informação, o Decreto-Lei nº 7.724/2012 (BRASIL,2012a), que regula a Lei nº 12.527/2011(BRASIL, 2011d) define acesso de informação, obrigando os órgãos públicos federais, estaduais e municipais, bem como entidades privadas sem fins lucrativos que recebem verbas públicas como ONGs, a oferecer informações relacionadas a suas atividades a qualquer cidadão que solicitá-las. Esta lei revoga disposição anterior prevista na Lei nº 11.111/2005 e dispositivos da Lei nº 8.159/91 e Lei nº8112/90. Neste caso, podemos considerar que a publicidade de informações públicas passou a ser regra, e o sigilo exceção, em respeito ao cuidado com o bem público que prevalece sobre o privado.

A Medida Provisória 2.200-2, de 24 de agosto de 2001, institui a Infraestrutura de Chaves Públicas Brasileira-ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em meio eletrônico, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (BRASIL, 2001). Esta medida considera documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos que ela trata. As declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil, presumem-se verdadeiras em relação aos signatários. Caso haja outro meio de prova de autoria e integridade documental que utilize outro tipo de certificado, que não emitido pela ICP-Brasil, será respeitada sua legitimidade desde que aceito pela parte a quem for entregue o documento.

A Norma ABNT NBR ISO/IEC 27002 (ABNT, 2005) substituiu a norma ABNT NBR 17799 (ABNT, 2000) e trata sobre política de segurança da informação, com o objetivo de prover uma orientação para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. Norma ISO /IEC 15408 (ISO IEC, 2009) define os critérios para avaliação da segurança da informação no desenvolvimento de softwares.

A Declaração de Tel Aviv, Israel, 1995 – 51ª Assembleia Geral da Associação Médica Mundial é considerada o marco histórico para a regulação do programa de telemedicina, e foi a partir de suas de-

finições que o Brasil regulamentou o programa no país através da (AMM,1999):

- Portaria Ministério da Saúde nº 402, de 24 de fevereiro de 2010: - Institui, em âmbito nacional, o Programa Telessaúde Brasil para apoio à Estratégia de Saúde da Família no Sistema Único de Saúde e institui o Programa Nacional de Bolsas do Telessaúde Brasil (BRASIL, 2010)
- Portaria 2.546, de 27 de outubro de 2011. Redefine e amplia o Programa Telessaúde Brasil, que passa a ser denominado Programa Nacional Telessaúde Brasil Redes (Telessaúde Brasil Redes) (BRASIL,2011b).
- Portaria do Ministério da Saúde nº 2.554, de 28 de outubro de 2011 - Institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes (BRASIL,2011c). Posteriormente alterada pelas Portarias MS/GM nº 3.127, de 28 de outubro de 2012 (BRASIL, 2012d) e nº 2.525 de 29 de outubro de 2013 (Brasil, 2013).

A Agência Nacional de Saúde Suplementar estabelece em Resoluções específicas normas pertinentes à segurança da informação de saúde do usuário dos serviços de saúde suplementar, como se vê na Resolução nº 255/2011, que revoga a RDC nº 64/2001 e dispõe sobre a designação de médico responsável pelo fluxo de informações relativas à assistência médica prestada aos consumidores de planos privados de assistência à saúde (BRASIL,2011a). A Resolução nº 305/2012, que estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde (BRASIL, 2012b).

Os Conselhos Federais dos Profissionais de Saúde, através da prerrogativa que lhes permite legislar sobre assuntos relacionados à prática do exercício profissional da categoria que representam, definem em Resolução as normas referentes ao sigilo e à privacidade de dados e informações de saúde, merecendo destaque:

Resolução das normas dos conselhos referentes ao sigilo e à privacidade de dados e informações de saúde

Referência	Descrição da norma	Assunto
CRM- PR,2000	Resolução CRM- PR nº 89/2000	Criou a Câmara Técnica de Informática em Saúde.
CFM, 2002a	Resolução Conselho Federal de Medicina-CFM nº 1.638/2002	Criação da Comissão de Revisão de prontuários nas instituições de saúde.
CFM, 2002b	Resolução CFM nº 1.643 publicada em 2002	Disciplina a prestação de serviços; telemedicina.
CFM, 2002c	Resolução CFM nº 1.653/2002	Demonstrações cirúrgicas ao vivo; autorização e ciência sobre os fatos.
CFM, 2002d	Resolução CFM nº 1.639/2002	Normatiza uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico",
CFM,2003	Resolução CFM nº 1.665/2003	Responsabilidade ética; portadores do vírus HIV soropositivos; sigilo profissional.
CFM, 2007a	Resolução CFM nº 1.819/2007	Diagnóstico codificado CID; tempo de doença no preenchimento das guias da TISS de consulta e solicitação de exames.
CFM,2007b	Resolução CFM nº 1.821/2007	Digitalização e uso de sistemas informatizados; guarda e manuseio dos documentos dos prontuários dos pacientes.
CFM,2011	Resolução CFM nº 1.976/2011	Altera a redação do parágrafo único do artigo 1º da Res. nº 1819/2007

Nos Estados Unidos da América está em vigor o Código Eletrônico de Regulamentos Federais, lei que determina a troca de informações eletrônicas em saúde, através da HIPAA *Health Insurance Portability and Accontability Act*,(HIPAA,1996) Esta lei cria padrões, com identificadores únicos para beneficiários, prestadores, fontes pagadoras e operadoras. Os procedimentos dirigem-se à proteção, uso e divulgação de informação protegida de saúde, contabilidade das divulgações, acesso por indivíduos e por terceiros. Ela equilibra a necessidade de proteção da privacidade do usuário dos serviços e as possibilidades de aplicação da TI na saúde.

Seu uso é obrigatório quanto à segurança desde 20/04/2005 e quanto à privacidade, desde 2003.

Cabe à instituição de saúde o papel de depositária e guardiã das informações do usuário, e é dela a obrigação na adoção de todas as ferramentas necessárias para que se façam cumprir as exigências legais acima citadas. Zelando pela segurança da informação de seus usuários, através de um sistema que possua mecanismos de proteção, salvaguarda, auditabilidade, confiabilidade e privacidade.

Quando não cumpridos os ditames legais, o infrator, profissional de saúde, responderá pelas consequências penais, civis e também administrativas relacionadas às sanções disciplinares previstas em seu Código de Ética Profissional.

Desafio à segurança da informação

- ***Monitoramento eletrônico do usuário do sistema de saúde no Brasil***

Atualmente, o monitoramento eletrônico de paciente à distância é uma das principais inovações em softwares de saúde. Diversas empresas especializadas no desenvolvimento de programas para telemedicina estão disponibilizando para o mercado especializado em saúde softwares que monitoram a distância o indivíduo que faz uso dos serviços destas instituições. O desenvolvimento deste tipo de programa é possível graças à tecnologia ubíqua que pode ser entendida como um sistema que trata e realiza a fusão de dados heterogêneos ligados ao espaço e ao tempo em um processo dinâmico, com variação e atualização contínua em tempo real. (MESSIAS, 2011)

- ***O desafio está em definir os ditames legais e éticos para o compartilhamento destas informações, pois os avanços tecnológicos não esperam***

No âmbito do Sistema Único de Saúde, algumas normas definidas pelo Ministério da Saúde para programas de Telemedicina no SUS

encontram-se em vigor, porém, há que se estabelecer normas gerais para o desenvolvimento de softwares, com o uso de sistemas de segurança que garantam a privacidade, a integralidade, a confiabilidade e a atualidade das informações compartilhadas. Com relação ao comportamento dos usuários destes programas, caberá às instituições, através de suas políticas de segurança, estabelecerem os limites de uso e acesso considerando como princípio basilar de toda e qualquer determinação, o respeito à privacidade e à dignidade do paciente.

Considerações finais

O avanço tecnológico é irreversível, progrediremos à velocidade de nossa capacidade intelectual de abstração, ou seja, não há limites para esse processo. Assim, devemos ser agentes desse fenômeno tecnossocial, para analisá-lo criticamente e contribuir de forma consciente no desenvolvimento e implementação de medidas que visem à democratização digital com respeito ao direito de privacidade e à segurança da informação. Esses objetivos pode ser alcançados através de:

Política de segurança institucional da informação de saúde: a qual considere, além dos aspectos técnicos necessários para manutenção do sistema de registro eletrônico de saúde, também as questões ético-legais relacionadas à responsabilidade da instituição, bem como de seus colaboradores e usuários.

Programas de Educação tecnológica: oferecidos pela instituição de saúde, objetivando instrumentalizar o colaborador para uma participação cada vez mais consciente sobre os benefícios do uso adequado do sistema informatizado de saúde, questões de caráter técnico: conceitos básicos sobre operacionalização de sistemas, uso de aplicativos; questões legais: principais leis e normas relacionadas à informática em saúde, além de conceitos sobre cidadania digital e ética na manipulação de dados. Assim, o acesso às informações seria respeitado por ser compreendido e não apenas imposto, pois, o que sensibiliza, integra a realidade, traz mudança de comportamento e consciência de cidadania. A educação tecnológica em saúde deve buscar soluções para valorização do colaborador.

Comitês internacionais: os quais definam regras sobre o uso e o compartilhamento da informação eletrônica em saúde e normas de segurança, para o controle sobre a manipulação destas, onde a questão da territorialidade seja suplantada pela busca do entendimento global, haja vista ser uma questão que ultrapassa as barreiras físicas e interfere simultaneamente na vida política e social de todas as nações.

Portanto, é necessário considerar a interpretação do avanço tecnológico em saúde como fenômeno abrangente e irreversível onde os benefícios sociais sejam o principal elemento na implementação desse processo. Tecnologia e Sociedade caminham juntas, e alterações em uma delas transforma imediatamente a outra, como vimos através da história; os indivíduos são os agentes das revoluções e mudanças sociais. É a eles que a tecnologia deve servir, às mudanças coletivas, e não à individualização e à segregação social.

Avançar tecnologicamente com prudência, visando sempre o bem comum, o respeito ao ser humano e seu direito à segurança e privacidade, estes devem ser os objetivos dos sistemas de registro eletrônico em saúde, meio pelo qual pode-se alcançar a facilitação no processo de atendimento e a melhoria na qualidade de vida da população, sendo uma das formas inequívocas de se alcançar também a democratização digital.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT., **NBR ISO/IEC 27002.** Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005. Disponível em: <http://www.abntnet.com.br/ecommerce/default.aspx>. Acesso em: 5 abr. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ISO/IEC 17799** Tecnologia da Informação – Código de prática para a Gestão da Segurança da Informação. International Organization for Standardization, Switzerland, 2000. Disponível em: <http://www.e-services.com.br/portal/artigos/nbriso17799r1.pdf>. Acesso em: 2 abr. 2015.

ALBUQUERQUE JUNIOR, A. E. de; SANTOS, E. M. dos. Controles e práticas da segurança da informação em um Instituto de Pesquisa Federal. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA-SEGeT, 8., 2011. – 2011. Disponível em: <http://gpi.aedb.br/seget/artigos11/3414310.pdf>. Acesso em: 30 jan. 2015.

ASSOCIAÇÃO MÉDICA MUNDIAL – AMM. **Declaração de Tel Aviv. Responsabilidade e Normas Éticas na Utilização da Telemedicina**. 1999. Disponível em: <http://www.dhnet.org.br/direitos/codetica/medica/27telaviv.html>. Acesso em: 7 abr. 2015].

BASTOS, C. R. **Curso de direito constitucional**. 20.ed.atual. São Paulo: Saraiva, 1999.

BONAVIDES, P. A evolução constitucional do Brasil. **Estud. av.**, São Paulo, v. 14, n. 40, dez. 2000. Disponível em: < http://www.scielo.br/pdf/ea/v14n40/v14n40a16.pdf>. Acesso em: 2 abr. 2015.

BRASIL. Código Penal. Decreto-lei nº 2.848 de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del-2848compilado.htm>. Acesso em: 1 abr. 2015].

BRASIL. Código de Processo Civil. Lei nº 5.869 de 11 de janeiro de 1973. Institui o Código de Processo Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l5869compilada.htm>. Acesso em: 1 abr. 2015.

BRASIL. Senado Federal. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988. Organização do texto: Juarez de Oliveira. 4. ed. São Paulo: Saraiva, 1990. 168 p. (Série Legislação Brasileira).

BRASIL. Código de Defesa do Consumidor. Lei nº 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 2 abr. 2015.

BRASIL. Medida Provisória nº 2.200-2 de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 4 abr. 2015.

BRASIL. **Novo Código Civil**. Lei nº 10.403 de 10 de janeiro de 2002. Aprova o novo código civil brasileiro. Brasília, DF, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 1 abr. 2015.

BRASIL. Portaria nº 675/GM de 30 de março de 2006. Dispõe sobre os direitos e deveres dos usuários da saúde. Disponível em: <http://dtr2001.saude.gov.br/sas/PORTARIAS/Port2006/GM/GM-675.htm>. Acesso em: 2 abr. 2015.

BRASIL. Portaria MS nº 402 de 24 de fevereiro de 2010. Institui em âmbito nacional, o Programa de Telessaúde Brasil. Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2010/prt0402_24_02_2010.html>. Acesso em: 7 abr. 2015.

BRASIL. Agência Nacional de Saúde Suplementar. RN nº 255 de 18 de maio de 2011a. Disponível em: <http://www.ans.gov.br/index.php?option=com_legislacao&view=legislacao&task=TextoLei&format=raw&id=1750>. Acesso em: 8 abr. 2015.

BRASIL. Portaria nº 2.546, de 27 de outubro de 2011b. Redefine e amplia o Programa Telessaúde Brasil, que passa a ser denominado Programa Nacional Telessaúde Brasil Redes (Telessaúde Brasil Redes). Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2546_27_10_2011.html>. Acesso em: 7 abr. 2015.

BRASIL. Portaria GM nº 2.554 de 28 de outubro de 2011c. Institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: <http://old.cremerj.org.br/skel.php?page=legislacao/resultados.php> [Acesso em: 7 abr. 2015.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011d. Lei de acesso à informação. Disponível em: <http://www2.camara.leg.br/legin/fed/lei/2011/lei-12527-18-novembro-2011-611802-norma-pl.html>. Acesso em: 2 abr. 2015.

BRASIL. Decreto nº 7.724 de 16 de maio de 2012a. Regulamenta a Lei no 12.527, que dispõe sobre o acesso a informações. Disponível em: <http://www.governoeletronico.gov.br/biblioteca/arquivos/decreto-no-7-724-de-16-de-maio-de-2012-regulamenta-a-lei-no-12-527-que-dispoe-sobre-o-acesso-a-informacoes/view>. Acesso em: 8 abr 2015.

BRASIL. Agência Nacional de Saúde Suplementar RN nº 305 de 09 de outubro de 2012b. Disponível em: <http://www.ans.gov.br/index.php/index2.php?option=com_legislacao&view=legislacao&task=TextoLei&format=raw&id=2268>. Acesso em: 8 abr. 2015.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012c. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 7 abr. 2015.

BRASIL. Ministério da Saúde. Portaria GM. nº 3.127, de 28 de dezembro de 2012d. Altera dispositivos da Portaria nº 2.554/GM/MS, de 28 de outubro de 2011. Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2012/prt3127_28_12_2012.html>. Acesso em: 8 abr. 2015.

BRASIL. Portaria MS/GM nº 2.525 de 29 de outubro de 2013. Altera dispositivos da Portaria nº 2.554/GM/MS, de 28 de outubro de 2011, que institui, no Programa de Requalificação de Unidades Básicas de Saúde, o componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt2525_29_10_2013.html. Acesso em: 7 abr. 2015.

BRASIL. Marco Civil Regulatório da Internet. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 3 abr. 2015.

CAVALCANTE, W. F. Crimes cibernéticos: investigação e ameaças na internet. **Jus Navigandi**, Teresina,v.18, n.3782, 8 nov. 2013. Disponível em: <http://jus.com.br/artigos/25743>. Acesso em: 6 mar. 2015.

COHEN, C.; SEGRE, M. Definição de valores, moral, eticidade e ética. In: _____. **Bioética**. São Paulo, EDUSP, 1995. p.17.

CONSELHO FEDERAL DE ENFERMAGEM-COFEN. Resolução 311/2007. Aprova a Reformulação do Código de Ética dos Profissionais de Enfermagem. Disponível em: < http://www.cofen.gov.br/resoluo-cofen-3112007_4345.html>. Acesso em: 18 mar. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.638 de 09 de agosto de 2002a. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Disponível em: < http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>. Acesso em: 9 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.643 de 07 de agosto de 2002b. Define e disciplina a prestação de serviços através da Telemedicina. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1643_2002.htm>. Acesso em: 9 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.653 de 06 de novembro de 2002c. Demonstrações Cirúrgicas ao Vivo. Disponível em: < http://www.portalmedico.org.br/resolucoes/CFM/2002/1653_2002.htm>. Acesso em: 13 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.639 de 10 de julho de 2002d. Aprova as "Normas técnicas para uso de Sistemas Informatizados para a guarda e manuseio do prontuário médico", dispõe sobre tempo de guarda dos prontuários, estabelece critérios para certificação dos sistemas de informação e dá outras providências. Disponível em: < http://www.portalmedico.org.br/resolucoes/cfm/2002/1639_2002.htm>. Acesso em: 13 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.665 de 07 de maio de 2003. Dispõe sobre a responsabilidade ética das instituições e profissionais médicos na prevenção, controle e tratamento dos pacientes portadores do vírus da SIDA (AIDS) e soropositivos. Disponível em: < http://www.portalmedico.org.br/resolucoes/cfm/2003/1665_2003.htm>. Acesso em: 09 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.819 de 22 de maio de 2007a. Proíbe a colocação do diagnóstico codificado (CID) ou tempo de doença no preenchimento das guias da TISS de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde concomitantemente com a identificação do paciente e dá outras providências. Disponível em: < http://www.portalmedico.org.br/resolucoes/CFM/2007/1819_2007.htm>. Acesso em: 9 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.821 de 11 de julho de 2007b. 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 em: <http://www.sbis.org.br/indexframe.html>. Acesso em: 9 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.976 de 29 de setembro de 2011. Altera o parágrafo único do art. 1º da Resolução CFM nº 1.819, publicada no D.O.U. de 22 de maio de 2007, Seção I, p. 71, que proíbe a colocação do diagnóstico codificado (CID) ou tempo de doença no preenchimento das guias da Tiss de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde concomitantemente com a identificação do paciente, e dá outras providências. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2011/1976_2011.htm>. Acesso em: 9 abr. 2015.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução 1.997 de 18 de agosto de 2012. Código de Ética Médica. **Diário Oficial da União**, 16 ago. 2012, Seção1, p.149. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2012/1997_2012.pdf>. Acesso em: 18 mar. 2015.

CONSELHO FEDERAL DE MEDICINA. **Cartilha sobre prontuário eletrônico – a certificação de sistemas de registro eletrônico de saúde**. Brasília, D.F.:CFM/SBIS, 2012. Disponível em: <http://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf>. Acesso em: 12 fev. 2015.

CONSELHO REGIONAL DE MEDICINA DE SÃO PAULO – CREMESP. **Missão, visão e valores: Juramento de Hipocrátes**. Disponível em: <http://www.cremesp.org.br/?siteAcao=Historia&esc=3>. Acesso em: 20 de fev. 2015.

CONSELHO REGIONAL DE MEDICINA PARANÁ-CRM-PR. Resolução CRM-PR nº 89 de 28 de fevereiro de 2000. Disponível em: < http://www.portalmedico.org.br/resolucoes/CRMPR/resolucoes/2000/89_2000.htm>. Acesso em: 8 abr. 2015.

FORTES, P.A.C. **Ética e Saúde - Questões éticas, deontológicas e legais. Tomada de decisões, autonomia e direitos do paciente:** estudos de casos. São Paulo: EPU; 1998.

GOLDIN, J. R.; FRANCISCONI, C. F. **Bioética e informação.** Porto Alegre**,** 2004. [aula]. Disponível em: <http://www.ufrgs.br/bioetica/bioinfo.htm>. Acesso em: 25 fev. 2015.

HAUGHN, M.; GIBILISCO, S. Confidentiality, integrity and availability (cia triad). 2014. Disponível em: <http://whatis.techtarget.com/definition/confidentiality-integrity-and-availability-cia>. Acesso em: 27 jan. 2015.

HEALTH Insurance Portability and Accountability Act of 1996. Public Law 104-191 104th Congress. Disponível em: < http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf>. Acesso em: 9 abr. 2015.

ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341>. Acesso em: 7 abr. 2015.

LABRADBURY, L. C. S. Estados liberal, social e democrático de direito: **Revista Jus Navigandi**, Teresina, v.11, n.1252, 5 dez. 2006. Disponível em: <http://jus.com.br/artigos/9241>. Acesso em: 9 abr. 2015.

LOWY, M. Lucien Goldmann ou a aposta comunitária. **Estud. av.**, São Paulo, v. 9, n. 23, abr. 1995. Disponível em: <http://www.scielo.br/pdf/ea/v9n23/v9n23a12.pdf.>. Acesso em: 9 abr. 2015.

MAGALHÃES, J.L.Q. de. **Direitos Humanos**: evolução histórica. Enciclopédia Digital de Direitos Humanos; 2007. Disponível em: <http://www.dhnet.org.br/direitos/anthist/jose_quadros.htm>. Acesso em: 14 nov. 2014.

FERRAZ, A.S.;MESSIAS, D.J S. **Computação Ubíqua**. Pernambuco: Universidade Federal de Pernambuco, 2011. 5p. Disponível em: <http://www.folhadointerior.com.br/v2/page/noticiasdtl.asp?t=UFF+DESENVOLVE+SISTEMA+PARA+MONITORAMENTO+%C0+DIST%C2NCIA+DE+PACIENTES+EM+SEUS+DOMIC%CDLIOS&id=19348>. Acesso em: 9 abr. 2015.

PFAFFENSELLER, M. Teoria dos direitos fundamentais. **Rev. Jur.,** Brasília, v. 9, n. 85, jun./jul, 2007. Disponível em: http://www.planalto.gov.br/ccivil_03/revista/Rev_85/artigos/MichelliPfaffenseller_rev85.htm. Acesso em: 19 nov. 2014.

TKOTZ, V. **Criptografia – segredos embalados para viagem**. São Paulo: Novatec, 2005.

TREVISAN, A. C. Papel ou arquivo eletrônico?. **Revista Jus Navigandi**, Teresina,v.9, n.482, 1 nov. 2004. Disponível em: <http://jus.com.br/artigos/5850>. Acesso em: 9 abr. 2015.

UNITED NATION EDUCATIONAL SCIENTIFIC AND CULTURAL ORGANIZATION-UNESCO DO BRASIL. **Declaração universal dos direitos humanos**. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 16 fev. 2015.

VITORINO, A. J.; COSTA, R. H. da; KENCHIAN, M. R. B. **Política de segurança em tecnologia da informação na saúde**: modelo corporativo aplicado no HCFMUSP. 2011. Disponível em: <http://www.sbis.org.br/cbis11/arquivos/818.pdf>. Acesso em: 13 fev. 2015.

11

Segurança de transferência de dados em Telessaúde e Telemedicina

Felipe Rodrigues Martinez Basile[1]
Marcel Thomé Filho[2]
Flávio Cézar Amate[3]
Robson Rodrigues da Silva[4]
Silvia Helena Bastos de Paula[5]
Daniel Gustavo Goroso[6]

Introdução

A indústria de telefonia móvel cresceu em ritmo acelerado nas duas últimas décadas. A Internet móvel é um mercado em desenvolvimento e com potencial de crescimento exponencial desenvolvida na plataforma da rede celular, representando novo modelo de negócios para operadores do sistema e maior comodidade ao usuário. A transmissão de dados pela rede de telefonia móvel é uma demanda do mercado suportada por

1 Felipe Rodrigues Martinez Basile é graduado em Sistemas de Informação e Doutor em Engenharia Biomédica pelo Núcleo de Pesquisas Tecnológicas da Universidade Mogi das Cruzes.
2 Marcel Thomé Filho é graduado em Sistemas de Informação/Universidade Santa Ana, Mestre pelo Centro Universitário Ibero-Americano e Doutorando em Engenharia Biomédica pelo Núcleo de Pesquisas Tecnológicas da Universidade Mogi das Cruzes.
3 Flávio Cézar Amate é Matemático/CURP, Pós-Doutorado pela UFSC e Pesquisador do Núcleo de Pesquisas Tecnológicas da Universidade Mogi das Cruzes.
4 Robson Rodrigues da Silva é Bacharel em Matemática pela UMC, Doutor em Engenharia Biomédica pelo NPT/UMC e Pesquisador do Núcleo de Pesquisas Tecnológicas da Universidade Mogi das Cruzes.
5 Silvia Helena Bastos de Paula é graduada em Enfermagem, Doutora em Ciências e Pesquisadora Científica (PqC III) do Núcleo de Investigação em Políticas e Práticas de Saúde do Instituto de Saúde da Secretaria de Estado da Saúde de São Paulo.
6 Daniel Gustavo Goroso (danielg@umc.br) é Físico pela UNT, Argentina, Doutor em Engenharia Biomédica / Politécnica/USP e Pesquisador do Núcleo de Pesquisas Tecnológicas da Universidade Mogi das Cruzes.

tecnologia. Nesse contexto, mercado e tecnologia se complementam e se desafiam a um só tempo. O mercado exigiu e a tecnologia transformou a Internet tirando-a do espaço limitado e estático de escritórios para o mundo sem fronteiras da mobilidade, criando a Internet móvel. A rede de telefonia móvel surgiu como solução para serviços de voz, porém, para atender à demanda de acessos e serviços, entre eles os serviços de Telessaúde e Telemedicina, evoluiu em capacidade, qualidade, abrangência e padrões passando a oferecer tráfego de dados em alta velocidade, tornando-se o maior suporte em infraestrutura terrestre para a Internet móvel, em transporte e conexão com a rede pública de dados e, como todo dado que circula pela Internet, está exposta aos riscos de ataques que podem afetar a segurança dos dados em trânsito. A segurança na rede móvel é tratada ao longo do percurso de uma conexão envolvendo as interfaces físicas e lógicas, e ao utilizar os recursos de protocolos específicos e de criptografia, assegura a mesma segurança dada nas redes de computadores e na Internet convencional. A arquitetura da rede provê segurança na interface entre rede móvel pública terrestre e a rede de conjuntos de dados. Desse modo, a segurança na Internet fica a cargo dos provedores de acesso e fornecedores de conteúdos. Neste capítulo pretende-se apresentar quais são as consignas que se deve considerar na transferência de dados utilizados por fornecedores de serviços de Telemedicina e Telessaúde sob aspectos ético e legal. O primeiro parágrafo apresenta ao leitor na descrição os conceitos de Telemedicina e Telessaúde. Na sequência se aborda os aspectos ético-legais e o parágrafo seguinte apresenta um estado da arte no contexto brasileiro. Logo depois, é apresentado o uso de sistemas de monitoramento e aplicativos instalados em telefones celulares, uma vez que a tendência dos serviços de Telemedicina e Telessaúde segue esse caminho. Finalmente são apresentadas as considerações finais.

Tecnologia e Saúde integradas pela Telemedicina e Telessaúde

A Telemedicina e Telessaúde representam novas opções na assistência à saúde das pessoas. Esta constatação é feita pela observação da

ascendente utilização de novas Tecnologias da Informação e Comunicação (WHO, 2010).

As origens da Telemedicina remontam ao início do século passado, em 1906, com Willem Einthoven (1860-1927), fisiologista holandês (prêmio Nobel de Medicina e Fisiologia em 1924), que inventou um galvanômetro de mola que levou ao eletrocardiograma. Durante a 1ª Guerra Mundial, em 1916 e nos anos seguintes, o rádio foi utilizado para permitir a comunicação entre médicos de estações costeiras ou nas frentes de batalha, com hospitais de campanha ou navios em busca de apoio e informações logísticas.

A telemedicina teve impulso a partir da Declaração de Tel Aviv, Israel, em 1995 – 51ª Assembleia Geral da Associação Médica Mundial – (AMM,1999;WMA,2014) e, com suas recomendações, o Brasil definiu normas específicas para instituição e utilização dessa tecnologia. Hoje em dia o uso da telemedicina se espalhou rapidamente e está agora integrado nas atividades de hospitais, departamentos especializados de saúde, serviços móveis de atenção de urgência e remoção, consultórios médicos privados, na saúde domiciliar pública e privada.

O termo telessaúde se refere de forma ampla à assistência médica remota que nem sempre envolve serviços clínicos. A telemedicina é a utilização de tecnologias de telecomunicações e informação, a fim de prestar cuidados de saúde clínicos à distância por meio de informações médicas enviadas de um site para outro site através de comunicações eletrônicas. A telemedicina inclui variedade cada vez maior de aplicativos e serviços que utilizam diversos meios – vídeo, e-mails, telefones inteligentes, tecnologias sem fio e outras formas de tecnologia de telecomunicações.

A telemedicina ajuda a eliminar as barreiras da distância e pode melhorar o acesso a serviços médicos, que, muitas vezes, não estariam disponíveis de forma consistente em comunidades rurais ou distantes de áreas com infraestrutura de serviços de saúde. A telemedicina está intimamente ligada à tecnologia da informação de saúde e é a tecnologia de informação mais aplicada aos registros médicos eletrônicos e sistemas de informação em saúde e documentos relacionados.

A telemedicina refere-se à entrega efetiva dos serviços clínicos remotos usando tecnologia, e abrange ampla definição de cuidados de saú-

de à distância: consultas a paciente por meio de videoconferência, transmissão de imagens fixas, e-saúde, incluindo portais de pacientes, monitoramento remoto de sinais vitais, educação médica continuada, aplicações sem fio focadas no consumidor e *call centers* de enfermagem, entre outras aplicações. Todos esses recursos são considerados parte de Telemedicina e Telessaúde.

O uso de modernas tecnologias interativas e de telecomunicações tem importância significante para o desenvolvimento de novas soluções, que aumentem a eficiência na assistência à saúde (CHAO, 2013), por meio da integração entre a área da informática com a área da saúde.

Telessaúde e Telemedicina: abordagem ético-legal

A Associação Americana de Telemedicina (ATA, 2015) usa os termos Telessaúde e Telemedicina como sinônimos, considerando que Telemedicina não é por si mesma uma especialidade médica, e adota protocolos por área de especialidades. Nos Estados Unidos da América está em vigor o Código Eletrônico de Regulamentos Federais, que trata da troca de informações eletrônicas em saúde, pelo HIPAA (*Health Insurance Portability and Accontability Act*) (HIPAA,1996), que estabelece procedimentos de proteção à privacidade no uso e divulgação da informação e acesso por parte de terceiros.

A utilização de tecnologia requer reflexão sobre aspectos éticos de equidade, justiça e autonomia dos sujeitos, e seus efeitos beneficentes e danos possíveis, que incluem quebra de sigilo e violação de privacidade de informações pessoais.

No Brasil, o Ministério da Saúde regulou essas áreas pela Portaria de 2.546 de 27 de outubro de 2011(BRASIL, 2011a), que amplia o Programa de Telessaúde Brasil e cria o Programa Nacional de Telessaúde Brasil Redes e pela Portaria do Ministério da Saúde nº 2.554 de 28 de outubro de 2011(BRASIL, 2011b), que "Institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes". Estas normas foram alteradas pelas Portarias MS/

GM nº 3.127 de 28 de outubro de 2012 (BRASIL, 2012) e nº 2.525 de 29 de outubro de 2013 (BRASIL, 2013).

Ademais, tem vigência na Agência Nacional de Saúde Suplementar - ANS a Resolução Normativa nº 72 de 24 de março de 2004 (BRASIL, 2004), que instituiu o Programa de Transmissão de Arquivos – PTA e regulamentou a transmissão dos arquivos de dados de todos os sistemas que não possuírem mecanismo de envio próprio entre Operadoras de planos privados de assistência à saúde.

Para Berlinguer (1993), o progresso da biomedicina pode ser um dos fatores de aprofundamento das desigualdades nos sistemas de saúde. A inclusão de maior número possível de pessoas, sempre que seja útil para elas, é uma questão crítica a ser colocada a governantes e gestores de setores de produção e incorporação tecnológica, sobretudo na área da saúde, na qual o princípio da universalidade deve ser considerado para reduzir desigualdades e exclusão de acesso. Para adoção dessas tecnologias é necessário instituir aparato administrativo, legal e normativo, que previna e detecte abusos na utilização de tecnologias e promovam vigilância constante para detectar ações maliciosas em função de lucros ou manipulações de informações.

Telessaúde e Telemedicina no Brasil

No país, o desenvolvimento da Telemedicina e Telessaúde ocorre com ações permanentes e importantes – tanto do Ministério da Saúde quanto de esferas estaduais e municipais e de instituições públicas e privadas, além de hospitais de referência como: Hospital Alemão Oswaldo Cruz (HAOC), Hospital do Coração (HCor), Hospital Israelita Albert Einstein (HIAE), Hospital Sírio-Libanês (HSL), além de núcleos universitários em telemedicina e telessaúde espalhados por todo o país, formando redes de colaboração – tanto pela Rede Nacional de Pesquisa (RNP) quanto pela Rede Universitária de Telemedicina (RUTE, 2015).

A disciplina de Telemedicina, do Departamento de Patologia do Sistema da Faculdade de Medicina da Universidade de São Paulo (USP) e Hospital das Clínicas (FMUSP-HC), tem desenvolvido projetos que utili-

zam tecnologias interativas para melhorar a assistência à saúde: projetos como Jovem Doutor, Homem Virtual e a Estação Digital Médica (EDM) tornam possível o envolvimento da comunidade com as equipes multiprofissionais em saúde na educação, na assistência e em pesquisas multicêntricas (CHAO, 2012).

O meio ambiente computacional de apoio à prática clínica é um dos exemplos de propostas de soluções que utilizam recursos da informática para os cuidados da saúde (CHAO, 2000). O ambulatório virtual (Cyberambulatório) é outro exemplo de apoio ao diagnóstico clínico de teleassistência na área médica de dermatologia, demonstrando a integração de especialistas que estão em lugares distantes (CHAO, 2003a).

Outros importantes ambientes computacionais, como o sistema funcional de interconsulta dermatológica à distância e via Internet (MIOT, 2005), o ambulatório de oftalmologia (TALEB et al., 2005), o curso de extensão universitária em hanseníase (rede de detecção de casos e diagnósticos) (PAIXÃO et al., 2009), além do website voltado à microbiologia clínica (ROSSI et al., 2002), assim como, também ambientes voltados às práticas cirúrgicas (BERNARDO et al., 2004); e ambientes desenvolvidos para estudos de nutrição (SIGULEM et al., 2001).

Existem trabalhos na literatura que tratam da repercussão da telemedicina e telessaúde em conjunto com novas tecnologias da informação e comunicação (TIC), muitas vezes comparadas à educação da medicina clássica (ROSSARO et al., 2007), com a aplicação de novas estratégias na assistência à saúde utilizando a telemedicina e telessaúde quando a distância é um fator importante (CHAO et al., 2003b; ANDREAZZI et al., 2011; SANTOS et al., 2011; SKELTON-MACEDO et al., 2013).

Muitos desses meios ambientes de saúde utilizam-se não somente de estruturas computacionais fixas locais, mas também de tecnologias móveis como alternativa para potencializar o cuidado da saúde dos pacientes com mobilidade. Algumas pesquisas apontam que nos próximos 5 anos, ao considerar um índice de crescimento anual no mercado de *smartphones* de 25%, as vendas desses dispositivos móveis devem alcançar um número muito significante atingindo mais de 1 bilhão de vendas até 2017 (OVUM, 2012).

Atualmente o Brasil é considerado o 5º maior mercado de *smartphones* no mundo, fato que pode ser justificado, de certo modo, pela mudança de paradigma em relação ao uso desses dispositivos em países emergentes, pois a população desses países incorporam esses dispositivos em suas vidas, de maneira que esses telefones inteligentes proporcionem acesso a redes sociais, entretimento e negócios (IDC, 2012).

Ao analisar o aumento da capacidade de conexão com o uso das novas TIC, observa-se a utilização intensiva da transmissão de informações digitais. Nesse sentido existem previsões para os próximos anos de que o tráfego de *Internet Protocol* (IP) crescerá 20% ao ano até 2016 (CISCO, 2012), o que pode trazer preocupações:

- em relação à capacidade dos meios de transmissão e infraestruturas de rede em servir de maneira adequada as requisições;
- em relação ao número extraordinário de conexões entre recursos ativos de rede que serão feitas.

Como consequência do aumento dessa capacidade de conexão nota-se diversas ameaças virtuais que atingem os mais diferentes sistemas computacionais. No Brasil, na primeira década do século 21, houve um aumento significante no número de incidentes relacionados à segurança da informação por meio de: *worms* (processos automatizados de propagação de códigos maliciosos na rede), invasão, negação de serviço web (ataques que intentam o comprometimento de servidores e desconfigurações de páginas na Internet), *scan* (varredura de portas com o propósito de verificar quais portas utilizadas por programas estão ocupadas e livres) e fraude (CERT.BR, 2012). É importante destacar nesse contexto que existem evidências de que muitos desses vírus, classificados como *malwares*, infiltram-se nos dispositivos móveis por meio de aplicativos falsamente tipificados como *games* (SYMANTEC, 2012).

Estudos na literatura mostram a necessidade do desenvolvimento de outros métodos para segurança da informação diante das mais recentes ameaças que atingem ambientes computacionais no exercício da telemedicina e telessaúde (NOBRE et al., 2007; KOBAYASHI; FURUIE, 2006, 2007; KANTER et al., 2009; BASILE; AMATE, 2011; EL EMAM et al., 2011; MARTINÊZ; AMATE, 2011). A World Medical Association (WMA), desde

1999, frisa a necessidade de consenso internacional para o estabelecimento de estruturas tecnológicas adequadas para transmissão de dados médicos (WMA, 2014). No Brasil, tanto a Associação Médica Brasileira (AMB), quanto o Conselho Federal de Medicina (CFM) por meio de resoluções como a do CFM nº 1.821/2007(CFM,2007), com a Sociedade Brasileira de Informática em Saúde (SBIS), promovem discussões ressaltando a necessidade da adoção de mecanismos de segurança capazes de garantir autenticidade, privacidade e integridade das informações em saúde.

Aproximadamente 52% das aplicações móveis em saúde no Brasil não têm a instituição de mecanismos seguros para exercício da telemedicina, o que podem ocasionar, em futuro próximo, problemas na garantia de aspectos da segurança da informação no contexto da área médica (IWAYA et al., 2013). A utilização do protocolo *Hyper Text Transfer Protocol Secure* (HTTPS) era considerada uma medida eficaz para execução da segurança digital quanto à privacidade dos dados. Em 2014, o ataque *Heart Bleed* mostrou a vulnerabilidade do HTTPS no vazamento de informações confidenciais. O que pode ter comprometido milhares de aplicações em *internet banking, e-commerce* e aplicações de Telemedicina e Telessaúde. As consequências deste fato são graves porque informações em saúde precisam ser resguardadas em razão dos princípios de privacidade, confidencialidade e integridade (KOBAYASHI; FURUIE, 2006, 2007).

Por isso, há necessidade da continuidade de pesquisas que apresentem opções para instituição de segurança digital para meios ambientes computacionais em Telemedicina e Telessaúde 3.0., que sejam inovados com o uso de serviços à distância, com apoio de Segunda Opinião Especializada à Distância e Interconsulta Multiprofissional e de núcleos técnicos científicos dedicados à Atenção Primária, através do processo de Referência e Contrarreferência, bem como a criação do *e-Care* e humanização para apoio domiciliar ao *Telehomecare* e telecuidado.

No Brasil, as operadoras de telefonia celular usam, entre outros, o sistema global para comunicações móveis (GSM) com cobertura em frequências de 900 MHz a 1800 MHz e o *General Packet Radio Service* (GPRS) ou serviço de rádio de conjunto geral, que é extensão do serviço GSM de conjuntos de dados enviados através da atribuição de canais de rádio para os usuários somente quando se precisa enviar dados. O GPRS

pode oferecer velocidades de até 171,2 Kbps e é empregado pela maioria de usuários em uma rede GSM.

Para a concepção de arquitetura orientada a serviços é necessário converter os requisitos do usuário (rede de telemedicina) e o cliente (paciente) em produtos instaláveis em qualquer plataforma lógica (código aberto), com as fases da análise de cada requisito, definição da arquitetura do microcomputador, aplicação de engenharia (princípios e métodos) para testar o serviço proposto e para garantir a portabilidade, a interoperabilidade e a segurança do serviço.

No contexto brasileiro, os sistemas de saúde devem instituir outras formas de expansão para os serviços de bem-estar em suas políticas de inclusão social, e foram encontrados nas TIC elementos e instrumentos de mudança tecnológica, que tornam possível oferecer modelos de monitoramento de serviços a pacientes em diferentes situações da vida cotidiana e assim atingir a continuidade no processo de reabilitação fora do centro médico. No entanto, estas tecnologias exigem compatibilidade entre redes de comunicação diferentes que permitam aplicar os conceitos de globalidade e interoperabilidade quanto à maioria das organizações de saúde.

Os celulares e sistemas de monitoramento: segurança na rede móvel

O potencial tecnológico da rede de telefonia móvel é resultado da padronização dos sistemas por meio de protocolos abertos que criam um sistema móvel global (Global Mobile System - GSM). O modelo global de telefonia móvel dá potência à rede em abrangência e capacidade de transmissão de dados. Com acesso à Internet por telefones móveis, um novo segmento de rede é integrado à Internet: a *Wireless Web Phone*. A Internet móvel é sustentada por vários pilares: a mobilidade - necessária aos profissionais que estão em constante movimento e cuja atividade demanda comunicação em tempo real como vendedores, por exemplo, a transformação das características de várias atividades que podem ser levadas ao cliente sem a presença necessária de uma pessoa; o fornecimento de extratos bancários; novos modelos de negócios já desenvol-

vidos para esse fim, como a venda de produtos e serviços e a própria Internet convencional, e em caso particular, a transferência de dados clínicos (p.e: dados fisiológicos de um paciente) por meio de aplicativos e sistemas de monitoramento, entre tantos. Contudo, existem adversidades e futuro incerto. Independentemente das adversidades e do futuro desconhecido, o uso da Internet móvel no Brasil cresce vertiginosamente. A cada dia instituições em todas as áreas do setor produtivo e do conhecimento, de todos os portes, e consumidores de varejo, aderem ao uso de dispositivos móveis para ter acesso à Internet. E, na perspectiva de tendência de consumo em massa, surge a preocupação como um elemento indispensável na troca de dados na Internet, sobretudo nas comunicações sem fio, como a telefonia móvel: a segurança do conteúdo. A segurança dos dados transmitidos pela Internet é um duelo permanente entre desenvolvedores de soluções e invasores de sistemas. A segurança é elemento preponderante na transmissão de dados em todos os segmentos. No segmento corporativo estabelece diferencial competitivo, bem de valor e instrumento de sobrevivência, exigindo cuidados ainda maiores. No caso de transmissão de dados fisiológicos, como ocorre no Sistema de Monitoramento On-line de Sinais Fisiológicas (GOROSO et al, 2013), os dados de frequência cardíaca e dados pessoais do paciente precisam ser protegidos da mesma maneira tal qual se protege a conta bancária dos usuários.

As técnicas utilizadas nos telefones celulares até a segunda geração não são suficientes para evitar a clonagem dos terminais. O modelo GSM e seu desenvolvimento, até então, apresentam-se como seguros contra roubo nas autenticações, e os algoritmos de criptografia utilizada na transmissão da informação digitalizada são robustos e eficientes contra os ataques. Tais recursos, no que diz respeito à transmissão dos dados, conferem elevado grau de segurança. Como os ataques a uma rede variam em sua importância, indaga-se: a transmissão de dados via telefonia móvel é segura? Outros trabalhos já trataram da segurança na transmissão de dados pela rede móvel explorando as técnicas de segurança no modelo WAP em suas versões 1.X e 2.0. As matérias encontradas na Internet e na literatura especializada apontam pontos vulneráveis nas versões anteriores ao WAP 2.0. Com o advento da transferência de dados

em pacotes usando a rede GPRS/EDGE disponível pelo padrão GSM, as ameaças e riscos tornam-se maiores por causa do maior fluxo de dados e o uso em maior escala do novo modelo. Nesse sentido, este parágrafo tenta explorar a existência de pontos vulneráveis e os respectivos mecanismos de proteção contra invasões na rede móvel. Especificamente, buscam-se conhecer a arquitetura e infraestrutura da rede de telefonia celular, as tecnologias disponíveis para a transmissão de dados e as interfaces com a rede pública de dados, os tipos de ataques e as políticas de segurança e defesa.

A arquitetura GPRS apresentada por Sverzut (2005) é o modelo genérico de qualquer rede móvel que disponibilize serviços de dados. Baseado nesse modelo, fornecedores de hardware e software desenvolveram equipamentos e protocolos capazes de garantir a segurança em transmissão de dados fim a fim pela rede de telefonia celular. Por medida de segurança e/ou estratégia de negócios, as operadoras não costumam divulgar a topologia da rede de dados que operam, mas a variedade topológica decorre de facilidades e contingência operacional. Quando se considera a arquitetura da rede isoladamente, a segurança se aplica em dois segmentos: na interface física ou aérea, formada pelos canais de rádio frequência, e na interface lógica formada pelos protocolos utilizados nas conexões entre os diferentes elementos de rede. Considerando que uma transmissão de dados por comutação de pacotes pode envolver a rede de dados (PDN) e a Internet, a segurança é necessariamente tratada ao longo do percurso envolvido entre origem e destino dos dados. Na percepção de Taurion (2002), a Internet móvel está exposta às mesmas condições de riscos da rede convencional, acrescida de vulnerabilidades existentes nas interfaces aéreas e demais elementos que constituem a rede. Outro ponto de vulnerabilidade é a exposição ao ambiente do usuário de um dispositivo móvel e o uso de tecnologias de conectividades geralmente utilizadas para facilitar o conforto durante os acessos. No modelo de estrutura de rede utilizada, o suporte tecnológico para a segurança na rede móvel está disponível em todos os estádios quando há risco iminente de violação ou acesso indevido aos dados, quando se utiliza protocolos e algoritmos de criptografia seguros, porém os riscos de invasão de privacidade não se dão apenas por falhas de tecnologia,

como também pelos métodos utilizados na rede convencional, como, por exemplo, a engenharia social. Na rede móvel existem outras fragilidades que podem contribuir para insegurança do conteúdo, como maior exposição, perda do dispositivo, etc., mas esses pontos não estão relacionados com a tecnologia em si.

Segurança na interface aérea de uma rede GSM consiste em autenticar as unidades móveis contra uso indevido e na proteção dos dados durante a transmissão pela rede sem fio. Num tutorial sobre segurança, Melo (2006) afirma que a autenticação está relacionada à clonagem de aparelhos e não à segurança dos dados em si, consistindo, portanto, da identificação do terminal móvel na interface aérea e do usuário. Esse processo não garante a autenticidade dos dados transmitidos, a menos que numa possível clonagem de um *chip* ou um cartão de memória de um aparelho GSM sejam levadas informações confidenciais como senhas ou outros dados sigilosos do usuário. A segurança dos dados é garantida pelo uso de algoritmos de criptografia que impedem conhecer os dados, caso os sinais de radiofrequência sejam captados e decodificados. Segundo Sverzut (2005), o esquema de modulação usado na rede GSM pode ser a GMSK (Gaussian Minimum Shift Keying) ou a 8-PSK (8-Phase Shift Keying). A mais utilizada é a GMSK. Existem duas especificações para o sistema: CDPD (Cellular Digital Packet Data) e a Mobitex. A CDPD utiliza o tempo vago nos canais para transmitir os pacotes de dados dentro dos canais de voz. Com isso consegue-se alto índice de transferência, porém corre o risco de interrupção abrupta caso o sistema tenha elevado tráfego de dados.

Da perspectiva de segurança dos pacotes eminentemente de dados, os esquemas de modulação não têm mecanismo de proteção. Porém, o processo de transmissão requer transceptores operando em sincronismo, o que, de certo modo, dificulta a captação de dados de modo clandestino. Segundo Gomes (1985), o processo de transmissão de um sinal digital exige que o dado recuperado no destino seja idêntico ao dado enviado na origem. Vários algoritmos são utilizados para recuperar o dado transmitido como algoritmos de detecção e correção de erros, e no grau mais baixo, algoritmos para detecção do dado e nível de decisão que é necessário por causa da variedade que ocorre durante a transmissão pela interface

aérea podendo ocorrer interferências, atenuação ou outros efeitos que provocam desvanecimento do sinal, etc.

Com as alterações ocorridas no sinal modulado pode ocorrer que os níveis de tensão referente a um bit de dados seja atenuado e que outro bit seja amplificado criando uma área de conflito para identificação na recepção. O algoritmo de decisão não é uma técnica de segurança, porém precisa de parâmetros que torne o sinal recebido idêntico ao que foi transmitido. Tal necessidade dificulta a recuperação do sinal feita por um equipamento que não esteja parametrizado de acordo com o equipamento de recuperação definido. As técnicas de modulação e de modulação utilizadas na transmissão de dados por um sistema sem fios cuidam especificamente da proteção no que diz respeito à autenticidade dos dados transmitidos, ou seja, garantir que uma sequência de dígitos entregue na origem tenha recuperação idêntica. Técnicas de divisão de tempo e divisão de código (TDMA e CDMA) são as mais utilizadas pelas operadoras de celular e não se encontrou registro de danos causados por captação de sinal. O mais comum são ações de fraudadores no sentido de sabotar o sinal ao utilizarem sistemas transmissores de alta potência, na frequência utilizada pelas operadoras. De acordo com Melo (2006), a princípio, todo sinal de rádio frequência está sujeito à captação, bastando para isso que o interessado disponha de equipamentos capazes de sintonizar a frequência e decodificar e, consequentemente, interpretar os dados e transformá-los em informação. A interpretação dos dados depende da capacidade do invasor em quebrar os métodos de segurança utilizados. É possível inserir privacidade nos sistemas celulares e todas as prestadoras de serviços utilizam padrões de criptografia para evitar escuta de mensagens dos usuários (voz e dados) e nas mensagens de sinalização inerentes ao sistema. Os mecanismos de segurança são ajustados entre os elementos de rede antes do início da transmissão que definem quais regras de criptografia serão empregadas. Segundo Burnett (2002), as regras de criptografia utilizam chaves públicas e privadas em que somente as partes envolvidas conhecem os parâmetros utilizados que decodificam a informação. Aos demais, a menos que rompa a criptografia, os dados são imperceptíveis ou são recuperados de forma errada.

Considerações finais com críticas quanto à segurança nas transferências

O estudo de ameaças, segurança em transmissão de dados e Internet pela rede de telefonia móvel envolveu todos os elementos relacionados com o tema proposto. Procurou-se mostrar o conjunto de tecnologias que se somam à rede de telefonia móvel para tornar possível a mobilidade na Internet. A rede de telefonia móvel celular, como meio de acesso e veículo de transporte de dados de usuários, está exposta a qualquer ameaça que pode ocorrer numa rede de computadores, consequentemente na Internet convencional, acrescidos dos riscos peculiares aos sistemas de transmissão sem fio, convencionado chamar-se de interface aérea. O tratamento na interface aérea é dedicado à confiança da informação quando são feitas a detecção e a correção dos erros dos pacotes de dados que modulam a portadora de radiofrequência. A autenticação da estação móvel, um procedimento de segurança inerente à interface aérea, tem o propósito de proteger o usuário de clonagens nos aparelhos de tecnologias vulneráveis a essa prática.

Em sistemas GSM, o controle de acesso é feito pelo módulo de identificação do usuário. As interfaces lógicas funcionam como túneis de tráfego de dados entre elementos de uma intrarrede, inter-redes e entre uma rede móvel e a rede pública de dados, estão expostas a ataques de invasores ou usuários mal-intencionados, porém dispõem de tratamento de segurança por meio de protocolos e de *firewalls*. A transmissão de dados fim a fim, ou seja, do dispositivo móvel ao destino final é suportada pelo protocolo IP, que apresenta pontos frágeis em relação à segurança, porém a integridade e a autenticidade dos dados são asseguradas por algoritmos de criptografia confiáveis. As características técnicas e de operação de alguns dispositivos móveis, como os telefones celulares e assistentes digitais pessoais, que dispõem de pouca capacidade de armazenamento e geralmente trabalham com a conexão GPRS na condição quando necessário e com IP dinâmico, põem esses elementos de redes em situação privilegiada no que diz respeito às práticas de *fingerprinter* comum aos ataques em redes IP, haja vista a inexistência de sistemas operacionais

de grande porte nesses acessórios. As técnicas de enumeração estariam associadas à identificação dos hábitos de usuários, incluídas a utilização de tecnologias de conexão entre aparelhos celulares, tablets e notebooks. Como qualquer rede de transmissão de dados, os serviços de GRPS/ EDGE e WAP disponíveis pela rede de telefonia móvel celular estão sujeitos a ataques. Entretanto, o modelo operacional da rede e o tratamento inerente à segurança dos dados que por ela trafegam permitem concluir tratar-se de um serviço confiável, porém, em face do crescimento do uso, o volume e a importância dos dados transmitidos requerem aperfeiçoamento dos mecanismos de proteção e vigilância contínua.

Agradecimentos

Os autores FRMB e MTF agradecem o apoio financeiro da CAPES, respectivamente. Os professores RRS, FA e DGG agradecem o apoio da FAEP para a elaboração deste manuscrito.

Referências

ANDREAZZI, D. B.; ROSSI, F.; WEN, C. L. Interactive Tele-Education Applied to a Distant Clinical Microbiology Specialization University Course. **Telemedicine and e-Health,** v.17, n.7, p. 524-529, 2011.

ASOCIACION MEDICA MUNDIAL (AMM). **Recopilación de Comentarios a la Revisión Propuesta de la Declaración de Helsinki de la AMM**. Tel Aviv: Asociación Médica Mundial, 1999. (mimeo.)

AMERICAN TELEMEDICINE ASSOCIATION-ATA. ATA Standards and Guidelines. Disponível em: <http://www.americantelemed.org/resources/telemedicine-practice-guidelines/telemedicine-practice-guidelines#.VTEpxvnIaRM>. Acesso em: 2 fev. 2015.

BASILE, F. R. M.; AMATE, F. C. Secure Transmission of Medical Imagesby SSH Tunneling. In: International Conference on Human-Computer Interaction, 14., Florida, 9-14 july, 2011. Posters Extended Abstracts. v. 173. 486490.

BERLINGUER, G. **Questões de vida**. **Ética, Ciência, Saúde.** Tradução, M. Orrico, M. Porru e Shirley M. Gonçalves. Rev. José Rubens de Alcântara Bomfim. Salvador: APCE, São Paulo: Hucitec, Londrina: Cebes, 1993.

BERNARDO, V.; RAMOS, M.P.; PLAPLER, H. et al. Web based learning in undergraduate medicaleducation: development and assessment of an online course on experimental surgery. **Int J MedInform**. v.73, n. 9-10, p.731-42, set. 2004.

BRASIL. Agência Nacional de Saúde Suplementar. RN n° 72, de 24 de março de 2004. Dispõe sobre a instituição do Programa de Transmissão de Arquivos – PTA, entre Operadoras de planos privados de assistência à saúde e a Agência Nacional de Saúde Suplementar - ANS para transmissão dos arquivos de dados de todos os sistemas que não possuírem mecanismo de envio próprio ou para os que não possuírem um sistema específico. Disponível em: <http://www.ans.gov.br/index.php?option=com_legislacao&view=legislacao&task=TextoLei&format=raw&id=767>.

BRASIL. Ministério da Saúde. Gabinete do Ministro. Portaria n° 2.546 de 27 de outubro de 2011a. Redefine e amplia o Programa Telessaúde Brasil, que passa a ser denominado Programa Nacional Telessaúde Brasil Redes (Telessaúde Brasil Redes). Disponível em: < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2546_27_10_2011.html>.

BRASIL. Ministério da Saúde. Gabinete do Ministro. Portaria nº 2.554, de 28 de outubro de 2011b. Institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2554_28_10_2011.html>.

BRASIL. Ministério da Saúde. Gabinete do Ministro. Portaria nº 3.127, de 28 de dezembro de 2012. Altera dispositivos da Portaria nº 2.554/GM/MS, de 28 de outubro de 2011, que institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2012/prt3127_28_12_2012.html>.

BRASIL. Ministério da Saúde. Gabinete do Ministro**.** Portaria nº 2.525, de 29 de outubro de 2013. Altera dispositivos da Portaria nº 2.554/GM/MS, de 28 de outubro de 2011, que institui, no Programa de Requalificação de Unidades Básicas de Saúde, o componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt2525_29_10_2013.html>.

BURNETT, S. **Criptografia e segurança:** o guia oficial RSA. 4.ed. Rio de Janeiro: Campus, 2002.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. BR. **Total de incidentes reportados ao CERT.br por ano.** Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 9 jan. 2012.

CHAO, L. W. **Ambiente computacional de apoio à prática clínica**. 2000. Tese - Faculdade de Medicina, Universidade de São Paulo. São Paulo, 2000.

CHAO, L.W. **Modelo de ambulatório virtual (cyber ambulatório) e tutor eletrônico (*cybertutor*) para aplicação na interconsulta médica, e educação à distância mediada por tecnologia.** 2003. Tese (Livre-docência) - Faculdade de Medicina, Universidade de São Paulo. São Paulo, 2003a.

CHAO, L. W.; ENOKIHARA, M. Y.; SILVEIRA, P. S. P. et al. Telemedicine model for training non-medical persons in the early recognition of melanoma. **Journal of telemedicine and telecare. v**.9, suppl 1, p.4-7, 2003b.

CHAO, L.W. **Telemedicina e a Telessaúde: uma abordagem sob a visão de estratégia de saúde apoiada por tecnologia**, 2012. Disponível em: <http://www.chaowen.med.br/artigos/telemedicina.aspx>. Acesso em: 6 ago. 2012.

CHAO, L. W. Conselho Brasileiro de Telemedicina e Telessaúde (CBTms 2006-2013). **J. Health Inform**., v.5. n.4, p.1, out./dez. 2013.

CISCO. Cisco Visual Network Index: Forecast and Methodology, 2011 - 2016. Cisco Whitepaper, 30 May 2012. Disponível em: <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf>. Acesso em: 30 maio 2012

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

EL EMAM, K.; HU, J.; MERCER, J. et al. A secure protocol for protecting the identity of providers when disclosing data for disease surveillance. **J Am Med Inform Assoc.** v.18. n.3, p.212-7, 2011. Disponível em: < http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3078664/pdf/amiajnl-2011-000100.pdf>. Acesso em: 17 maio 2015.

GOMES, A.T. **Telecomunicações: transmissão e recepção AM-FM, sistemas pulsados.** 3.ed. São Paulo: Érica, 1985.

GOROSO, D. G.; SILVA, R. R. da.; BATTISTELLA, L.R. et al. Monitoring heart rate variability online using e-health oriented 3G mobile telephone services. **Journal of Physics Conference Series**, v. 477, p.1-8, 2013. Disponível em: <http://iopscience.iop.org/1742-6596/477/1/012036/pdf/1742-6596_477_1_012036.pdf>. Acesso em: 17 maio 2015.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT of 1996 (HIPAA). Public Law 104-191 104th Congress. Disponível em: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf>. Acesso em: 9 abr. 2015.

INTERNATIONAL DATA CORPORATION-IDC. China to Become the Largest Market for Smartphones in 2012 with Brazil and India Forecast to Join the Top 5 Country-Level Markets by 2016. IDC - Press Release – International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, 15 Mar 2012. Disponível em: <http://www.idc.com/getdoc.jsp?containerId=prUS23381112#.UOlkuLTA9LN>. Acesso em: 30 ago. 2012.

IWAYA, L.H.; GOMES, M.A.; SIMPLÍCIO,M.A. et al. Mobile health in emerging countries: a survey of research initiatives in Brazil. **Int J Med Inform**, v.82, n.5, p.283-98, maio 2013.

KANTER, G. S.; REILLY, D.; SMITH, N. Practical Physical-Layer Encryption: the marriage of optical noise with traditional cryptography. **Ieee Communications Magazine**, v. 47, n.11, p. 74-81, nov. 2009.

KOBAYASHI, L. O. M.; FURUIE, S. S. Abordagem alternativa para Segurança em Imagens Médicas. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, 10., Florianópolis, 2006. **Anais**... p. 427-428, 2006.

KOBAYASHI, L. O. M.; FURUIE, S. S. Segurança em informações médicas: visão introdutória e panorama atual. **Revista Brasileira de Engenharia Biomédica**. v.23, n.1, p.53- 57, abr. 2007.

MARTINÊZ, F. B. R.; AMATE, F. C. Open source application for secure transmission of medical images. IFMBE Proceedings. In: LATIN AMERICAN CONGRESS ON BIOMEDICAL ENGINEERING CLAIB, 5., Habana, Cuba, 16-21 maio. 2011. P.280-283.

MELO, S. **Exploração de vulnerabilidades em redes TCP/IP**. 2.ed. Rio de Janeiro: Alta Books, 2006.

MIOT, H. A. **Desenvolvimento e sistematização da interconsulta dermatológica à distância.** 2005. Tese - Faculdade de Medicina, Universidade de São Paulo. São Paulo, 2005.

NOBRE, L. F.; WANGENHEIM, A. V.; MAIA, R. S. et al. Digital certification in teleradiology: a necessary warning. **Radiol Bras**., São Paulo, v.40, n.6, p.415-421, nov./dec. 2007. Disponível em: <http://www.scielo.br/pdf/rb/v40n6/en_a11v40n6.pdf>.

OVUM expects smartphone shipments to reach 1.7 billion in 2017 and Android to dominate as OS, May, 2012. Disponível em: <http://ovum.com/press_releases/ovum-expectssmartphone-shipments-to-each-1-7-billion--in-2017-and-android-to-dominate-as-os/>. Acesso em: 3 maio 2012.

PAIXÃO, M. P.; MIOT, H. A.; DE SOUZA P. E. et al. A university extensioncourse in leprosy: telemedicine in the Amazon for primary healthcare. **J Telemed Telecare,** v.15, n.2, p.64-7, 2009.

REDE UNIVERSITÁRIA DE TELEMEDICINA-RUTE, 2015. Disponível em: <http://rute.rnp.br/arute>. Acesso em: mar. 2015.

ROSSARO, L.; TRAN, T. P.; RANSIBRAHMANAKUL, K. et al. Hepatitis C videoconferencing: The impact on continuing medical education for rural healthcare providers. **Telemed J E Health**, v. 13, n. 3, p. 269-277, Jun. 2007.

ROSSI, F.; ANDREAZZI, D., CHAO, L.W. Development of a website for clinical microbiologyin Brazil. **J Telemed Telecare**, v.8, suppl 2, p.14-7, 2002.

SANTOS, A. F.; SANTOS S. F.; MELO, M. C. B. et al. Telehealth in primary health care: an analysis of Belo Horizonte experience. **Telemedicine Journal and e-Health**, v. 17, p. 25-29, 2011.

SIGULEM, D. M.; MORAIS, T. B.; CUPPARI, L. et al. Web-based distance education course in nutrition in public health: case study. **J Med Internet Res**, v.3, n.2, p.e16, 2001.

SKELTON-MACEDO, M. C.; ANTONIAZZI, J. H.; WEN, C. L. et al. Núcleo de Teleodontologia da Faculdade de Odontologia da Universidade de São Paulo: uma melhor educação para uma melhor saúde em tempos de TIC. **Jornal Brasileiro de Telessaúde**, v.2, n.2, p.84-86, 2013.

SVERZUT, J. **Redes GSM, GPRS, EDGE e UMTS**: evolução a caminho da Terceira Geração (3G). São Paulo: Érica, 2005.

SYMANTEC. Android. Dropdialer Identified on Google Play. textbfSymantec Official Blog. Disponível em: <http://www.symantec.com/connect/blogs/androiddropdialer-identified-googleplay>. Acesso em: 10 jul. 2012.

TALEB, A.C.; BOHM, G.M.; AVILA, M. et al. The efficacy of telemedicine for ophthalmology triage by a general practitioner. **J Telemed Telecare**, v.11, suppl 1, p.3-5, 2005.

TAURION, C. **Internet Móvel**: tecnologia e modelos. Rio de Janeiro: Campus, 2002.

WORLD HEALTH ORGANIZATION-WHO. Atlas e-Health Country Profiles: based on the findings of the second global survey on e-Health.2010. Disponível em: <http://www.who.int/goe/publications/goe_atlas_2010.pdf?ua=1>

WORLD MEDICAL ASSOCIATION-WMA. Statement on Accountability, Responsibilities and Ethical Guidelines in the Practice of Telemedicine. Adopted by the 51st World Medical AssemblyTel Aviv, Israel, October 1999 and rescinded at the WMA General Assembly, Pilanesberg, South Africa, 2006. Disponível em: <http://www.wma.net/en/30publications/10policies/20archives/a7/>

IV

Prontuário Eletrônico do Paciente: ponderações técnicas e éticas

12

Prontuário Eletrônico do Paciente no contexto do Sistema Único de Saúde: fundamentos e potencialidades no uso de informações para planejamento de políticas públicas

Flávia Mori Sarti[1]
Terry Macedo Ivanauskas[2]

Introdução

O presente capítulo apresenta uma abordagem introdutória quanto aos fundamentos e à potencialidade de adoção de sistemas de informação em saúde, especialmente no que tange ao prontuário eletrônico do paciente (PEP) no Sistema Único de Saúde.

A análise de conceitos básicos, assim como o estudo das principais vantagens e desvantagens dos diferentes tipos de registros médicos e exemplos da informatização em sistemas de saúde de diferentes países, constitui uma etapa importante ao aperfeiçoamento de ações que estejam em andamento no âmbito do sistema de saúde brasileiro, especialmente no que concerne ao ciclo de políticas públicas.

1 Flávia Mori Sarti (flamori@usp.br) é Bacharel em Economia pela Faculdade de Economia, Administração e Contabilidade (FEA-USP) e em Nutrição pela Faculdade de Saúde Pública (FSP-USP). Doutora em Nutrição Humana Aplicada (PRONUT-USP), Pesquisadora do Núcleo de Pesquisas em Estudos Interdisciplinares de Sistemas Complexos da Universidade de São Paulo (NISC-USP) e Docente da Universidade de São Paulo.

2 Terry Macedo Ivanauskas é Bacharel em Economia pela Universidade de São Paulo, Doutor em teoria econômica pela Universidade de São Paulo (2007) com estágio acadêmico na Wharton School (University of Pennsylvania), Pesquisador e docente da Universidade de São Paulo desde 2011.

O capítulo busca contemplar alguns questionamentos iniciais sobre a funcionalidade dos prontuários de pacientes no âmbito da privacidade dos dados pessoais do indivíduo, trabalho desempenhado pelos profissionais de saúde no âmbito de sistemas de informação, organização dos fluxos de trabalho em estabelecimentos de saúde e utilização de informações epidemiológicas em pesquisas e desenvolvimento de programas em políticas públicas de saúde, como forma de permear a ótica dos diferentes atores envolvidos no processo terapêutico: pacientes, profissionais de saúde, instituições e governo.

Sistemas de informação em saúde

A definição de sistemas de informação inclui um conjunto integrado de recursos composto por indivíduos, informações (dados), *software*, *hardware* e redes de comunicação, que apresenta capacidade de recepção e organização de dados em informações úteis à sociedade para produção sistemática de informações como subsídio a processos decisórios (PEREZ & ZWICKER, 2010).

Sistemas de informação são designados para facilitar o acesso a informações pertinentes e confiáveis para redução de incertezas nos processos decisórios pertinentes ao planejamento, operacionalização, monitoramento e avaliação de organizações e instituições, sejam pertencentes ao setor público ou ao setor privado. No caso específico de sistemas de informação em saúde, constituem-se em um instrumento estratégico para promoção de avanços em saúde (MAJEWSKI & AZAMBUJA, 2004; PEREZ & ZWICKER, 2010; WECHSLER e col., 2003).

O emprego de sistemas de informação em saúde apresenta significativas potencialidades no que tange à possibilidade de melhoria em aspectos de segurança do paciente e eficiência operacional do sistema de saúde, a partir do uso de infraestruturas já existentes em várias organizações. Em termos de fragilidades, há registro de problemas na utilização de sistemas de informação em saúde caso haja ausência de integração de sistemas de informação existentes (impossibilitando a comunicação e o envio de dados para melhor gestão de serviços de saúde) ou lentidão e resistência dos indivíduos na adoção de inovações, em decorrência da necessidade de redesenho de processos gerenciais e operacionais da organização (MAJEWSKI & AZAMBUJA, 2004; PEREZ & ZWICKER, 2010; WECHSLER e col., 2003).

Há uma miríade de questões de interesse no estudo do emprego de sistemas de informação em saúde, resultando na criação de uma área de conhecimento específica denominada informática em saúde. A informática em saúde é definida como campo de conhecimento que lida com armazenamento, recuperação e uso da informação, dados e conhecimento biomédico para resolução de problemas e tomada de decisão (BLOIS & SHORTLIFFE, 1990).

Segundo Perez & Zwicker (2010), a informática em saúde apresenta como principais espectros temáticos a análise de sistemas de informação sob ótica organizacional e sob ótica dos usuários. No caso da análise do ponto de vista organizacional, há sistemas de informações operacionais e sistemas de informações gerenciais. No caso da análise do ponto de vista dos usuários, há sistemas de informações individuais, sistemas de informações para grupos, sistemas de informações organizacionais, sistemas de informações interorganizacionais ou sistemas de informações globais.

Os avanços atuais nas tecnologias de computação e comunicação permitem superar dificuldades na gestão dos conhecimentos médicos e das informações sobre pacientes que ocorrem em métodos tradicionais de gerenciamento de dados.

Assim, a informática em saúde apresenta um papel central no processo de disseminação do acesso ao conhecimento e no processo de tomada de decisão na medicina moderna; tendo em vista que a tecnologia de informação na área de saúde contempla uma multiplicidade de aplicações, desde sistemas típicos de gestão de informações até sistemas de automatização e apoio a diagnóstico (MAJEWSKI & AZAMBUJA, 2004; PEREZ & ZWICKER, 2010).

No que tange a algumas das dificuldades para plena adoção de sistemas de informação em saúde, deve-se destacar o papel determinante do usuário da informática em saúde. Há necessidade de alinhamento do sistema de informação aos processos de trabalho e objetivos do usuário, de forma que possa ter percepção da utilidade e da facilidade de uso para aderência aos sistemas de informação em saúde, caso contrário, é possível ocorrer um cenário de resistência à mudança de procedimentos institucionais devido à inovação trazida pela informatização (PEREZ & ZWICKER, 2010).

Segundo Magalhães (2006), a Teoria da Resistência de Usuários a Sistemas de Informação analisa fatores inerentes a pessoas ou grupos específicos de usuários (características subjetivas), falhas no sistema ou problemas na interação do usuário com sistema de informações, de forma a buscar soluções à formação de uma cultura de rejeição à informatização das instituições e organizações de saúde. O estudo das características subjetivas da resistência dos usuários à implantação de sistemas de informação contempla questões relativas às denominadas 'variante sociotécnica' (resistência gerada pela necessidade de redistribuição de funções e responsabilidades) e 'variante política' (resistência decorrente da possibilidade de ocorrência de redistribuição intraorganizacional de poder ou *status*).

Assim, Perez & Zwicker (2010) sugerem uma análise da resistência à adoção de sistemas de informação dentro do contexto de disseminação de inovações, conforme proposto por Rogers (1983) (Quadro 1).

Quadro 1. Definição dos cinco atributos de inovações

Atributo	Descrição
Vantagem relativa	Melhorias em relação à situação anterior
Compatibilidade	Coerência com valores, necessidades e experiências do adotante
Complexidade	Dificuldade de adoção
Observabilidade	Observação de resultados decorrentes da adoção
Experimentação	Possibilidade de experiência prévia antes da adoção

Fonte: Adaptado de Rogers (1983); Perez & Zwicker (2010).

Diversos estudos demonstram que vários fatores podem resultar na rejeição da informática em saúde, incluindo (LOUREIRO, 2004; MAGALHÃES, 2006; PEREZ & ZWICKER, 2010):

- Interferência em processos ou incompatibilidade com práticas de trabalho: sendo uma atividade-meio, a informatização deve apresentar baixa interposição nos fluxos das atividades-fim;
- Características dos profissionais de saúde: devido à formação altamente especializada e específica, profissionais de saúde

buscam autonomia em relação ao processo burocrático-organizacional representado pela informatização;
- Preocupações com privacidade de informações e segurança dos pacientes, assim como possibilidade de alteração da qualidade do serviço e eficiência no atendimento.

Consequentemente, há possibilidade de redução da resistência dos profissionais de saúde à informatização, a partir da adoção de algumas medidas básicas no ambiente de trabalho, como (MAGALHÃES, 2006; PEREIRA & PAIVA, 2012):

- Busca por certificação de segurança nos sistemas de saúde informatizados no Brasil junto à Associação Brasileira de Normas Técnicas (ABNT) ou à Sociedade Brasileira de Informática em Saúde (SBIS);
- Realização de sessões de treinamento dos usuários e condução de testes piloto na organização, previamente à efetiva instalação do sistema de informação;
- Adoção de instrumentos que permitam maior facilidade de uso do sistema, como codificação por barras e padronização de terminologia médica;
- Instituição de gestão competente de tecnologia de informação, baseada em equipe de profissionais habilitados;
- Promoção de ajustes do sistema de informação aos processos de trabalho e à cultura organizacional.

Prontuários médicos: Histórico e evolução para sistemas de informação em saúde

Os prontuários médicos constituem "*documento único constituído por 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, utilizado para possibilitar a comunicação entre membros da equipe multiprofissional e*

> *a continuidade da assistência prestada ao indivíduo*" (CFM 2002a, artigo 1º.).

As principais funções do prontuário médico referem-se a: manutenção de fonte de informação clínica e administrativa, apoio do processo de atenção à saúde, meio de comunicação compartilhado entre profissionais de saúde no atendimento ao paciente, registro legal das ações médicas, apoio à pesquisa em saúde e avaliação da qualidade dos serviços, promoção do ensino por meio de documentação de casos e gestão dos serviços de saúde. O conteúdo básico de um prontuário médico inclui (MAJEWSKI & AZAMBUJA, 2004; MASSAD e col., 2003; PEREIRA & PAIVA, 2012):

- Folha de rosto contendo identificação e anamnese;
- Ficha de evolução e prescrição médica;
- Ficha de evolução de enfermagem;
- Ficha de registro de exames e diagnósticos;
- Relatório de cirurgias, anestesias e demais procedimentos terapêuticos;
- Ficha de resumo de alta;
- Outras informações e anexos.

O primeiro registro de prontuário médico conhecido refere-se ao Egito no período de 3.000 a 2.500 a.C. Em 1897, há adoção do primeiro sistema de organização de arquivos médicos no âmbito do Hospital Geral de Massachussets (EUA) (MASSAD e col., 2003; MURAHOVSCHI, 2000; PEREIRA & PAIVA, 2012).

O uso do prontuário médico foi introduzido no Brasil em 1944, no contexto do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (HCFMUSP), a partir de sistemas de arquivos e classificação de observações médicas (MASSAD e col., 2003; MURAHOVSCHI, 2000; PEREIRA & PAIVA, 2012).

Em 1989 é instituída obrigatoriedade do registro e arquivamento do prontuário médico em estabelecimentos de saúde pela Resolução 1.331 do Conselho Federal de Medicina (CFM, 1989). Em 2002, adota-se uma definição abrangente de prontuário médico por meio da Resolução 1.638

(CFM, 2002a). No mesmo ano, a publicação da Resolução 1.639 revoga a Resolução 1.331, que definia critérios bastante rígidos para adoção do prontuário eletrônico do paciente (PEP) (CFM, 2002b).

Posteriormente, em 2007, a normatização dos prontuários de pacientes torna-se objeto da Resolução 1.821, que autoriza a guarda e o manuseio de prontuários de pacientes, assim como troca de informações identificadas em saúde, utilizando sistemas informatizados, eliminando-se a obrigatoriedade do registro em papel, desde que garantidos requisitos de segurança estabelecidos por lei (inclusive certificação digital) (CFM, 2007).

No contexto do registro das informações em saúde dos pacientes, a manutenção e a atualização do prontuário médico são necessárias a partir da inclusão das documentações geradas durante vários níveis de atendimento prestado ao paciente (como laudos, relatórios médicos e solicitações e resultados de exames) pelos diferentes profissionais de saúde envolvidos (MAJEWSKI & AZAMBUJA, 2004).

Consequentemente, qualquer prontuário de paciente apresenta inúmeras diferentes fontes de dados, incluindo vários procedimentos realizados em diversos setores por diferentes tipos de profissionais de saúde, o que resulta em significativa heterogeneidade no registro de dados. Assim, a organização de um sistema de informações em saúde apresenta necessidade de agregação e organização de informações em um único banco de dados, de forma a possibilitar apoio à tomada de decisão em saúde (MAJEWSKI & AZAMBUJA, 2004).

Os prontuários médicos em papel, adotados pela maioria dos hospitais brasileiros, apresentam características que dificultam o cumprimento de tais objetivos. De maneira geral, estudos quanto ao conteúdo de prontuários em papel indicam predominância de padrões irregulares de preenchimento ou extravio de dados importantes, que resultam em graves prejuízos ao acompanhamento da saúde do paciente e à pesquisa científica. Em diversos casos, estudos retrospectivos baseados em dados de prontuários médicos em papel indicam necessidade de descarte de informações, em decorrência de anotações ilegíveis, informações de leitura penosa, falta de organização no conteúdo ou no arquivamento dos prontuários, assim como

omissão ou extravio de fatos relevantes (MASSAD e col., 2003; PEREIRA & PAIVA, 2012).

Em particular, um estudo conduzido para avaliação de prontuários médicos em papel no Brasil, provenientes de hospitais de ensino, indicou que a maioria dos prontuários apresentava qualidade regular ou baixa no registro de informações dos pacientes. Os autores apontam a coerência no comportamento organizacional das instituições estudadas, tendo em vista a coexistência de descaso no registro de dados em prontuários e baixa informatização ou inexistência de prontuário eletrônico no mesmo hospital (SILVA & TAVARES-NETO 2007).

Destaca-se que o preenchimento incoerente de prontuários médicos apresenta consequências deletérias à ética médica e à saúde do paciente, devido à possibilidade de equívocos na leitura de dados importantes ao tratamento em saúde. Várias organizações de saúde utilizam bases de dados eletrônicas somente no gerenciamento de atividades-meio (setores administrativos, operacional e financeiro, farmácia, laboratório e radiologia), resultando em aproveitamento parcial das potencialidades de um sistema de informação em saúde à gestão hospitalar (SILVA & TAVARES-NETO 2007).

Entre as possíveis vantagens de manutenção de registro em papel dos prontuários médicos, incluem-se (CFM, 2002a; CFM, 2002b; CFM, 2007; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007; WECHSLER e col., 2003):

- Facilidade para transporte e manuseio, caso esteja organizado de forma estruturada;
- Liberdade na forma de escrever e menor necessidade de treinamento específico;
- Disponibilidade física do material contendo dados.

Entretanto, os prontuários médicos em papel apresentam também diversas desvantagens em comparação com registros eletrônicos (CFM, 2002a; CFM, 2002b; CFM, 2007; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007; WECHSLER e col., 2003):

- Ineficiência no armazenamento e organização;
- Necessidade de espaço físico para arquivamento;
- Dificuldade de acesso;
- Multiplicidade de pastas;
- Fragilidade do meio físico de armazenamento;
- Limitação física do meio de informação (arquivos situados fisicamente em um único local e impossibilidade de integração com outros sistemas de informação para acesso do próprio paciente);
- Dificuldade de pesquisa coletiva;
- Ilegibilidade, ambiguidade, perda frequente da informação, falta de padronização ou preenchimento incompleto;
- Necessidade de transcrição para estudos científicos (resulta em maior probabilidade de erro).

A partir da evolução tecnológica ocorrida durante as últimas décadas, houve desenvolvimento de várias ferramentas computacionais inovadoras destinadas ao registro, armazenamento e análise de dados e informações, inclusive em sistemas de saúde, resultando no desenvolvimento de sistemas de informação em saúde dedicados à gestão de diferentes dimensões das organizações de saúde (MASSAD e col., 2003; WECHSLER e col., 2003; PEREIRA & PAIVA, 2012).

Prontuário eletrônico do paciente (PEP)

O prontuário eletrônico do paciente (PEP) constitui um meio físico de repositório digital dos prontuários pela conversão de informações para meio eletrônico (ou seja, incorporação de registros de pacientes em um sistema informatizado) que permite adoção de um sistema de gestão de conteúdo para geração de informações para diagnóstico médico e organização de documentação de consultas. Assim, é possível realizar uma melhor gestão de tarefas organizacionais pela recuperação de informações para vários usos (MASSAD e col., 2003; WECHSLER e col., 2003; PEREIRA & PAIVA, 2012).

A adoção do PEP produz resultados nos serviços oferecidos, processos organizacionais, ensino e aprendizagem, assim como inovações administrativas (MASSAD e col., 2003; WECHSLER e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010). Há cinco estágios de evolução do registro eletrônico de dados em saúde reconhecidos (PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010):

1. Registro médico automatizado (*automated medical record*): Registro e armazenamento da informação em computadores pessoais e papel, simultaneamente (ausência de cumprimento de requisitos legais);
2. Registro médico computadorizado (*computerized medical record*): Registro da informação em papel e armazenamento digitalizado em um sistema computacional de baixa integração (cumprimento de requisitos legais permite dispensar registro em papel);
3. Registro médico eletrônico (*electronic medical record*): Registro e armazenamento da informação em sistema integrado, incluindo requisitos legais para confidencialidade, segurança e integridade dos dados;
4. Registro eletrônico do paciente (*electronic patient record*): Registro e armazenamento da informação em sistema integrado, inclusive fora da instituição (interinstitucional), sendo necessária identificação unívoca da identidade do paciente;
5. Registro eletrônico de saúde (*electronic health record*): Registro e armazenamento da informação em sistema integrado, inclusive fora da instituição (interinstitucional) com compartilhamento da responsabilidade de manutenção do prontuário por profissionais de saúde e paciente, sendo necessária identificação unívoca da identidade do paciente.

O prontuário eletrônico do paciente refere-se ao terceiro estágio do registro eletrônico de dados, que permite a interação da instituição de saúde com paciente pelo processo de acompanhamento desde sua recepção até sua liberação ou alta, via coleta de informações no início do atendimento e recuperação de dados históricos de consultas an-

teriores e resultados de exames já existentes de outros atendimentos passados (CFM, 2002a; CFM, 2002b; CFM, 2007; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007).

Entre as vantagens do PEP, destacam-se (CFM, 2002a; CFM, 2002b; CFM, 2007; MAJEWSKI & AZAMBUJA, 2004; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007; WECHSLER e col., 2003):

- Facilidade de armazenamento e transferência de dados;
- Possibilidade de controles de segurança (senha / *backup* / auditoria);
- Adoção de avaliação de qualidade do serviço;
- Acessibilidade para consulta local ou remota de forma simultânea para vários usuários da informação;
- Organização e indexação de informações;
- Agilidade no registro e recuperação de dados;
- Flexibilidade de consulta;
- Padronização de registros e legibilidade de informações;
- Possibilidade de processamento contínuo de dados;
- Facilidade na integração de sistemas;
- Redução de redundância de procedimentos;
- Melhoria na gestão de recursos;
- Análise de tendências para intervenções em saúde;
- Possibilidade de captação de dados de monitoramento de pacientes em tempo real.

Em contrapartida, o PEP também apresenta algumas potenciais desvantagens em comparação com o registro em papel de prontuários médicos (CFM, 2002a; CFM, 2002b; CFM, 2007; MAJEWSKI & AZAMBUJA, 2004; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007; WECHSLER e col., 2003):

- Custo de implantação e manutenção;
- Necessidade de infraestrutura e treinamentos;
- Resistência dos profissionais de saúde;

- Necessidade de garantia de segurança da informação (controle de acesso);
- Definição dos procedimentos éticos no uso de dados de pacientes;
- Questionamento da validade legal de documentação eletrônica;
- Falhas de *hardware* e *software* (*backup*/prevenção de perdas de dados/possibilidade de interrupção no acesso *on-line*).

Um dos pontos sensíveis à adoção do PEP, de forma interligada entre diversas organizações de saúde, refere-se à necessidade de garantia de segurança do sistema de informação. Os mecanismos de segurança a serem adotados devem incluir diversos aspectos de controle de acesso às informações disponíveis, sem comprometer possibilidades de gestão de informação em nível agregado ou mesmo acessibilidade do próprio paciente às suas informações de saúde (CFM, 2002a; CFM, 2002b; CFM, 2007; MAJEWSKI & AZAMBUJA, 2004; MASSAD e col., 2003; PEREIRA & PAIVA, 2012; PEREZ & ZWICKER, 2010; SILVA & TAVARES-NETO, 2007; WECHSLER e col., 2003). Destacam-se, particularmente, mecanismos de controle de acesso, segundo tipo de usuário do sistema, direcionados a:

- Permissão de acesso aos dados;
- Privacidade e confidencialidade;
- Autenticação de usuário;
- Controle de alteração de dados;
- Integridade e auditoria da informação.

Tais mecanismos devem garantir a ausência de disseminação de informações sensíveis em termos de estado de saúde do paciente, assim como evitar adulteração de documentos oficiais, desvios de recursos da organização de saúde, entre outros crimes potencialmente decorrentes do mau uso de sistemas de informação em saúde (FREIRE, 2004).

Em contrapartida, o *Institute of Medicine* (IOM, 1997) destaca os potenciais usos primários e secundários dos sistemas de informação em saúde (Quadro 2).

Quadro 2. Usos primários e secundários de prontuários eletrônicos de pacientes.

Tipo de uso	Dimensão institucional/ Usuário da informação	Caracterização
Primário	Paciente	Documentação dos serviços recebidos Prova de identidade Autoadministração de cuidados de saúde Verificação dos serviços prestados/cobranças realizadas
	Organização de saúde	Manutenção de cuidados em saúde (instrumento de comunicação com paciente) Descrição de morbidades e causas (apoio a diagnóstico) Sistema de apoio à decisão em diagnósticos e terapias Avaliação e gestão de risco de pacientes Padronização de cuidados de acordo com recomendações em prática clínica Documentação de fatores de risco dos pacientes Avaliação e registro de expectativas e satisfação do paciente Planejamento dos cuidados em saúde Provisão de informações sobre ações de prevenção ou promoção da saúde Envio de alertas aos profissionais de saúde Apoio ao cuidado de enfermagem Documentação de serviços realizados (terapias, medicamentos, entre outros)
	Gestão da saúde	Registro de casos e práticas clínicas em diferentes instituições Análise de severidade da doença Formulação de recomendações em prática clínica Apoio à gestão de riscos em saúde Caracterização da utilização de serviços Provisão de evidências para revisão de usos e práticas Possibilidade de garantia de qualidade
	Sistemas de apoio	Alocação de recursos Análise de tendências e desenvolvimento de previsões Avaliação da carga de trabalho Comunicação entre departamentos da organização de saúde
	Administração e auditoria	Documentação de serviços para pagamento Cobrança por serviços Envio de solicitações ao seguro-saúde Apoio à decisão em requerimentos administrativos ou demandas judiciais Diagnóstico de incapacidade (compensação por perdas produtivas) Gestão de custos Prestação de contas Análise atuarial

(continua)

(continuação)

Tipo de uso	Dimensão institucional (Usuário da informação)	Caracterização
Secundário	Educação	Registro de experiência para profissionais de saúde Preparação de palestras e apresentações Ensino a estudantes na área de saúde
	Regulação	Registro de evidências para litígios Fiscalização e vigilância pós-atendimento de saúde Análise de cumprimento de padrões de atendimento em saúde Acreditação de profissionais de saúde e hospitais Comparação de organizações de saúde
	Pesquisa	Desenvolvimento de novos produtos e serviços de saúde Realização de pesquisas clínicas Avaliação de tecnologias em saúde Estudo de desfechos em saúde Análise de efetividade e custo-efetividade no atendimento a pacientes Identificação de populações em risco Desenvolvimento de bancos de dados e registros Avaliação de custo-efetividade a partir de sistemas de registro
	Governo	Alocação de recursos Realização de planejamento estratégico Monitoramento de indicadores de saúde pública
	Indústria	Realização de pesquisa e desenvolvimento Planejamento estratégico de marketing

Fonte: Adaptado de IOM (1997:78-79).

Considerando-se potenciais benefícios e malefícios decorrentes da adoção de sistemas de informação em saúde direcionados ao armazenamento de prontuários médicos de pacientes, um estudo conduzido pelo *Committee on Improving the Patient Record* do *Institute of Medicine* (1997) destaca requerimentos básicos para sistemas de informação em saúde contendo prontuários médicos de pacientes em oito diferentes dimensões (Quadro 3).

Quadro 3. Requerimentos básicos de sistemas de informação em saúde.

Dimensão	Requerimentos básicos
Conteúdo do prontuário	• Registro uniforme de informações fundamentais • Padronização de códigos e formatos de informação • Dicionário compartilhado de codificação de dados • Informação sobre desfecho e estado funcional do paciente
Formato do prontuário	• Lista de principais morbidades • Possibilidade de explorar dados em registros e prontuários • Integração entre diferentes especialidades e organizações de saúde
Desempenho do sistema de informação	• Agilidade na busca e recuperação de dados • Acessibilidade permanente • Disponibilidade remota da informação • Facilidade no registro de dados e informações
Integração do sistema de informação	• Integração com outros sistemas de informação em saúde • Transferência de informações entre especialidades e organizações de saúde • Integração com literatura científica relevante • Integração com outras bases de dados e registros institucionais • Integração com registro de saúde de familiares • Transferência eletrônica de informações de cobrança pelos serviços de saúde
Inteligência do sistema de informação	• Sistema de apoio à decisão em saúde • Emissão de alertas aos profissionais de saúde • Inclusão de sistema de alertas personalizável
Produtos do sistema de informação	• Emissão de documentos comprobatórios ou formulários para serviços de saúde integrados • Personalização de relatórios e outras interfaces com usuário • Emissão de relatórios clínicos padronizados • Emissão de relatórios personalizados e formulários ad hoc • Elaboração de relatórios e gráficos de evolução do estado de saúde
Controle e acesso	• Acessibilidade aos pacientes e seus representantes legais • Garantias contra violação de confidencialidade da informação
Treinamento e implementação	• Necessidade de baixo nível de especialização e treinamento dos usuários do sistema de informação • Possibilidade de implementação gradual

Fonte: Adaptado de IOM (1997:80).

De forma geral, é possível resumir os requerimentos anteriormente delineados nos seguintes aspectos de um prontuário médico com integração a sistemas informatizados de monitoramento da saúde de pacientes (MASSAD e col., 2003; PEREIRA & PAIVA, 2012):

- Histórico de morbidades e registro longitudinal do paciente;
- Capacidade de mensuração de estado funcional e de saúde do paciente;

- Flexibilidade de registro para inclusão de raciocínio clínico do profissional de saúde;
- Garantia de confidencialidade e privacidade;
- Apoio a processos de auditoria clínica e administrativa da organização;
- Possibilidade de acesso contínuo aos usuários autorizados;
- Visualização simultânea e personalizada de relatórios;
- Acesso em tempo real localmente ou remotamente;
- Inclusão de instrumentos de apoio à análise e à decisão clínica;
- Oferta de mecanismos e interfaces amigáveis para entrada de dados;
- Apoio ao gerenciamento e controle de custos;
- Flexibilidade para expansão em vista de necessidades futuras.

Sistemas de informação em saúde no Brasil

A organização de bancos de dados e sistemas de informação no contexto do sistema de saúde brasileiro inclui um conjunto de vários subsistemas de notificação compulsória de agravos, comunicação de morbidades, registro de mortalidade e nascimento, assim como informações gerenciais para subsídio à operacionalização do Sistema Único de Saúde (SUS), que buscam integrar bancos de dados em saúde do setor público e setor privado (BARROS e col., 2002; FREIRE, 2004; LOUREIRO, 2004; RÖTZCH, sd), inclusive:

- No âmbito do Departamento de Informática do Sistema Único de Saúde (DATASUS):
  - Sistema de Informações Hospitalares (SIH);
  - Sistema de Informações Ambulatoriais (SIA);
  - Sistema de Informações de Nascidos Vivos (SINASC);
  - Sistema de Informações de Mortalidade (SIM);
  - Sistema de Informação de Agravos de Notificação (SINAN);
  - Sistema de Informação da Atenção Básica (SIAB);
  - Sistema de Vigilância Alimentar e Nutricional (SISVAN);

  - Sistema do Cadastro Nacional de Estabelecimentos de Saúde (SCNES);
  - Sistema de Informações sobre Orçamentos Públicos em Saúde (SIOPS);
  - Entre outros sistemas de informação.
- No âmbito da Agência Nacional de Saúde Suplementar (ANS):
  - Sistema de Informações Epidemiológicas (SIEPI) para uso interno;
  - Sistema de Informações de Beneficiários (SIB) para integração ao SUS.

De maneira geral, a coexistência de vários subsistemas de informação operacionalizados em paralelo no interior do sistema de saúde brasileiro, sendo alguns caracterizados pelo desenvolvimento de *softwares* e bancos de dados próprios, tem gerado dificuldades para integração de bancos de dados em saúde no país, tendo em vista: ausência de identificador único dos pacientes para buscar integração das bases de dados preexistentes, existência de registros em duplicidade e ocorrência de pacientes com homônimos, deficiências na coleta e padronização dos dados, registro com grafia incorreta do nome do paciente (incluindo abreviaturas ou variações de escrita do mesmo nome), assim como inclusão de diferentes diagnósticos no mesmo óbito (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004; MASSAD e col., 2003; PEREIRA & PAIVA, 2012).

Tais problemas impedem uma completa integração de sistemas de informação em saúde no Brasil, que poderia constituir uma base de dados de significativa importância aos processos de planejamento, operacionalização e monitoramento da saúde da população brasileira. Os avanços tecnológicos atuais permitiriam a manutenção de registros eletrônicos longitudinais do paciente desde nascimento até morte, dentro de um único sistema de informação com capacidade de coleta, armazenamento e pesquisa de dados de amplo escopo com possibilidade de adoção de um identificador único integrado das informações dos indivíduos em várias bases de dados (além da saúde) via redes de compartilhamento e integração de informações (organizacionais *on-line*), constituindo um avanço

significativo ao bem-estar da população e à eficiência no gerenciamento de um sistema de saúde universal em um país de dimensões amplas e população numerosa, como o Brasil (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004).

A concepção de um cartão como forma de identificação pessoal com dados do paciente para ingresso no sistema de saúde foi iniciada no Sistema Único de Saúde brasileiro ao final da década de 1990. Denominado Sistema Cartão Nacional de Saúde, foi alvo de edital de concorrência internacional do Ministério da Saúde, em 1999, tendo sido implementado por meio de projeto piloto que incluiu gestor federal, 27 gestores estaduais e 44 municípios heterogêneos situados em 11 estados das cinco regiões do país (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004).

Em princípio, o desenho do sistema de informação foi planejado para captura automática de dados do atendimento em saúde, de forma a possibilitar uma vinculação direta entre usuário, profissional de saúde e estabelecimento de saúde. Seria construída uma base de dados com capacidade de geração de informações para processos de gestão em saúde, a partir de um conjunto de ações oferecidas aos indivíduos e à coletividade com garantia de aplicação das normas éticas e legislação pertinente. O Sistema Cartão Nacional de Saúde deveria incluir mecanismos para garantia de facilidade de operação, segurança, eficácia e eficiência na coleta de dados e operacionalização do sistema em diferentes cenários, assim como funcionalidades baseadas em padrões de organização para vinculação e integração das informações em diferentes níveis (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004).

Havia previsão de módulos que contemplassem funcionalidades direcionadas ao atendimento em saúde (via interface de PEP) e à gestão da organização e do sistema de saúde (direcionada à geração de relatórios técnicos para profissionais e estabelecimentos de saúde). O Sistema Cartão Nacional de Saúde deveria apresentar integração plena com sistemas já existentes do DATASUS, incluindo Sistema das Centrais de Regulação (SISREG), Sistema de Repositório de Tabelas, Sistema da Atenção Básica (SAB), Cadastro Nacional de Estabelecimentos de Saúde (CNES) e Sistema da Média e Alta Complexidade (SIMAC), sendo o último designado como sistema de informação unificador do Sistema de Informações Am-

bulatoriais (SIA), Sistema de Informações Hospitalares (SIH) e Sistemas da Vigilância Sanitária e Vigilância Epidemiológica (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004).

Entretanto, vários problemas têm sido enfrentados na transposição dos sistemas de informação em saúde já existentes para completa implementação do Sistema Cartão Nacional de Saúde, destacando-se, principalmente, questões relativas à resistência dos usuários do sistema de informação, descritas ao início do presente capítulo. As principais barreiras detectadas à adoção do inovador sistema de informação em saúde proposto referem-se a (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004):

- Incremento da carga de trabalho dos profissionais de saúde por duplicidade de procedimentos para lançamento de informações no sistema;
- Prejuízo na relação médico-paciente devido à redução do tempo de atenção na consulta ambulatorial;
- Ausência de indicação das responsabilidades dos profissionais de saúde na operacionalização do sistema;
- Falta de entendimento entre entes federativos e organizações de saúde quanto à responsabilidade pelo custeio da implantação e manutenção da infraestrutura;
- Instabilidade e ausência de confiabilidade na operacionalização do sistema de informação;
- Mediação do Ministério da Saúde para transferência de informações contidas no cadastro de usuários;
- Rejeição no uso de Terminais de Atendimento do SUS, tendo em vista inclusão de mecanismos de avaliação dos profissionais de saúde pela qualidade do atendimento em saúde prestado e controle de horários de trabalho.

A síntese dos problemas enfrentados na operacionalização do Sistema Cartão Nacional de Saúde desde seu projeto piloto refere-se diretamente aos pontos destacados da Teoria da Resistência de Usuários a Sistemas de Informação (MAGALHÃES, 2006), tendo em vista falhas do sistema de informação, interferência na rotina de trabalho, custos de ma-

nutenção do sistema de informação e redistribuição de funções, responsabilidades e poder no interior da organização de saúde.

Conclusão

A partir da utilização de bancos de dados integrados, contendo informações em saúde, é possível alavancar pesquisas e ações estratégicas em programas de políticas públicas de saúde. A existência de sistemas informatizados contendo dados pessoais de pacientes atendidos no sistema de saúde brasileiro permite execução de diversos tipos de análises de interesse social para guiar a realização de estudos clínicos e intervenções em saúde pública; no entanto, é necessária abordagem das questões éticas relativas à segurança no sigilo dos dados pessoais dos indivíduos em questão.

O Sistema Cartão Nacional de Saúde, baseado na integração de bancos de dados e subsistemas de informação já existentes no âmbito do Sistema Único de Saúde brasileiro, pode constituir uma importante fonte de conhecimento público para fomentar ações estratégicas em termos de planejamento, operacionalização e monitoramento da saúde da população do país, equacionando problemas relativos à escassez de recursos no sistema de saúde.

Entretanto, ainda deve enfrentar questões relativas à sua completa operacionalização no contexto de um sistema público de saúde caracterizado por universalidade e integralidade nas ações de saúde direcionadas a uma população numerosa, espalhada em um território de amplas dimensões geográficas.

Os principais desafios ao Sistema Cartão Nacional de Saúde incluem ações relativas a: imposição de identificador único dos pacientes, celeridade na emissão de cartão de identificação definitivo ao paciente, vinculação do cartão do usuário ao número do prontuário, padronização das informações em saúde coletadas, uniformização das terminologias em saúde, adoção de protocolos clínicos bem definidos, garantia de segurança do sistema em termos de sigilo do paciente, estabilidade no funcionamento contínuo do sistema de informação *on-line*, inclusão

de treinamentos aos profissionais de saúde envolvidos na alimentação das informações, atribuição de responsabilidades na gestão do sistema de informação (em nível organizacional e em nível de esferas de governo), melhoria da interface de uso do sistema de informação e inclusão de funcionalidades adicionais, como possibilidade de emissão de relatórios personalizáveis para uso em planejamento e gestão, agendamento de atendimentos *on-line* para usuários do sistema de saúde e acesso a prontuários pelos profissionais de saúde situados em diferentes especialidades ou instituições de saúde (BARROS e col., 2002; BRASIL, 2006; LOPES e col., 2004; LOUREIRO, 2004).

Referências

BARROS, R.S.M.; FERREIRA, S.M.G.; HEXSEL, R.A. Desenvolvimento de solução única de software para o Sistema Cartão Nacional de Saúde. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS), 8., Natal, 29 set.- 2 out., 2002.

BLOIS, M.S.; SHORTLIFFE, E.H. The computer meets medicine: Emergence of a discipline. In: SHORTLIFFE, E.H.; PERREAULT, L.E. (Ed.). **Medical informatics:** computer applications in medical care. Massachusetts: Addison-Wesley, 1990. p.1-36.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. **Relatório do seminário nacional de comunicação, informação e informática em saúde.** Brasília, D.F.: Ministério da Saúde, 2006.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução 1.331, de 25 de setembro de 1989**. Diário Oficial da União**, 25 set., p.17145, 1989.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução 1.638, de 09 de agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, de 9 ago. 2002, Seção I, p.184-5, 2002a.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução CFM nº 1.639 de 10 de julho de 2002b. Aprova as "Normas técnicas para uso de Sistemas Informatizados para a guarda e manuseio do prontuário médico", dispõe sobre tempo de guarda dos prontuários, estabelece critérios para certifi-

cação dos sistemas de informação, e dá outras providências. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1639_2002.htm>.

CONSELHO FEDERAL DE MEDICINA-CFM. Resolução 1.821, de 23 de novembro de 2007b. 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 em: <http://www.sbis.org.br/indexframe.html>.

DALMATI, C.F.; SANTOS, L.L.; LEMOS, R.N. et al. Informatização da estratégia de prevenção de doenças e promoção de saúde em Unidades de Saúde da Família. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS),11., Campos do Jordão, 2008.

FREIRE, S.M. Sigilo das informações. In: BRASIL. Ministério da Saúde. Agência Nacional de Saúde Suplementar. **Documentos técnicos de apoio ao fórum de saúde suplementar.** Brasília, D.F., 2004 . p.337-380.

INSTITUTE OF MEDICINE-IOM. Committee on Improving the Patient Record. The computer-based patient record: Meeting health care needs. In:____. **The computer-based patient record: an essential technology for health care.** ed.rev. Washington, D.C.: National Academy , 1997. p.74-99.

LOPES, J.P.; PINHEIRO, L.F.R.; CARVALHO, N.L. et al. Cartão Nacional de Saúde - Projeto piloto no estado do Paraná avaliação do grau de satisfação dos gestores municipais. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS), 10., Florianópolis, SC, 14-18 out. 2006.

LOUREIRO, S. Sistema Único de Informação em Saúde? Integração dos dados da Assistência Suplementar à Saúde aos sistemas de informações do SUS. In: BRASIL. Ministério da Saúde. Agência Nacional de Saúde Suplementar. **Documentos técnicos de apoio ao fórum de saúde suplementar.** Brasília, D.F**,** 2004. p.317-336.

MAGALHÃES, C.A.S. **Análise da resistência médica à implantação de sistemas de registro eletrônico de saúde.** In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS), 10., Florianópolis, SC, 14-18 out. 2006.

MAJEWSKI, C.; AZAMBUJA, G. Implantação do PEP na ótica dos usuários**.** In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE (CBIS), 9., Ribeirão Preto, 7-10 nov. 2004.

MASSAD, E.; MARIN, H.F.; AZEVEDO NETO, R.S. **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico.** São Paulo: UNIFESP, 2003.

MURAHOVSCHI, D. **Implantação de prontuário eletrônico em um hospital de grande porte: estudo de caso.** 2000. Dissertação (Mestrado em Administração) - Fundação Getúlio Vargas. São Paulo, 2000.

PEREIRA, S.R.; PAIVA, P.B. Segurança da informação em saúde: prontuário eletrônico do paciente. In:. CONFERÊNCIA INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO (CONTECSI), 9., São Paulo, 31 maio-1 jun. 2012.

PEREZ, G.; ZWICKER, R. Fatores determinantes da adoção de sistemas de informação na área de saúde: um estudo sobre o prontuário médico eletrônico. **Revista de Administração Mackenzie,** v. 11, n. 1, p.174-200, 2010.

RÖTZCH, J.M. **Relacionamento Nominal de Banco de Dados - Record Linkage.** Brasília, D.F.: ANS, s.d. Disponível em: <www.ans.gov.br/portal/upload/noticias/Relacionamento_banco_dados.ppt>. Acesso em: 2 fev. 2015.

SILVA, F.G; TAVARES-NETO, J. Avaliação dos prontuários médicos de hospitais de ensino do Brasil. **Revista Brasileira de Educação Médica,** v. 29, n. 1, p.113-126, 2007.

WECHSLER, R.; ANÇÃO, M.S.; CAMPOS, C.J.R. et al. A informática no consultório médico. **Jornal de Pediatria**, v.79, supl.1, p. S3-S12, 2003.

13

Prontuário Eletrônico do Paciente e ética profissional

Moise Dalva[1]

Introdução

Os aspectos relativos à geração e armazenamento de informações assumem papéis cada vez mais proeminentes nas relações humanas, impactando de forma irreversível o relacionamento dos indivíduos com a sociedade, com consequências que por vezes extrapolam o plano das intenções originais. Na área da saúde, tal aspecto apresenta-se de forma crítica, pois as informações geradas e armazenadas a partir do relacionamento do paciente com o sistema de saúde podem ter impacto considerável sobre a evolução clínica do indivíduo.

Dado que o conjunto de informações disponíveis sobre determinada pessoa encontra-se armazenado em documento denominado "Prontuário do Paciente", há que se examinar os desdobramentos advindos da assim chamada "revolução digital" nos modos de gerar, armazenar e disponibilizar essas informações, ressaltando seus aspectos positivos e negativos.

Uma questão premente diz respeito ao fato de que a prática assistencial dos trabalhadores em serviços de saúde pode efetivamente ser modificada com a agregação de novas ferramentas digitais. Nesse senti-

1 Moise Dalva (moise.dalva@gmail.com) é médico formado pela UNICAMP, Doutor em Ciências pela Faculdade de Medicina da Universidade de São Paulo, Membro Titular da Sociedade Brasileira de Cirurgia Cardiovascular e Acadêmico de Direito nas Faculdades Metropolitanas Unidas (FMU).

do, a adoção do assim chamado Prontuário Eletrônico do Paciente (PEP) deve ser examinada à luz do melhor interesse do paciente, principalmente no que tange aos aspectos éticos da relação entre os agentes e os usuários dos serviços de saúde.

A relação entre a ética e as modificações sociais oriundas da adoção de tecnologias digitais verificadas na sociedade pós-moderna extrapolam em muito os aspectos da privacidade pura e simples do indivíduo, em todas as esferas da experiência humana. Diariamente a imprensa veicula notícias sobre exposição indevida em meios digitais ou redes sociais de aspectos íntimos de determinados indivíduos, muitas vezes com consequências trágicas, tais como alguns casos de suicídio de adolescentes claramente associados à prática do *cyber bullying.* Por outro lado, tem-se como normal a utilização por parte de companhias e governos dos meta-dados, que são as pegadas digitais originadas a partir de atuação digital dos indivíduos objetivando coleta de tendências de comportamento.

O objetivo desse capítulo é a análise do impacto ético da adoção do PEP nas relações entre os agentes e usuários dos serviços de saúde, destacando-se os aspectos positivos e potenciais aspectos negativos.

Ética e moral

Em primeiro lugar, é necessário que se tenha clara noção do que deve ser entendido como ética e qual a relação entre ética e moral.

Segundo o dicionário Michaelis Online, define-se ética como "1- Parte da Filosofia que estuda os **valores morais e os princípios ideais da conduta humana.** É ciência normativa que serve de base à filosofia prática. 2- Conjunto de **princípios morais** que se devem observar no exercício de uma profissão."

Já a moral, segundo a mesma fonte, é definida da seguinte forma: "1- Relativo à moralidade, **aos bons costumes.** 2 - Que procede conforme à honestidade e à justiça, que tem bons costumes. 3 - Favorável aos bons costumes"

Dessas definições, pode-se perceber claramente que, em sentido estrito, ética e moral são conceitos diferentes.

A ética possui caráter interno, definindo conduta no âmbito do indivíduo, sendo atemporal e reflexiva, ao passo que a moral possui caráter externo, definindo conduta no âmbito da sociedade, sendo temporal e imposta a partir do binômio "Norma X Sanção".

Como exemplo prático dessa dicotomia, pode-se citar o comportamento de uma pessoa dentro de determinada loja, onde existem mercadorias expostas e não há ninguém por perto. Se a pessoa desse exemplo não furta a mercadoria por achar que não é correto, está agindo de forma ética, porém se não furta imaginando que eventualmente poderia ser flagrado no ato está agindo de forma moral, pois seu comportamento é definido a partir de pressão externa advinda de uma norma (não furtar), que se transgredida resulta na aplicação de uma sanção (Código Penal- Decreto-Lei 2848, de 7 de dezembro de 1940, artigo 155 - Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa).

Dessas definições, pode-se inferir o fato de que por razões de transitoriedade temporal e relativismo cultural, diversas condutas antiéticas e degradantes adotadas ao longo da história humana podem ter sido socialmente toleradas com chancela de "conduta moralmente aceita". Dentre tais fatos, pode-se citar as práticas da escravidão e da aplicação de castigos físicos mutilantes.

Ética e a Constituição

A Constituição Federal de 1988 estabelece os princípios fundamentais que norteiam todo o ordenamento jurídico nacional, possuindo como um de seus fundamentos basilares a dignidade da pessoa humana.

Dentro dessa premissa, tem-se no artigo 5º que "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação - inciso X" e "É assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional- inciso XIV".

Deve-se lembrar que a Constituição Federal é a lei máxima da nação, e de que todos os outros dispositivos, tais como o Código Civil e os

códigos de ética das sociedades profissionais devem seguir os preceitos constitucionais, não podendo nunca confrontá-los.

Desta forma, o Código de Ética Médica (Resolução do Conselho Federal de Medicina nº 1.931/2009) contém as normas que devem ser seguidas pelos médicos no exercício de sua profissão, inclusive no exercício de atividades relativas ao ensino, à pesquisa e à administração de serviços de saúde, bem como no exercício de quaisquer outras atividades em que se utilize o conhecimento advindo do estudo da medicina.

Da mesma forma a Resolução do Conselho Federal de Enfermagem 311/2007 aprova a reformulação do Código de Ética dos Profissionais de Enfermagem.

Bioética

A etimologia do termo é composta das palavras *bios* (vida) + ética.

O termo foi utilizado pela primeira vez pelo pastor protestante alemão Paul Max Fritz Jahr, em 1927, em um artigo de editorial da revista Kosmos, intitulado *Bio-Ethik. Eine Umschau über die ethischen Beziehungen des Menschen zu Tier und Pflanze (Do alemão; Bioética: uma revisão do relacionamento ético dos humanos em relação aos animais e plantas.)*

Trata-se de conceito transdisciplinar, abarcando áreas de ciências biológicas, ciências da saúde, filosofia e direito.

Com relação à área da saúde, todas as ações devem ser pautadas pelos princípios éticos basilares e respeitar o ordenamento jurídico nacional.

Seus principais postulados são:

- Autodeterminação da pessoa em tomar decisões relacionadas à sua vida e à sua saúde. Pressupõe existência de opções, liberdade de escolha e requer que o indivíduo seja capaz de agir de acordo. Fundamenta-se no princípio da dignidade humana, acatando-se o imperativo categórico kantiano "O ser humano é um fim em si mesmo".

- Beneficência - Refere-se à obrigação ética de maximizar o benefício e minimizar o prejuízo. O profissional deve ter a maior convicção e informação técnica possíveis que assegurem ser o ato de saúde benéfico ao paciente.
- Não Maleficência - Estabelece que a ação do agente de saúde sempre deve causar o menor prejuízo ou agravos à saúde do paciente. Princípio universalmente consagrado através do aforismo hipocrático *primum non nocere* (primeiro não prejudicar), cuja finalidade é reduzir os efeitos adversos ou indesejáveis das ações diagnósticas e terapêuticas no ser humano.
- Justiça e Equidade: obrigação ética de tratar cada indivíduo conforme o que é correto e adequado, de dar a cada um o que lhe é devido. Os recursos devem ser equilibradamente distribuídos, com o objetivo de alcançar, com melhor eficácia, o maior número de pessoas assistidas.

Prontuário do paciente

Inicialmente, deve-se ter em mente que o termo "prontuário médico" é absolutamente inadequado, pois as informações coligidas no prontuário dizem respeito e pertencem ao paciente. Desta forma, deve-se adotar a terminologia "prontuário do paciente".

Tal documento é de suma importância, sendo o principal veículo de comunicação entre os membros da equipe de saúde que assistem ao paciente.

Constitui-se do conjunto de documentos padronizados e ordenados, onde devem ser registrados todos os cuidados profissionais prestados aos pacientes e que atesta o atendimento médico a uma pessoa numa instituição de assistência médica ou num consultório médico. É também o documento repositário do segredo médico do paciente.

Deve conter os seguintes elementos:

- Ficha clínica com as seções: identificação, anamnese, exame físico, hipótese diagnóstica e plano terapêutico;

- Exames complementares;
- Folha de evolução multiprofissional;
- Folha de pedido de parecer;
- Prescrições;
- Anotação de sinais vitais;
- Resumo de alta / óbito.

O prontuário é parte fundamental da ralação médico-paciente, de forma que vários dispositivos do código de ética médica se referem a este documento.

O capítulo X do código de ética médica trata especificamente de documentos médicos e estabelece as seguintes vedações aos médicos:

- Art. 85. Permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade.
- Art. 87. Deixar de elaborar prontuário legível para cada paciente.

  § 1º O prontuário deve conter os dados clínicos necessários para a boa condução do caso, sendo preenchido, em cada avaliação, em ordem cronológica com data, hora, assinatura e número de registro do médico no Conselho Regional de Medicina.

  § 2º O prontuário estará sob a guarda do médico ou da instituição que assiste o paciente.
- Art. 88. Negar ao paciente acesso a seu prontuário, deixar de lhe fornecer cópia quando solicitada, bem como deixar de lhe dar explicações necessárias à sua compreensão, salvo quando ocasionarem riscos ao próprio paciente ou a terceiros.
- Art. 89. Liberar cópias do prontuário sob sua guarda, salvo quando autorizado, por escrito, pelo paciente, para atender ordem judicial ou para a sua própria defesa.

  § 1º Quando requisitado judicialmente, o prontuário será disponibilizado ao perito médico nomeado pelo juiz.

  § 2º Quando o prontuário for apresentado em sua própria defesa, o médico deverá solicitar que seja observado o sigilo profissional.

- Art. 90. Deixar de fornecer cópia do prontuário médico de seu paciente quando de sua requisição pelos Conselhos Regionais de Medicina.

Particularidades do PEP

A premissa fundamental que regula a relação entre o modo de agir ético e o prontuário do paciente postula que não há diferença entre os deveres dos profissionais de saúde no que tange ao meio de registro dos dados, vale dizer, tudo o que é obrigatório para o prontuário registrado em papel também o é para o prontuário eletrônico.

Ainda assim, o PEP apresenta particularidades próprias que devem ser levadas em consideração.

O PEP apresenta as seguintes características:

- Foi idealizado para que a equipe de saúde recordasse de forma sistemática os fatos e eventos clínicos ocorridos em um indivíduo, sendo importante veículo de comunicação entre os membros de uma equipe de saúde responsável pelo atendimento.
- É sistema utilizado para apoiar os usuários, disponibilizando acesso a um completo conjunto de dados corretos, alertas e sistemas de apoio à decisão.
- Os fatores que impulsionaram a implementação do PEP foram: possibilidade de compartilhar informações, melhoria da qualidade da assistência, aumento da eficiência de processos clínicos e redução de erros.

A implantação do PEP oferece inúmeras vantagens aos usuários e gestores dos serviços de saúde, tais como acesso veloz aos problemas de saúde atuais; disponibilidade remota; uso simultâneo; legibilidade; eliminação da redundância; fim da redigitação de informações; integração com outros sistemas de informação; processamento contínuo dos dados; organização sistemática; acesso a conhecimento científico atualizado; melhoria da efetividade do cuidado; possível redução de custos; otimi-

zação dos recursos; minimização da desatenção a detalhes importantes; busca coletiva; pesquisa e análises estatísticas.

Da perspectiva dos usuários dos serviços de saúde, a adoção do PEP constitui grande avanço, permitindo ao paciente assumir uma posição mais responsável perante a sua saúde, uma vez que ele passa a ser atuante no processo de decisão sobre as condutas a serem tomadas e também na pesquisa de informações sobre a sua doença.

Por outro lado, a adoção do PEP traz algumas desvantagens, tais como:

- Necessidade de grandes investimentos de hardware, softwares e treinamento; resistência dos profissionais ao uso de sistemas informatizados; demora em se obter reais resultados da implantação do PEP; sujeição a falhas de hardwares, redes e software, deixando o sistema inoperante.
- Uso e acesso indevidos podem colocar a questão da confiabilidade e segurança das informações do paciente em risco.

PEP e ética em saúde

Com relação aos aspectos éticos e o uso do PEP, alguns quesitos precisam ser observados:

- O profissional de saúde que recebe, registra, manipula, digita, armazena e processa dados e informações é responsável pela sua guarda e integridade e deve estar atento para a importância e significado de preservar o sigilo da informação e assegurar a privacidade da pessoa cujos dados estão sendo manuseados.
- As informações contidas no PEP são de propriedade do paciente. As instituições e os profissionais da área da saúde que tem acesso a elas são fiéis depositários do prontuário.
- A confidencialidade das informações do PEP é um direito de todo cidadão, com respaldo na CF de 1988, em seu artigo 5º, inciso X que garante a inviolabilidade da intimidade, da vida privada, da imagem e da honra das pessoas.

- Dever de preservação de segredo é previsto no Código Penal, artigo 154, e na maioria dos códigos de ética profissional da saúde.
- O código de Ética Médica, artigo 11, impõe o segredo como princípio fundamental para o exercício da medicina. No Capítulo IX estão as obrigações com o segredo profissional (dever do médico de orientar seus auxiliares e zelar para que todos respeitem o segredo profissional, proibição do médico em facilitar o acesso ao prontuário por pessoas que não são obrigadas ao segredo profissional).
- As instituições e os profissionais envolvidos são obrigados a não revelar as informações fornecidas sem autorização prévia do paciente, exceto quando possam ser utilizadas em função da necessidade de cuidado ao paciente, por justa causa ou dever legal.
- Fica sob responsabilidade das instituições de saúde a implementação e o aprimoramento continuado, estabelecendo normas de controle de acesso e de identificação de usuários, como parte de um sistema seguro de proteção ao conteúdo do Prontuário Eletrônico do Paciente.

Dentre todas as preocupações concernentes ao uso do PEP destaca-se a questão da privacidade dos usuários dos serviços de saúde, pois o vazamento de informações sigilosas pode alcançar grande repercussão, gerando ações de reparação por danos morais.

Existe também o dever ético para que a segurança do PEP seja a mais efetiva possível, através da adoção de medidas que protejam os seguintes quesitos:

- Integridade: processo de assegurar que dados não sejam alterados por entidades não autorizadas;
- Confidencialidade: necessidade de proteger informações sensíveis;
- Disponibilidade: acesso ao sistema para usuários autorizados;
- Autenticação: processo pelo qual a identidade do usuário possa ser verificada;

- Autorização: associar uma identidade a uma lista de direitos, privilégios, ou áreas de acesso;
- Não repúdio (ou legalidade): quando alguém não pode negar a autenticidade de um documento, a sua assinatura ou o seu envio;
- Auditoria: processo de assegurar que a atividade de um usuário possa ser devidamente registrada e revista para detectar eventos suspeitos.

Por derradeiro, há que se pontuar que o fenômeno da massificação, acarretado pela prática de "copiar e colar", deve ser evitado a todo custo, pois favorece a propagação de grande número de informações incorretas, com possibilidade de graves consequências.

Conclusões

Diante do exposto, chega-se às seguintes conclusões:

- O usuário do sistema de saúde é considerado hipervulnerável, pois à vulnerabilidade de seu estado de saúde soma-se a vulnerabilidade técnico-eletrônica.
- Deve-se reconhecer a extensão eletrônica dos direitos da personalidade, garantindo a tutela da personalidade virtual dos pacientes.
- Os substratos éticos da relação profissional de saúde-paciente devem ser salvaguardados em todas as situações, porém os aspectos particulares concernentes ao PEP devem ser sempre levados em conta, principalmente no sentido de resguardar a privacidade e a segurança dos pacientes.

Referências

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. Lei Nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil. Diário Oficial da União**, 11 jan. 2002.

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Diário Oficial da União, 12 set. 1990.

CENTRO DE BIOÉTICA DO CREMESP. Disponível em: <http://www.bioetica.org.br/>. Acesso em: 16 março 2015.

CONSELHO FEDERAL DE ENFERMAGEM. Resolução COFEN 311/2007, 08 de fevereiro 2007. Aprova a Reformulação do Código de Ética dos Profissionais de Enfermagem. Rio de Janeiro, 2007.

CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SANTA CATARINA. **Manual de orientação ética e disciplinar.** 2.ed.rev.atual. Florianópolis: Comissão de Divulgação de Assuntos Médicos 2000. Disponível em: <http://www.portalmedico.org.br/Regional/crmsc/manual/parte3b.htm>. Acesso em: 16 março 2015.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM Nº 1931/2009, 17 de setembro de 2009. Aprova o Código de Ética Médica. **Diário Oficial da União**, 24 set. 2009, seção I, p.90.

DICIONÁRIO ONLINE MICHAELIS. São Paulo: Melhoramentos, 1998-2009. Disponível em: < http://michaelis.uol.com.br/>. Acesso em: 16 março 2015.

MAIA, M.C. Telemedicina, prontuário eletrônico e atualização do código de defesa do consumidor. **Revista de direito do consumidor**, São Paulo, v.89, p.303-19, 2013.

SALVADOR V.F.M.; ALMEIDA FILHO, FGV **Aspectos Éticos e de Segurança do Prontuário Eletrônico do Paciente**. In: JORNADA DO CONHECIMENTO E DA TECNOLOGIA, UNIVEM, 2., Marília, São Paulo.

14

Segurança em Prontuário Eletrônico

Nélio Fernandes Borrozzino[1],
Raquel Franco Zambom[2],
Claudia Galindo Novoa Barsottini[3]
Ivan Torres Pisa[4]

Introdução

O prontuário médico é definido pelo Conselho Federal de Medicina (CFM) como um "*documento único composto pelo 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*" (BRASIL, 2002). Trata de informações contínuas de determinada pessoa, contendo seus dados pessoais, registros médicos, contemplando não apenas textos com evoluções médicas, mas também imagens e resultados de exames, tornando esse documento importante no tratamento do paciente, em sua segurança e na própria comunicação entre a equipe multidisciplinar (BRASIL, 2002; 2007).

1 Nélio Fernandes Borrozzino (nelio.borrozzino@informarsaude.com.br) é Especializando no Curso de Especialização em Informática em Saúde, UAB/UNIFESP, 3. ed.
2 Raquel Franco Zambom é Especializanda no Curso de Especialização em Informática em Saúde, UAB/UNIFESP, 3. ed.
3 Claudia Galindo Novoa Barsottini é Doutora em Informática em Saúde pela Universidade Federal de São Paulo, Professor(a) Adjunto(a) da UNIFESP e Coordenadora do Curso de Especialização em Informática em Saúde, UAB/UNIFESP, 3. ed.
4 Ivan Torres Pisa (ivanpisa@gmail.com) é Bacharel em matemática, Professor Adjunto do Departamento de Informática em Saúde, Escola Paulista de Medicina, UNIFESP e Vice-coordenador do Curso de Especialização em Informática em Saúde, UAB/UNIFESP, 3. ed.

Em ambiente físico tais arquivos médicos se tornam volumosos com o passar dos anos. Este aumento de volume no armazenamento dos prontuários, dos diversos estabelecimentos de saúde nacionais, sejam eles serviços de apoio, diagnóstico ou terapêuticos, insurgem como justificativa para elaborar novas tecnologias para armazenar e transferir dados em saúde.

Com a inovação tecnológica e o aumento do uso de sistemas computadorizados para controle de dados do paciente, o prontuário médico atinge o âmbito digital e em 23 de novembro de 2007 ocorre a publicação pelo CFM da Resolução nº 1.821/07, que 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 (BRASIL, 2002).

A tecnologia atrelada à área da saúde contribui de forma positiva aos cidadãos com um aumento significativo da qualidade desses serviços, especialmente quando o assunto é prontuário eletrônico do paciente, considerado como a principal ferramenta de tecnologia da informação e comunicação em saúde (TICs) que o profissional médico e a própria equipe multidisciplinar trabalharão em suas rotinas diárias (BRASIL, 2002; PINTO, 2006).

De forma semelhante aos cuidados já preconizados nos prontuários em papel, que incluem privacidade, sigilo e segurança das informações do prontuário do paciente, são temas que mereceram destaques nas regulamentações do CFM, regras e comportamentos que garantam a segurança do paciente e de sua informação. De forma mais abrangente, a própria Constituição Federal vigente de 1988, em seu art. 5º, inciso X dispõe que "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*", direito subjetivo fundamental, que não exclui essa garantia para o uso de informações individuais em saúde (BRASIL, 1988). Em complementação, as resoluções do CFM tratam o assunto de forma bastante específica, iniciando no Art. 1º da Resolução CFM nº 1.638/2002 ao citar o caráter sigiloso do documento e no Art. 3º e 4º da resolução CFM nº 1.821/07 que estabelece os níveis de garantia de

segurança 1 (NGS1) e 2 (NGS2), traçando diretrizes que regulamentam de forma voluntária essas questões.

Essa segurança consiste em garantir que a informação esteja protegida contra os acessos por pessoas não autorizadas, esteja sempre disponível quando necessária e que seja confiável e autêntica, ou seja, protegendo os dados de eventuais ameaças (SANTOS, 2012).

Normas (ISO e Certificação SBIS/CFM)

Para o gerenciamento da segurança na área da saúde, tendo em vista a sua criticidade, foi publicada em 2008 a norma internacional ISO 27799 de Gestão de Segurança da Informação em Saúde, com uma visão específica do setor de saúde para apoiar a interpretação de controles de segurança da informação. Esta norma fornece orientações às organizações que possuem informações pessoais de saúde sobre a melhor maneira de proteger a confidencialidade, integridade e a disponibilidade das informações através da implementação dos controles previstos na ABNT NBR ISO/IEC 27002 (ABNT, 2005). No Brasil, a Sociedade Brasileira de Informática em Saúde (SBIS) é quem está mais empenhada nesta área, contemplando aspectos de segurança dentro do seu processo de certificação dos sistemas de registros eletrônico de saúde (S-RES), juntamente com o CFM (Kobayashi; Feruje, 2007).

A Certificação SBIS-CFM não é obrigatória. A SBIS e o CFM não exigem que qualquer sistema seja certificado. O processo é voluntário. Sendo assim, a certificação pode ser entendida como uma opinião técnica, qualificada e imparcial de duas instituições dispostas a garantir a privacidade e confidencialidade da informação de saúde dos cidadãos, atender à legislação brasileira sobre documentos eletrônicos e melhorar a qualidade dos sistemas de informação em saúde (SBIS, 2013). Uma das principais motivações do CFM ao participar deste processo de certificação foi o de garantir o sigilo profissional, ou seja, que o acesso à informação identificada só possa ser feito por pessoas autorizadas. Aos interessados em eliminar o registro das informações em papel, é obrigatória a conformidade ao Nível de Garantia de Segurança 2 (NGS2), que contempla obri-

gatoriamente o uso de certificados digitais, conforme descrito abaixo. O processo de certificação SBIS-CFM classifica o S-RES do ponto de vista de segurança da informação, em dois Níveis de Garantia de Segurança (NGS) (SBIS, 2013).

> NGS1 - categoria aplicável a S-RES que não pretende eliminar a impressão dos registros em papel. Assim, mantém a necessidade de impressão e assinatura manuscrita;
> NGS2 - categoria constituída por S-RES que viabiliza a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. Para atingir o NGS2 é necessário que o S-RES atenda aos requisitos já descritos para o NGS1 e apresente ainda total conformidade com os requisitos especificados para o Nível de Garantia 2. Gottberg, Costa, Leão e Pisa (2012) ressaltam, ainda, que a segurança para diferentes serviços é exigida, porque o padrão estabelece os requisitos mínimos das proteções administrativas, técnicas e físicas necessárias à garantia da confidencialidade das informações em saúde.

Segundo Patrício, et Al (2011), com relação à complexidade da abrangência das normas técnicas, o sistema também precisa atender alguns requisitos: identificação e autenticação do usuário, controle de sessão do usuário, possibilidade de geração e recuperação de cópias de segurança, confiabilidade e segurança dos dados.

HIPAA e HL7

Um aspecto importante relacionado à segurança dos pacientes exposto em uma parte considerável de artigos internacionais é a utilização de padrões HIPAA. Criado em 1996 pelo Departamento de Saúde e Serviços Humanos dos Estados Unidos da América (US Department of Health and Human Services), como um conjunto de normas, no âmbito nacional norte-americano, para proteção de determinadas informações em saúde,

essas normas protegem em *stricto sensu* informações de saúde capazes de identificação: os dados pessoais, número de segurança social, data de nascimento e endereço, bem como informações em relação ao quadro de saúde e tratamento do paciente, seja no passado, na atualidade ou a serem realizados (HIPAA, 1996).

Outro padrão amplamente encontrado nos estudos é o Health Level Seven International (HL7), fundado em 1987, para fornecer regras sobre troca, compartilhamento, integração e recuperação de informações em saúde com rigor científico e conhecimentos técnicos para prática clínica e gestão. Preconizado pelo CFM, os PEP/RES também precisam se enquadrar em resoluções e normas para uma sustentação adequada de suas qualidade e segurança. Semelhante aos padrões encontrados nos estudos supra-citados, o próprio NGS1, mesmo sem a eliminação do documento em papel, traz diretrizes organizacionais e estruturais tão relevantes quanto as elencadas em outros países.

Outras medidas de segurança

Também com o objetivo de manter a segurança do PEP podem ser utilizados alguns mecanismos:

- Controle de acesso lógico: identificação e autenticação de usuários, normalmente com o uso de um ID (identificação do usuário) e uma senha (autenticação); gerência e monitoramento de privilégios; prevenção de acessos não autorizados (Brasil, 2012);
- Certificados digitais: são documentos eletrônicos que utilizam duas chaves, uma pública de conhecimento geral, e outra privada, que deve ser mantida em sigilo pelo titular do certificado (Salvador; Almeida Filho, 2005);
- Firewall: ferramenta de segurança e controle, com a função de limitar e controlar o acesso de terceiros a uma rede local interna (LAN Local Area Network) ligada a uma rede externa (Internet); controla e permite acessos somente a usuários autorizados evitando acessos indevidos (Martins; Santos, 2005);

- Backups: são cópias de segurança dos dados e arquivos, armazenando-os em outro local para o caso de perdas ou alterações indevidas (Carvalho, 2011);
- Log de auditoria: os arquivos de log são usados para registrar ações dos usuários, ótimas fontes de informação para auditorias futuras. Os logs registram quem acessou o sistema, quando foi feito o acesso e que tipos de operações foram efetuadas (Marciano, 2006).

Lopes (2009) afirma que esses mecanismos de segurança podem garantir um nível bastante elevado de confiabilidade e privacidade das informações dentro de um sistema de PEP, mas há necessidade de se criar políticas e práticas bem específicas e estruturadas de acesso a estas informações, objetivando a conscientização das pessoas quanto ao uso apropriado e seguro de sistemas informatizados. Para Bragança (Bragança; Luciano, 2010), é a participação dos usuários de sistemas que garante a segurança da informação. Eles desempenham um papel ativo na atividade de prevenir incidentes indesejáveis e proteger os ativos materiais e virtuais das organizações. Os usuários podem ainda contribuir com diversas ações seguras em seu dia a dia, como, por exemplo, bloquear sua estação de trabalho ao sair, adotar uma política de senhas, com trocas frequentes, cuidados no uso de e-mail e internet, uso de softwares licenciados e, principalmente, a comunicar falhas de segurança eventualmente detectadas.

Comentários finais

Cada vez mais as tecnologias estão fazendo parte do dia a dia das pessoas e organizações, sendo utilizadas para gerar transformações nos processos de armazenamento, comunicação e distribuição das informações. Na área da saúde, dentre outros objetivos, procuram melhorar a qualidade da assistência prestada e a tomada de decisão perante o grande número de informações geradas. A importância do(s) sistema(s) de saúde tem feito com que a confiabilidade e confidencialidade no acesso às informações dos pacientes e seus tratamentos seja um fator cada vez mais crítico.

O PEP armazena informações sobre a história clínica do paciente, de forma que todos os profissionais de saúde tenham acesso, auxiliando no diagnóstico e no tratamento da saúde de uma pessoa, possibilitando uma melhor assistência ao indivíduo. Essas informações também podem ser utilizadas para estudos e para a criação de novos conhecimentos. Os benefícios conquistados com o uso do PEP são grandes tanto para a população quanto para a administração da saúde. A implementação desta estratégia, por ser dependente de sistemas informatizados, adiciona à solução a complexidade de proteger os dados dos pacientes e sua privacidade.

O sigilo e a segurança das informações são notavelmente considerados no âmbito nacional e internacional. Atualmente, o próprio CFM emite o registro do conselho aos médicos com um chip para autenticação digital de assinatura objetivando um melhor controle e uma maior segurança no uso de tecnologias em saúde, a qual os registros médicos eletrônicos se incluem. Embora o próprio aspecto cultural e os objetivos governamentais, que englobam planejamentos estratégicos e ações com objetivos diferentes em comparação aos do Brasil com os demais países, a preocupação com a segurança das informações e com a privacidade do paciente se assemelham.

Os mecanismos e diretrizes norte-americanos apresentados são tão completos e detalhados quanto os preconizados pelas diretrizes brasileiras segundo o CFM e a SBIS. Porém, a problemática em manter as informações sigilosas não são extintas com o uso da tecnologia, embora se mostrem superiores aos prontuários de papel, e em grande parte dos estudos torna-se um importante fator que ainda carece de soluções e de novas ações.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BRAGANÇA, C.E.B.A.; LUCIANO, E.M.; TESTA, M.G. Segurança da Informação e privacidade de informações de pacientes de instituições de

saúde: uma análise exploratória da privacidade percebida pelos profissionais. In: ENCONTRO DA ANPAD, 34., Rio de Janeiro, 25-29 set. 2010. Disponível em: <http://www.anpad.org.br/admin/pdf/adi2653.pdf>. Acesso em: 24 jul. 2014.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 4.ed. Brasília, D.F.: Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Brasília, D.F.: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 1 jul. 2014.

BRASIL. Medida Provisória nº 2.200-2, de 24 de Agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial da União**, 27 ago 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 1 jul. 2014.

BRASIL. Resolução nº 1.638/2002, de 09 de Agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, 9 ago. 2002. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>. Acesso em: 1 jul. 2014.

BRASIL. Resolução nº 1.821/07, de 23 de Novembro de 2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. **Diário Oficial da União**, 23 nov. 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.htm>. Acesso em: 1 jul. 2014.

CARVALHO, I.R.F. **Segurança da informação**: um instrumento para avaliação do plano de continuidade de negócio aplicado em uma organização pública. 2011. Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras . Lavras, 2011.

CENTERS FOR MEDICARE AND MEDICAID SERVICES. Health Insurance Portability Accountability Act of 1996 (HIPAA). Disponível em: <http://www.cms.hhs.gov/hipaageninfo>. Acesso em: 1 jul. 2014.

GOTTBERG, H.; COSTA, T.M.; LEÃO, B.F. et al. **Revisão sobre normas e padrões de segurança da informação para o Registro Eletrônico em Saúde**. Disponível em: <http://www.sbis.org.br/cbis11/arquivos/910.pdf>. Acesso em: 1 jul. 2014.

HL7 International Inc. Disponível em: <http://www.hl7.org>. Acesso em: 1 jul. 2014.

KOBAYASHI, L.O.M.; FERUJE, S.S. Segurança em informações médicas: visão introdutória e panorama atual. **Revista Brasileira de Engenharia Biomédica**, v.23, n.1, p.53-77, 2007.

LOPES, A.C.F. **Segurança da informação versus prontuário eletrônico**: Hospital Geral de Fortaleza – CE. 2009. Trabalho de conclusão de curso apresentado à Escola de Saúde de Exército do Rio de Janeiro. Rio de Janeiro, 2009.

MARCIANO, J.L.P. Segurança da informação - uma abordagem social. 2006. Tese - Universidade de Brasília. Brasília, D.F., 2006.

MARTINS, A.B.; SANTOS, C.A.S. Uma metodologia para implantação de um sistema de gestão de segurança da informação. **J.Inf.Syst. Technol. Manag.** v. 2,n.2, p.121-136 2005.

PATRÍCIO, C.M.; MAIA, M.M.; MACHIAVELLI, J.L. et al. O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? **Scientia Medica**, v.21, n.3, p.121–31, 2011.

PINTO, B.V. Prontuário eletrônico do paciente: documento técnico de informação e comunicação do domínio da saúde. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, v. 21, p.34-48. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2006v11n21p34/329>. Acesso em: 1 jul. 2014.

SALVADOR ,V.F.M.; ALMEIDA FILHO, F.G.V. Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: JORNADA DO CONHECIMENTO E DA TECNOLOGIA UNIVEM, 2., Marília, 2005.

SANTOS, D.L.R.; SILVA, R.M.S. **Segurança da informação**: a norma ISO/IEC 27000 ISO/IEC. 2012. Trabalho de Segurança de Informação do MCI 2012/2013, Faculdade de Engenharia da Universidade do Porto, Porto, 2012.

SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE (SBIS). Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES), versão 4.1, 2013. Disponível em: <http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2013_v4-1.pdf>. Acesso em: 26 ago. 2014.

V

Acesso às informações em saúde: transparência e participação social

15

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*

Kleomara Gomes Cerquinho[1]
Wellington Tavares[2]
Irineu Amaro Vitorino[3]

Introdução

Atualmente é possível verificar um constante crescimento do interesse da sociedade em buscar informações e interações no ambiente virtual propiciado pela internet, também conhecido como ciberespaço. Estes espaços se constituem a partir do avanço das Tecnologias de Informação e Comunicação (TIC's) e das possibilidades que estas oferecem através de distintos tipos de ferramentas e recursos. Neste contexto, a oferta e demanda de serviços surgiram como extensão destas possibilidades comunicacionais e interacionais, levando inclusive o setor público a se inserir paulatinamente nesta dinâmica social a partir do que se tem convencionado denominar de Governo Digital.

1 Kleomara Gomes Cerquinho (kleomara@gmail.com) é Doutora em Administração e Professora Adjunta do Departamento de Administração da Universidade Federal do Amazonas.
2 Wellington Tavares é Doutor em Administração pela UFMG e Professor da Universidade Federal de Ouro Preto.
3 Irineu Amaro Vitorino é Mestrando em Administração da FUMEC e Professor da UNIP/Manaus.

Mais do que as relações de serviços, e ainda anterior a isso, parece haver um desejo de aproximação da sociedade em relação ao setor público com vistas a participar das formulações de políticas públicas, dos planos e programas de governo, bem como dos desafios de resolução de problemas e das proposições de melhorias sociais. Tal fato tem sido observado no aumento da participação social nos governos a partir da internet, a qual tem possibilitado acompanhar mais de perto as ações governamentais por meio de diversos tipos de espaços e ferramentas.

O campo criado a partir do entrosamento de parte do aparelho do Estado e das TIC's tem possibilitado uma série de experiências relacionais e comunicacionais, tanto nas formas unidirecionais ou bidirecionais, respectivamente, *e-government* e *e-participation*. Ou seja, a utilização dos espaços e ferramentas tecnológicas possibilitam tanto o oferecimento de informações e serviços por parte do Estado quanto também podem abrir novos canais de interlocução com a sociedade no ambiente virtual, possibilitando novas alternativas de participação cidadã na gestão pública.

No âmbito do Estado, a área da saúde se destaca como um setor carente de cuidados e reformas para conceder maior eficácia e qualidade dos serviços, bem como um setor que requer a solução de problemas históricos nas organizações e atividades que o constituem, principalmente se analisado o contexto brasileiro. Assim, a área da saúde se mostra como um dos principais campos governamentais que necessitam aproveitar os benefícios gerados pelo Governo Digital, em especial pelos desafios e necessidades de melhoria e por ser uma área de grande procura e de atenção da sociedade brasileira, assim como em outras várias partes do mundo.

O governo digital, foco deste estudo, tem se tornado um suporte muito grande para todos os países, proporcionando administrações públicas mais eficientes, oferecendo melhores serviços e respondendo às exigências de transparência e prestação de contas. (UNITED NATIONS, 2014). Compreendido o contexto relatado, surgem muitos questionamentos em relação à constituição e desenvolvimento das ferramentas e espaços criados pelo governo brasileiro em relação à área da saúde. Entre tantos questionamentos possíveis, este estudo busca responder à seguinte questão de pesquisa: Quais são as possibilidades de *e-government* e *e-participation* disponíveis na área da saúde pelo governo brasileiro e como têm sido gerenciados os recursos que estruturam estes elementos do governo digital?

A partir daí, este estudo pretende identificar as possibilidades de governo eletrônico na área da saúde no âmbito do governo federal brasileiro e analisar a gestão dos recursos tecnológicos utilizados, bem como os limites entre o *e-government* e o *e-participation*, conforme proposições de Cerquinho (2013) com base nos estudos de Arnstein (1967). Para o alcance destes objetivos, utilizou-se de uma metodologia composta por coleta de dados a partir de observação direta e navegação orientada, bem como de análise de conteúdo para o trato dos dados e fundamentação das discussões.

As seções que estruturam este estudo são, além desta introdução, a segunda seção que apresenta conceitos e características do Governo Digital e a terceira que traz discussões sobre a área da saúde e o uso da tecnologia. Na quarta seção é apresentada a metodologia que subsidiou esta pesquisa e na sequência, quinta seção, são apresentados os principais achados a partir da observação realizada no Portal da Saúde do Ministério da Saúde. Por fim, na sexta seção se apresentam as principais considerações sobre o presente estudo.

O Governo Digital

Governo Digital denota um tipo de governo e forma de governar, estruturado com bases na utilização da Tecnologia de Informação e Comunicação (TIC) e da internet, e ocorrendo de forma interativa por meio de espaços virtuais como *sites*, portais, redes sociais virtuais, entre outros (CERQUINHO, TAVARES e PAULA, 2014). São sinônimos deste conceito o Governo Eletrônico (RAMOS e RAMOS, 2003; PINHO, 2008; ROVER, 2008) e o Governo 2.0 (CERQUINHO, TAVARES e PAULA, 2014), sendo estas algumas das formas encontradas na literatura que trata do assunto.

De modo geral, este tipo de governo "tem se constituído em uma infraestrutura de rede compartilhada por diferentes órgãos públicos a partir da qual a gestão dos serviços públicos é realizada" (ROVER, 2008, p. 10).

O termo Governo Digital surge na contextualização deste estudo tentando abarcar dois conceitos que têm sido enfaticamente utilizados pela ONU para classificar os Estados-Membros: *e-government* e *e-partici-*

pation. Estes conceitos se desenvolveram em relação à utilização de tecnologias da informação e comunicação nas relações estabelecidas com os cidadãos por meio da internet.

O primeiro conceito, *e-government*, é definido a partir de uma concepção unidirecional, na qual os serviços públicos são ofertados por meio virtual e somente o estado demanda a interlocução, ainda que o cidadão o responda (RUELAS e ARÁMBURO, 2006; JARDIM, 2007; ALMEIDA JUNIOR, 2011; PERSEGONA e ALVES, 2011; DINIZ et. al., 2009). Já o segundo conceito, *e-participation*, também denominado de *I-government*, é definido a partir de um entendimento bidirecional, visto que a interação se torna uma via de mão dupla, a partir da qual o cidadão deixa de ser mero receptor ou respondente das informações provindas do estado, e passa a contribuir com este por meio de parcerias ou da formulação de demandas públicas (BHATNAGAR, 2006, KLAUS, 2009; BAUMGARTEN E CHUI, 2009; CERQUINHO, 2013).

De acordo com o E-*government* Survey 2014, documento elaborado pela Organização das Nações Unidas (ONU), o governo digital se apresenta como um suporte muito importante para os países, já que este permite que as administrações públicas em todo o mundo possam ser mais eficientes, oferecerem melhores serviços e responderem às exigências de transparência e prestação de contas. No âmbito deste contexto de virtualidade as Tecnologias de Informação e Comunicação (TIC's) provam ser eficazes na facilitação e no compartilhamento de conhecimentos, no desenvolvimento de competências, na transferência de soluções de governo inovadoras por meio eletrônico e na capacitação para o desenvolvimento sustentável entre os países-membros. Inclusive, este tipo de tecnologia pode possibilitar a geração de importantes benefícios sociais em setores como a educação e a saúde (UNITED NATIONS, 2014).

Em parte da literatura que trata do tema, é possível se encontrar outras denominações que versam sobre o tema governo digital, como, por exemplo, "governo eletrônico", já que o campo se encontra em construção e expansão. Neste sentido, Jardim (2007, p. 29) defende que "o tema 'governo eletrônico' insere-se num universo temático e teórico que expressa configurações político-informacionais emergentes, características da contemporaneidade, plasmadas no desenho de políticas públicas governamentais" (JARDIM, 2007, p. 29).

O *e-participation* é considerado uma evolução do *e-government*. Por meio dele o cidadão se torna ativo, participativo e, impulsionado pelos governos, passa a criar valor em conjunto com o Estado e a partir dos dados fornecidos publicamente (CERQUINHO, 2013). Desse modo, por meio da tecnologia o cidadão pode expressar sua opinião utilizando os mecanismos que lhe são possíveis, tais como a *e*-votação e a *e*-decisão, sendo a primeira a votação na forma virtual, tal como ocorre atualmente nos EUA e, a segunda, o poder que o cidadão exerce ao codesenhar opções políticas e coproduzir componentes de serviços e modalidades de entrega na área pública (UNITED NATIONS, 2014).

Todavia, apesar da tecnologia estar permitindo que as relações entre Estado e sociedade se modifiquem, três impactos podem restringir as ações do governo digital: a) governança sem efetividade; b) falta de rede adequada; e c) relutância em aceitar que o usuário participe na criação de aplicação e conteúdos (BAUMGARTEN e CHUI, 2009). Enfim, a vontade política também se torna necessária para que o uso da tecnologia governamental tenha êxito.

A saúde e o uso da tecnologia

A discussão em torno da tecnologia ligada à área da saúde envolve a pesquisa e produção de medicamentos e de equipamentos, desenvolvimento de procedimentos técnicos e de sistemas organizacionais, educacionais e de suporte, bem como a implantação de programas e protocolos assistenciais, por meio dos quais a atenção e os cuidados com a saúde são prestados à população (MINISTÉRIO DA SAÚDE, 2006).

Neste estudo, a tecnologia é abordada como instrumento da gestão governamental, ou seja, na forma como os organismos públicos de saúde têm se utilizado das Tecnologias de Informação e Comunicação (TIC's) para apresentar serviços públicos mais eficientes para os cidadãos por meio dos *sites* dos municípios, estados e da União. No Brasil, a tecnologia em saúde direcionada ao cidadão começou a ser utilizada em sistemas que apoiavam o agendamento de consultas médicas em hospitais e postos de saúde nos estados e municípios, o que foi considerado um avanço social (DINIZ, 2009).

Essa forma de gestão governamental na área da saúde foi avançando e criando interfaces entre conhecimento, tecnologia, ação governamental e sociedade, passando a representar um recurso importante para a qualificação da gestão descentralizada do Sistema Único de Saúde (SUS), principalmente quando começaram a ser empregadas na produção de respostas mais eficazes aos problemas que afetam os cidadãos (RIBEIRO, 2007).

As primeiras iniciativas no campo da tecnologia da saúde, de forma integrada, aconteceram com a criação do projeto de Descentralização On-Line (DOL) em 1999, realizadas pela Fundação Oswaldo Cruz com o apoio da extinta Secretaria de Políticas de Saúde do Ministério da Saúde (SPS/MS) que, à época, era responsável pela coordenação das reuniões da Comissão Intergestores Tripartite (CIT). Assim, o DOL foi desenvolvido para, entre outras atividades, facilitar o acesso público à agenda política da CIT e, também, divulgar opiniões, informações e análises desse público-alvo a partir de um espaço virtual de discussão. Nos primeiros 6 anos de trabalho, a implementação do projeto evidenciou algumas dificuldades para o desenvolvimento e sustentabilidade dessas iniciativas, como, por exemplo, ao mostrar que o público que recorreu a esse tipo de inovação ainda se apresentava como visitante e usuário, receptor da informação e pouco participativo na emissão de informação ou no compartilhamento de conhecimento (RIBEIRO, 2007).

Em 2005, o Ministério da Saúde lançou a Portaria n° 2.510/2005, a qual instituiu a Comissão para Elaboração da Política de Gestão Tecnológica no âmbito do Sistema Único de Saúde - CPGT. Em 2006, as Portarias n° 152/06 e 3.323/06 criaram a Comissão para Incorporação de Tecnologias do Ministério da Saúde (Citec), coordenada pela Secretaria de Atenção à Saúde (SAS) (BRASIL, 2010).

Já nos anos de 2007 e 2008 foram estabelecidos fóruns de debate que "identificaram como ponto de partida a necessidade de institucionalização de uma política nacional que orientasse a implantação da avaliação, incorporação e gestão de tecnologias no sistema de saúde." (BRASIL, 2010, p. 7). E, na sequência, vários debates ocorreram em torno da implementação da Avaliação de Tecnologias em Saúde (ATS). Em

2009, a Portaria nº 2.690/2009 instituiu a Política Nacional de Gestão de Tecnologias em Saúde e, por conseguinte, em 2010, foi elaborado o documento Política Nacional de Gestão de Tecnologias em Saúde (BRASIL, 2010).

Segundo o Ministério das Comunicações, atualmente, o Ministério da Saúde aderiu ao Governo Eletrônico - Serviço de Atendimento ao Cidadão (GESAC), conectando à Internet cerca de 13 mil unidades de saúde em todo o país (BRASIL, 2014b). Em termos de informação e interlocução governamental para com o cidadão, o Ministério da Saúde tem utilizado o Portal da Saúde com vários recursos tecnológicos que possibilitam a comunicação e interação junto à sociedade.

A metodologia

A metodologia aplicada a este estudo é qualitativa, descritiva, por observação direta e navegação orientada. Qualitativa por se tratar de um estudo de análise de conteúdo com base nos estudos de Bardin (2009), pois este estudo foi realizado por meio da interpretação das informações contidas no Portal da Saúde de forma objetiva e sistemática.

A observação direta se deu pela análise no Portal da Saúde nos meses de novembro e dezembro de 2014, no espaço destinado ao Cidadão. Foram, portanto, visualizados os *links*: Principal, Saúde para você, Orientação e Prevenção, Ações e Programas, Comunicação, Legislação, Redes Sociais e Entenda o SUS.

Para a navegação orientada optou-se pela ordem em que se encontram os dados no Portal da Saúde, a fim de seguir mais detidamente os direcionamentos com relação aos temas estudados. Portanto, neste caso foram analisados os seguintes elementos no espaço Cidadão: Principal, Saúde para você, Orientação e Prevenção, Ações e Programas, Comunicação, Legislação, Redes Sociais e Entenda o SUS.

A análise da participação foi baseada nos degraus de Arnstein (1967), os quais direcionam este estudo. O Quadro 1 é disposto, a seguir, para um melhor entendimento do que cada degrau representa e como forma de subsidiar as discussões.

Quadro 1: Escada de participação de Arnstein (1967) na forma conceitual

Degraus de poder	Definição (Arnstein)	Comentário sobre o nível de participação
NÃO PARTICIPAÇÃO		
1 – Manipulação	As pessoas são colocadas em comitês ou conselhos consultivos, para que os técnicos do setor público eduquem e aconselhem os cidadãos.	Em vez de uma verdadeira participação cidadã, o degrau mais baixo da escada significa a distorção da participação em um veículo de relações públicas por tomadores de decisão.
2 - Terapia	Os cidadãos são inseridos em reuniões de participação popular, para orientação de como proceder com o poder público.	O que torna esta forma de "participação" desagradável é o fato de que os cidadãos estão envolvidos em atividades extensas, mas o foco é curá-los de sua "patologia", ao invés de mudar o racismo e a vitimização que criam suas "patologias".
SIMBOLISMO		
3 – Informação	As pessoas são informadas de seus direitos, responsabilidades e opções com relação ao poder público.	Primeiro passo importante em direção à participação cidadã, contudo, com muita frequência, a ênfase é colocada em um fluxo unidirecional de informações - de funcionários para os cidadãos - sem canal de *feedback* e nenhum poder de negociação. Sob essas condições, as pessoas têm pouca oportunidade de influenciar o programa concebido "para seu benefício".
4 – Consulta	Os cidadãos participam por meio de pesquisas de opinião, assembleias de bairro e audiências públicas.	Saber as opiniões dos cidadãos pode ser um passo legítimo para a sua plena participação. Mas, se a consulta não for combinada com outros modos de participação, esse degrau da escada ainda é ritual de fachada, uma vez que não oferece nenhuma garantia de que as ideias e preocupações dos cidadãos serão levadas em consideração.
5 – Apaziguamento	As pessoas são envolvidas em comitês e colegiados deliberativos para emitir sua opinião.	Neste nível, os cidadãos começam a ter algum grau de influência, mas ainda pode ser aparente, se "alguns" escolhidos forem inseridos em agências de ação comunitária ou em órgãos públicos e não conseguirem formar número suficiente para passar as demandas da comunidade.

(continua)

(continuação)

Degraus de poder	Definição (Arnstein)	Comentário sobre o nível de participação
PODER DO CIDADÃO		
6 – Parceria	Os cidadãos participam compartilhando com o governo o planejamento e as responsabilidades de tomada de decisão por meio de conselhos paritários, comitês de planejamento e mecanismos de solução de conflitos.	Neste degrau da escada o poder é de fato redistribuído por meio de negociação entre cidadãos e tomadores de decisão. Há compartilhamento do planejamento e das responsabilidades de tomada de decisão por meio de estruturas de políticas conjuntas, comitês de planejamento e mecanismos para a resolução de impasses. Há mais eficácia quando existe uma base organizada na comunidade.
7 – Poder delegado	As pessoas participam assumindo poder deliberativo em um determinado plano ou programa público.	Neste nível os cidadãos detêm "cartas" significativas de poder para assegurar a responsabilidade sobre programas públicos. Os tomadores de decisão precisam fazer um processo de negociação para poder encaminhar os projetos.
8 – Controle cidadão	Os cidadãos participam gerindo um programa público ou uma organização, assumindo a responsabilidade pela definição das ações e os aspectos gerenciais, sendo capaz de negociar as condições sob as quais "pessoas externas" poderão introduzir mudanças.	Neste nível as exigências para os controles do cidadão ao poder público aumentam. As pessoas exigem o grau de poder que garanta aos participantes ou moradores da comunidade governar um programa ou instituição em termos políticos ou gerenciais e ser capaz de negociar como a "pessoa pública" poder alterá-los.

Fonte: Adaptado de Cerquinho (2013).

Como já informado, o Ministério da Saúde tem utilizado o Portal da Saúde para realizar um conjunto de atividades e, de acordo com esta pesquisa, conta com todos os recursos tecnológicos que estão identificados aqui. Apesar da importância deste Portal para a comunicação com o cidadão, durante a pesquisa não foi possível encontrar informações relevantes, como o ano de sua criação e nem seus objetivos. Além disso, tal espaço de comunicação e interação não consta como parte estratégica da Política Nacional de Gestão de Tecnologias em Saúde.

Na catalogação dos termos *e-government* e *e-participation* foi utilizado o estudo de Cerquinho (2013). O uso desse estudo serviu para sepa-

rar os dois termos e suas ferramentas de *Web* e *Web* 2.0, a fim de identificar os limites de participação do cidadão no Portal da Saúde.

No *e-government* as ferramentas consideradas para este estudo são as de *Web* (mais estáticas no seu uso, segundo a autora), ou seja, *e-mail*, *blog*, *site* informativo (notícias), perguntas frequentes, fale conosco, atendimento *online*, entre outras ferramentas com informação ou conversa unilateral (CERQUINHO, 2013).

No *e-participation* foram analisadas as ferramentas interativas da *Web* 2.0 – fórum, comunidades, redes sociais (como as atuais *Twitter*, *Facebook*, *Google* +, *Youtube*, *Flickr*, *Linkedin*), *chat* e *wiki* – as quais permitem uma maior interlocução e participação do cidadão, considerando que há interação, criação, integração, parceria, colaboração, avaliação, entre outras atividades realizadas entre governo e sociedade. Incluem-se nesse estágio as plataformas avançadas criadas e implantadas pelos governos que desenvolvem a participação política do cidadão via governança (CERQUINHO, 2013).

A Figura 1 que compõe a metodologia de análise, por conseguinte, pode ser desenhada envolvendo os estudos de Arnstein (1967) e Cerquinho (2013).

Figura 1: Limites de participação cidadã no Governo digital

Fonte: Atualização do modelo elaborado por Cerquinho (2013)

Vistos os degraus de participação cidadã, conceitos e ferramentas disponíveis no Portal da Saúde, na próxima seção são apresentadas as principais informações encontradas e as discussões a respeito destas.

A observação no Portal da Saúde

Administrado pela Assessoria de Comunicação Social, o Portal da Saúde é acessado pelo link <http://portalsaude.saude.gov.br/>. No local são encontradas as grandes áreas: Cidadão, Profissional e Gestor, O Ministério, Serviços, Biblioteca e Acesso a Informação.

A área "Cidadão", elemento desta pesquisa, contém os *links* que levam para as seções: Principal; Saúde para você; Orientação e Prevenção; Ações e Programas; Comunicação; Legislação; Redes Sociais; e Entenda o SUS. Cada uma destas seções foi analisada, sendo possível identificar que:

a) Principal – nesta seção encontram-se as "Notícias", "Serviços", "O Ministério", "Transparência", "Redes e Programas", Orientação e Prevenção (*link* para a página que está na parte do Espaço cidadão), SUS (*link* para a página "Entenda o SUS"), Sobre o Ministério (duplicidade de *link* para a página "O Ministério"), Saúde para você (*link* para a página que está na parte do Espaço cidadão), os Acessos (ícones que levam a algumas das páginas do Principal, tal como a de Transparência) e a disponibilização de telefones, bem como ícones das redes sociais utilizadas pelo Ministério da Educação.

O "Principal" é uma mescla de variadas informações e, ao se observar com maior profundidade, um direcionador para os outros espaços destinados ao cidadão. Quando os espaços aqui apresentados se tornaram redundantes, optou-se, nesta pesquisa, por tratá-los no espaço mais abrangente destinado ao assunto, focando a análise nos espaços com informações exclusivas de cada seção.

O "*Notícias*" apresenta o que há de informações gerais sobre saúde no Brasil. Há também nessa parte uma rádio acoplada ao Portal (*web* rádio saúde) que toca músicas brasileiras, um *link* para vídeos e outro *link* para imagens que apresentam notícias sobre a saúde no Brasil.

Os "*Serviços*" estão separados em: *Cartão SUS* – local onde as pessoas (usuários e profissionais de saúde) se inscrevem para obter a identificação do SUS, bem como para receber informações a respeito do que seja este cadastro; *CNES – Estabelecimento de saúde*, o qual indica a locali-

zação de todos os estabelecimentos particulares ou públicos cadastrados para o atendimento no SUS por estado e município, com a apresentação de suas competências médicas (contudo, nem todos apresentam); *Farmácia popular* é o *link* que leva à página do programa, a qual apresenta sua contextualização, a indicação da localização das farmácias de rede própria e particulares, bem com a lista dos medicamentos disponíveis; *CONITEC* é o *link* que leva à página da Comissão Nacional de Incorporação de Tecnologias do SUS, a qual descreve suas atividades junto à incorporação de novas tecnologias medicamentosas e também permite a participação popular por meio de consulta pública com base na exigência legal do Decreto nº 7.646, de 21 de dezembro de 2011 (art. 19); *SIOPS* é *link* para a página do Sistema de Informações Sobre Orçamentos Públicos em Saúde, o qual disponibiliza informações sobre despesas em saúde de todos os entes federados. No caso deste estudo, foram acessados os dados dos município de Manaus e do Rio de Janeiro para verificação e, no entanto, ambos não disponibilizam as informações de 2014, mas apenas as frases "Dados não homologados pelo gestor" ou "Município não transmitiu os dados"; e *Ciência e tecnologia*, a qual apresenta a Portaria nº 3.089/2013, que redefine a lista de produtos estratégicos para o Sistema Único de Saúde (SUS) e as regras e critérios para sua definição (a página está sem inserção de informação desde dezembro de 2013).

O espaço *"O Ministério"* apresenta com mais detalhes as informações sobre o Ministério da Saúde, sua atuação, sua história ao longo dos anos, bem como seus órgãos e unidades vinculadas.

O componente "*Transparência*" encaminha para variados acessos à Informação: Ações e Programas, Licitações, Auditorias, Despesas, Convênios e Repasses, Transparência da Saúde, Relatório de Gestão, Consulta Pública, Servidores, SargSUS, Índice de Desempenho do SUS, Sistema Eletrônico do Serviço de Informações ao Cidadão (e-SIC), Sala de Apoio à Gestão Estratégica (SAGE) e Redes e Programas; neste grupo de informações, o Ministério presta suas contas ao cidadão e inclusive destina espaços para o cidadão solicitar as informações sobre as contas da saúde. Buscou-se pesquisar os mesmos municípios em relatórios de 2013, sendo que o do Rio de Janeiro não tinha repassado a informação e o de Manaus estava em diligência. Já os dados de 2012 e de outros anos estavam disponibilizados.

O espaço *"Rede e Programas"* reúne um grupo de ícones que direcionam para a página explicativa dos respectivos programas, os quais, de certa forma, repetem as informações dos programas de forma mais simples.

Assim, após observar a seção "Principal" sob os limites averiguados neste estudo, ela se encontra no nível de *e-government*, atingindo o *Degrau de Informação* proposto por Arnstein (1967). Contudo, em espaços como "serviços", o usuário do portal pode, além das informações, requerer certos serviços.

b) Saúde para você – esta seção apresenta espaços específicos sobre Saúde da Mulher, do Idoso, Pessoas com Deficiência, do Homem, Mental, Sistema Penitenciário, do Trabalhador, Jovens e Adolescentes.

Cada um desses espaços possui um *link* que leva a informações sobre o assunto de que trata. Em geral as informações são voltadas para orientação dos programas de saúde existentes. O *link* do programa de Saúde do Trabalhador está quebrado direcionando para o aviso "A página solicitada não pôde ser encontrada". Dessa forma, após observar o "Saúde para você" sob os limites apresentados neste estudo, ela se encontra no nível de *e-government*, atingindo o *Degrau de Informação* proposto por Arnstein (1967).

c) Orientação e Prevenção – nesta seção, segundo o que se lê no Portal, o cidadão encontra informações sobre promoção e proteção da sua saúde, apresentando alguns dados especiais sobre algumas doenças e as políticas e ações do Ministério da Saúde para o controle dessas enfermidades.

Os dados especiais em alguns espaços referem-se às doenças contagiosas mais comuns, entre outras informações sobre: tabagismo; transplantes; calendário de vacinação; alimentação saudável; e medicamentos. Algumas dessas orientações possuem páginas específicas e bem trabalhadas, tais como o caso da AIDS a qual possui página própria e a do Transplante com suas explicações e estatísticas; algumas como a do Tabagismo, não trabalha a prevenção, mas apenas informações sobre as leis e locais em que a pessoa não pode fumar; outras, tais como as de Diabetes, Hipertensão, estão com os *links* quebrados direcionando para o aviso "A página solicitada não pôde ser encontrada". Neste item é trabalhada

a informação, dessa forma atinge o *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e-government*.

d) Ações e Programas – nesta seção são encontrados vinte e um (21) dos Programas oferecidos pelo Ministério da Saúde, tais como: Provab, Academia da Saúde, Saúde da Família, Mais Médicos, Melhor em Casa, Família Popular. Cada programa tem sua própria página com notícias e informações. Algumas dessas páginas são simples – tal como a do Provab -, outras mais elaboradas – como a do Mais Médicos - e outras estão quebradas – como a Academia da Saúde. A parte "Ações e Programas" foi elaborada para distribuir informação, dessa forma atinge o *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e-government*.

e) Comunicação - sob a responsabilidade direta da Assessoria de Comunicação Social, nesta seção são divulgadas informações sobre a imagem, a missão e as ações, bem como objetivos estratégicos do ministério. Esta é uma área da Assessoria de Comunicação Social que administra o Portal da Saúde e nela são encontradas informações tais como: um calendário de datas comemorativas em geral; os materiais usados em campanhas de saúde dos anos 2013 e 2014; o *link* para a página Publicidade que está em manutenção para mudança de linguagem em sua plataforma desde 28 agosto 2013. A "Comunicação" foi destinada também para a informação. Assim como os itens anteriores, alcança o *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e-government*.

f) Legislação – nesta seção são encontradas a Legislação básica do SUS, o Saúdelegis e o Alertalegis. É possível se encontrar desde o *link* para a Constituição até os *links* para a Legislação básica do SUS. O Saúdelegis é o local onde o cidadão pode pesquisar as normas legislativas da saúde, desde que saiba o que está procurando, visto que a informação é direcionada. O Alertalegis leva à página da Biblioteca Virtual em Saúde, porém o *link* está quebrado, apresentando a seguinte informação "Página inexistente. Por favor, retorne à página principal". A seção "Legislação"" foi proposta para transmitir leis em nível de informação. Atinge, portanto, o *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e--government*.

g) Redes Sociais - o Ministério da Saúde informa que atua no diálogo e na aproximação do governo federal com a sociedade, pois as "infor-

mações divulgadas são ações de saúde pública que auxiliam na melhoria da qualidade de vida do cidadão, seja para a promoção da saúde, prevenção de doenças ou adesão da população às mobilizações de campanhas" (BRASIL, 2014a).

Nesta seção encontram-se *Blog* da Saúde, *Facebook*, *Ask.fm*, *Twitter*, *Slideshare*, *Youtube* e *Soundcloud*.

O *Blog da Saúde* é utilizado para repasse de notícias do Ministério.

O *Facebook* da Saúde, com 973.963 curtidas, serve para repassar as informações das campanhas do Ministério e esclarecer dúvidas dos internautas quanto aos procedimentos de atendimento pelo SUS.

O *Ask.fm* está com o *link* quebrado.

No *Twitter*, com 280 mil seguidores, o Ministério da Saúde repassa informações mais curtas (característica do *Twitter*) sobre a saúde, incluindo *links* para o cidadão que queira informações mais completas fora da rede social.

O *Slideshare* é utilizado como uma biblioteca virtual dos documentos das campanhas de saúde, disponibilizando trezentos e dezessete (317) documentos e dois (02) infográficos no local.

O *Youtube*, com 5.088 inscritos, oferece uma variedade de vídeos com informações e campanhas publicitárias sobre saúde.

O *Flickr* tem disponibilizadas as fotografias das ações dos vários órgãos do Ministério.

No *Soundcloud*, o Ministério disponibiliza suas campanhas por meio de áudio. Apesar de todas essas ferramentas de *Web* 2.0 estarem sendo utilizadas pelo Ministério da Saúde e permitirem maior participação, além da Consulta, ainda não estão sendo utilizadas para tal fim.

Assim, apesar da sua potencialidade, as redes sociais ainda se encontram no *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e-government*.

h) Entenda o SUS – por fim, esta seção apresenta o Direito dos usuários do SUS, Entendendo o SUS, SUS: a saúde do Brasil, Participanet SUS, Mesa de Negociação do SUS, Painel de Indicadores, Conselhos e Portarias.

No *Direito dos usuários do SUS*, o *link* está quebrado, ou seja, não há informação.

O *Entendendo o SUS* é uma cartilha de vinte e oito (28) páginas que tem a finalidade de reunir informações essenciais sobre o Sistema Único de Saúde para apresentar temas que envolvem a saúde pública no Brasil aos jornalistas e demais profissionais de comunicação.

O *SUS: a saúde do Brasil*, é uma exposição de mesmo nome, que já percorreu vários estados brasileiros e foi exibida na sede da Organização Pan-Americana da Saúde, nos EUA e pode ser visitada virtualmente, no *site* do Centro Cultural do Ministério da Saúde (CCMS) – não há um *link* para a exposição.

O *Participanet SUS* é destinado a gestores de saúde e, para ter acesso à página, o Ministério solicita uma inscrição.

A *Mesa de Negociação do SUS* é o espaço destinado a informar quais são as mesas e quais suas atividades. Nela participam, presencialmente, grupos e pessoas ligadas a saúde para "implementar novas metodologias para aprimoramento do processo de negociação do trabalho no âmbito do SUS, bem como orientar o desenvolvimento das estratégias e metodologias de negociação do trabalho, visando ao atendimento das demandas, utilizando formas de resoluções de conflitos decorrentes das relações de trabalho, tendo em vista as finalidades, princípios e diretrizes do Sistema Único de Saúde." (BRASIL, 2014). Apesar dessa informação, os dados de nenhuma das mesas estão disponibilizados no Portal.

O *Painel de Indicadores* não tem *link*, e apresenta apenas a seguinte informação "Cerca de 55% da população brasileira está coberta pelo Serviço de Atendimento Móvel de Urgência e Emergência (Samu 192). Atualmente, o Serviço já funciona em 1.150 municípios do país" (BRASIL, 2014a).

Os *Conselhos* são *links* para as páginas do CNS - Conselho Nacional de Saúde, do Conass - Conselho Nacional dos Secretários de Saúde (*link* quebrado), e do Conasems - Conselho Nacional das Secretarias Municipais de Saúde.

As *Portarias* são *links* que levam para a Portaria nº 2.230/2009 a qual dispõe sobre a aplicação da Portaria nº 2.048/GM/2009 (sobre o Regulamento do Sistema Único de Saúde (SUS)) e para a Portaria nº 2.048/2009 (aprovação do Regulamento do Sistema Único de Saúde (SUS)).

Como se nota a natureza informativa desta seção, ela se encontra no *Degrau da Informação* (ARNSTEIN, 1967) apresentando o nível de *e-government*.

Na seção seguinte são realizados alguns aprofundamentos nos dados verificados na pesquisa, bem como se realiza uma comparação entre as seções pesquisadas com vistas a dar compreensão sobre os limites existentes entre os conceitos e práticas de *e-government* e *e-participation*.

O Portal da Saúde nos limites entre e-government e e-participation

Após a verificação de cada elemento, pôde-se elaborar o Quadro 2. Nele foram inseridas informações que delineiam os limites entre *e-government* e *e-participation* no Portal da Saúde, de forma mais clarificada e simplificada, de acordo com os resultados encontrados e para uma melhor visualização desta pesquisa.

Quadro 2: Limites em e-government e e-participation no Portal da Saúde

Seção do Portal Saúde	Público-alvo	Interlocução permitida ao cidadão	Nível da ferramenta	Limite
Principal	Cidadão	Informação/consulta	*Web*	*e-gov*
Saúde para você	Cidadão	Informação	*Web*	*e-gov*
Orientação e prevenção	Cidadão	Informação	*Web*	*e-gov*
Ações e programas	Cidadão	Informação	*Web*	*e-gov*
Comunicação	Cidadão	Informação	*Web*	*e-gov*
Legislação	Cidadão	Informação	*Web*	*e-gov*
Redes sociais	Cidadão	Informação	*Web e Web 2.0*	*e-gov*
Entenda o SUS	Cidadão	Informação	*Web*	*e-gov*

No Quadro 2 observa-se que a tendência maior no Portal da Saúde é pelo uso de ferramentas de *Web* e pelo nível de serviço *e-government*. Contudo, vale ressaltar que o Portal já atinge o nível de consulta, podendo evoluir para níveis mais altos de participação se assim o Ministério da Saúde permitir, já que possui ferramentas de *Web* 2.0, a exemplo do *Facebook* e *Twitter* que vêm sendo utilizados, apesar do uso abaixo de suas potencialidades.

O uso de ferramentas e espaços de *e-government* demonstra a capacidade do governo em expandir os espaços disponíveis para serviços de saúde, seja em relação às informações, prevenção e combate a doenças, como também em relação aos cuidados (ou necessidade destes) sobre distintos grupos de pessoas e doenças que requerem maior atenção por meio de políticas e programas. A expansão destes serviços para o espaço virtual (ciberespaço) permite ampliar as possibilidades de atenção ao cidadão nesta área, oferecendo uma série de informações importantes, o que possivelmente não ocorre nos espaços físicos disponíveis para o trato da saúde no país.

Além disso, pode-se notar que a não utilização de ferramentas com finalidades de *e-participation* pode limitar as interações entre governo e sociedade, relegando assim um papel passivo ao cidadão que busca se aproximar do Governo Digital. Há que se pensar inclusive que a falta de iniciativas concede um caráter excludente em termos de participação e pode gerar uma sensação de impotência no cidadão diante dos problemas enfrentados na área da saúde no Brasil. Ainda, é possível inferir que a falta de ferramentas e espaços de participação não permite que fóruns temáticos nacionais possam abordar assuntos locais de interesse global e levar ao compartilhamento de problemas e posteriores soluções coletivas e em rede.

Considerações finais

Este estudo teve por objetivo analisar a gestão do Portal da Saúde em termos de navegabilidade do cidadão, utilizando para tanto os limites entre o *e-government* e o e-*participation* propostos por Cerquinho (2013), composto com os estudos de Arnstein (1967) sobre degraus de participação.

A metodologia aplicada ao estudo foi a análise de conteúdo de Bardin (2009) com observação direta e navegação orientada. A pesquisa aconteceu entre os meses de novembro e dezembro de 2014 no Portal da Saúde do Brasil. Os resultados indicaram que a gestão do Portal da Saúde está nos dois primeiros Degraus de participação do Simbolismo

(Informação com maior incidência e Consulta com menor incidência), apresentando um nível de *e-governmen*t.

Os destaques positivos em termos de participação cidadã é que o Portal já utiliza ferramentas de *Web* 2.0, no espaço destinado às Redes Sociais, o que lhe permite ir mais além da Consulta se a vontade política caminhar nessa direção, permitindo que o cidadão possa participar ativamente nas políticas públicas utilizando a tecnologia. Outro destaque do Portal é a *Web rádio saúde* que funciona 24 horas.

Outra situação que sobressai, mas de modo inverso, é a quantidade de *links* quebrados no Portal – a exemplo do programa de Saúde do Trabalhador, das páginas de orientações sobre Diabetes, Hipertensão, entre outros, e um em manutenção desde 2013 – a página Publicidade. Neste caso, os gestores do Portal precisam atualizar os *links* quebrados e verificar o porquê da página de Publicidade ainda está em manutenção depois de tanto tempo, a fim de que seja disponibilizada toda a informação necessária para o cidadão. Também cabe repensar onde inserir o *ParticipanetSUS*, pois ele se destina a gestores de saúde e não ao cidadão comum.

A importância deste estudo é explicada em função do pouco e crescente conhecimento que se tem dos limites práticos existentes entre *e--government* e *e-participation* para a academia e o Ministério da Saúde. Assim, por meio de estudos como este, é possível levar à compreensão da necessidade de avançar no oferecimento de plataformas mais participativas, a fim de que o cidadão possa não só receber informações no *site* ou via consulta, mas também requerer e opinar por meio das TIC's, em programas, projetos e ações de saúde pública no país.

Assim, este estudo contribui teoricamente para o avanço nos entendimentos sobre Governo Digital e, especialmente, para o esclarecimento da natureza dos conceitos de *e-government* e *e-participation*. Já a contribuição empírica está no esclarecimento sobre a aplicação destes conceitos na prática e o distanciamento que estes provocam quando desenvolvidos separadamente, já que um se aplica mais sobre serviços e informações e o outro sobre a participação e demandas dos cidadãos.

As limitações deste estudo se deram pelo fato do tempo de espera da finalização das eleições presidenciais para poder se iniciar a pesquisa, já que o Portal se encontrava "fechado" para acesso durante o período

eleitoral. Além disso, foram encontradas dificuldades com relação à busca de dados sobre governo digital no Ministério da Saúde, visto que o que dispõem está concentrado no Portal Saúde.

Pesquisas futuras na área podem analisar as redes sociais para identificar qual o perfil do público que participa *versus* o público-alvo pretendido pelo Ministério da Saúde. Sugere-se também que se parta para análises das páginas dos Conselhos na Saúde, visando compreender quais seus objetivos e o público-alvo a quem se destina, bem como para análises dos dados abertos disponibilizados na prestação de contas públicas, a fim de verificar essa relação.

Referências

ALMEIDA JÚNIOR, A. de. O governo não quer ser seu amigo. **Correio Braziliense**, Brasília, 23 ago. 2011. p. 4.

ARNSTEIN, S. A. Ladder of citizen participation. **Journal of the American Planning Association**, London, v.35, n. 4, p. 216-224, 1967.

BARDIN, L. **Análise de Conteúdo**. Lisboa: Edições 70, *2009.*

BAUMGARTEN, J.; CHUI, M. E-government 2.0. **Mckinsey on government,** n. 4, p.26-31,jul.2009. Disponível em: <http://www.mckinsey.com/clientservice/publicsector/pdf/TG_MoG_Issue4_egov.pdf>. Acesso em: 16 jan. 2010.

BHATNAGAR, S. Paving the road towards pro-poor e-Governance: findings and observations from Asia-Pacific case studies. Paving the Road towards pro-poor e-governance, 2006, Bangkok. **Workshop Report**. Bangkok: UNDP, Asia Pacific Development Information Programme, 2006. Disponível em: <http://www.apdip.net/projects/e-government/capblg/casestudies/Overview.pdf>. Acesso em: 19 jan. 2012.

BRASIL. Ministério da Saúde. Avaliação de Tecnologias em Saúde: institucionalização das ações no Ministério da Saúde. Rev. Saúde Pública [online]. 2006, v.40, n.4, p. 743-747. Disponível em: <http://www.rsp.fsp.usp.br>

BRASIL. Ministério da Saúde. **Política Nacional de Gestão de Tecnologias em Saúde**. Brasília, D.F., 2010. 48 p.

BRASIL. Ministério da Saúde. **Portal da Saúde.** Disponível em: <http://portalsaude.saude.gov.br/>. Acesso em: 6 nov. 2014.

BRASIL. Ministério das Comunicações. **GESAC**. Disponível em: <http://www.mc.gov.br/gesac>. Acesso em: 10. nov. 2014b.

CERQUINHO, K. G. **Governo eletrônico**: a gestão da relação estado-sociedade no uso da internet. 2013. 173p. Tese - Universidade Federal de Minas Gerais. Belo Horizonte, 2013.

CERQUINHO, K. G.; TAVARES, W.; PAULA, A. P. P. Governo eletrônico: os limites conceituais e práticos entre *e-government* e *e-participation*. In: ENCONTRO ANUAL DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM CIÊNCIAS SOCIAIS, 38., 2014, Caxambu. **Anais**... Caxambu: ANPOCS, 2014.

DINIZ, E. H. et al. O governo eletrônico no Brasil: perspectiva histórica a partir de um modelo estruturado de análise. **Revista de Administração Pública - RAP**, Rio de Janeiro, v.43, n.1, p. 23-48, 2009.

JARDIM, J. M. Governo eletrônico no Brasil: o portal rede governo. **Arquivística Net**, Rio de janeiro, v. 3, n.1, p. 28-37, jan./jun. 2007. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/journals/2/articles/30773/public/30773-32930-1-PB.pdf>. Acesso em: 2 nov. 2009.

KLAUS, P. Participation and e-democracy: how to utilize *web* 2.0 for policy decision-making. In: CHUN, A. S.; SANDOVAL, R.; REGAN, P. (Ed.). ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 10., 2009, Puebla, Mexico. **Proceedings**... Puebla, Mexico: Digital *government* Society of North America, 2009. p. 254-263. Disponível em: <http://eprints.qut.edu.au/41614/>. Acesso em: 20 jan.2012.

PERSEGONA, M. F. M.; ALVES, I. T. G. **História da Internet**: origens do e-gov no Brasil. Disponível em: <http://www.unbcds.pro.br/conteudo_arquivo/280606_1e4182.pdf>. Acesso em: 10 fev. 2011.

PINHO, J. A. G. Investigando portais de governo eletrônico de estados no Brasil: muita tecnologia, pouca democracia. **Revista de Administração Pública - RAP**, Rio de Janeiro, v.42, n.3, p. 471-93, maio/Jun., 2008.

RAMOS, R. E. B.; RAMOS, A. S. M. As práticas internacionais de estratégia de governo eletrônico e inclusão digital e as perspectivas para estratégia de política pública no Brasil: os casos de Estados Unidos, Reino Unido e Canadá. In: ENCONTRO ANUAL DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM ADMINISTRAÇÃO ENANPAD, 27., 25-29 set. 2003. **Anais**... Atibaia: Anpad, 2003.

RIBEIRO, P.; SOPHIA, D. C.; GRIGÓRIO, D. A. Gestão governamental e sociedade: informação, tecnologia e produção científica. **Ciência e Saúde Coletiva**, v. 12, n. 3, p. 623-631, 2007.

ROVER, A. J. O governo eletrônico e a inclusão digital: duas faces da mesma moeda chamada democracia. In: ROVER, A. J. (Ed). **Inclusão digital e governo eletrônico**. Zaragoza: Prensas Universitárias de Zaragoza, 2008. p. 11-38. (Lefis, 3)

RUELAS, A. L.; ARÁMBURO, P. P. El gobierno electrónico: su estúdio y perspectivas de desarrollo. **UniREVISTA**, São Leopoldo, v. 1, n. 3, jul. 2006. 11 p.

UNITED NATIONS. **E-*government* Survey 2014**: e-*government* for the future we want. Department of Economic and Social Aff airs. United Nations: New York, 2014. 144 p. Disponível em: <http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf >. Acesso em: 11 out. 2014.

16

Lei de acesso à informação (Lei nº 12.527/2011) e administração pública: direito à informação, proteção à intimidade e desafios para regulação (o caso do Ministério da Saúde)

Ana Claudia Farranha[1]
Rafael Santos de Oliveira[2]
Francieli Puntel Raminelli[3]

Introdução

O direito à informação é um dos princípios fundamentais do Estado Moderno. A construção de sociedades democráticas tem se pautado na perspectiva de que é necessário que o cidadão exerça seu direito de escolha, a partir da perspectiva relacionada ao conhecimento de um determinado processo político. Tal modelo se contrapõe à perspectiva de "escuridão" existente em períodos anteriores à Modernidade e retoma a dicotomia existente entre a esfera pública e a esfera privada. A questão

1 Ana Claudia Farranha (farranha@unb.br) é Doutora em Ciências Sociais pela Unicamp, Professora Adjunta II da Universidade de Brasília (UnB – Faculdade de Direito e Programa de Pós-Graduação em Direito) e Coordenadora da Pesquisa Redes Sociais e Administração Pública (CNPq/UnB)
2 Rafael Santos de Oliveira é Doutor em Direito pela Universidade Federal de Santa Catarina, Professor Adjunto II no Departamento de Direito da Universidade Federal de Santa Maria (UFSM), em regime de dedicação exclusiva e no Programa de Pós-Graduação em Direito da UFSM (Mestrado).
3 Francieli Puntel Raminelli é Graduada em Direito e Mestranda pela Universidade Federal de Santa Maria, no Programa de Pós-Graduação em Direito, com ênfase em Direitos Emergentes da Sociedade Global.

importante levantada aqui é: como essa informação foi sendo processada ao longo da consolidação da experiência democrática?

Assim, no marco da proposta deste livro, esse texto busca mostrar como os regimes de divulgação de informações governamentais podem contribuir para a transparência e fortalecimento de instituições democráticas, mas, ao mesmo tempo, devem manter o direito à privacidade, principalmente, no caso dos dados relativos à saúde dos pacientes.

Nesse contexto, o texto se estrutura apresentando em primeiro lugar uma discussão acerca da importância das estratégias da informação na modernidade e como regimes de divulgação de dados contribuem para mais transparência das ações governamentais. Na sequência, faz-se um paralelo entre a Lei de Acesso à Informação (12.527/2011) e a atuação do Ministério da Saúde, destacando a atuação deste órgão nas redes sociais e na conclusão retomamos o debate sobre o direito à intimidade e a Lei de Acesso à informação.

Espera-se com esse texto contribuir para o aprofundamento de pesquisas na área e, ao mesmo tempo, apontar limites que possam estabelecer um melhor equilíbrio resultante do binômio publicização da informação e direito à intimidade.

Transparência, informação e participação: conceitos e suas aplicações

Retomando o desenho institucional deste Estado, tem-se que nos seus primórdios o valor informação teve um peso pequeno nos processos decisórios, uma vez que votar e ser votado não era um direito universal. A universalização do sufrágio ampliou o escopo da informação, fazendo com que os partidos de massa (DUVERGER, 1957) passassem a divulgar suas ideias ancoradas em programas de governo, as quais deveriam fornecer informações suficientes para convencer os cidadãos de suas escolhas e, ao mesmo tempo, fazer competir visões de mundo e plataformas políticas. Nascia a democracia de massas, constituída a partir do sufrágio universalizado, como também nascia a democracia competitiva, que possibilitava uma luta por votos para a chegada ao governo (MACPHERSON, 1977).

Esse modelo passou a ser questionado e a informação – eixo básico da democracia – ganhava um status mais qualitativo, deixando de ser vista como parâmetro para escolha de governantes e passando a ser compreendida como atributo importante para controle do agente público. Acresce-se a isso, também, o fato da informação proporcionar uma ativação da participação. Historicamente, os questionamentos acerca dos limites da representação política assinalam o surgimento de outros mecanismos de opinião e escolha.[4] Dentre eles, pode-se destacar a ampliação da participação no processo decisório.

Essa é uma visão geral das relações entre democracia e informação. Pensando em termos de Brasil, cuja trajetória democrática recentemente vem se consolidando, o direito à informação se situa junto à perspectiva de ampliação das esferas de decisão e cria elementos para construção de uma cultura de mais transparência e participação.

A institucionalidade brasileira, criada a partir da Constituição de 1988, estabelece alguns princípios fundamentais que consagram o direto à informação. O artigo 5º, incisos XIV e XXIII, prevê o direito de todos terem acesso à informação, como também de solicitar junto à Administração Pública informações de interesse particular ou público – e o artigo 37, estabelece como um dos princípios da Administração Pública a publicidade dos atos governamentais.

Abaixo destes dispositivos constitucionais há uma série de previsões da legislação ordinária e complementar, os quais reforçam a ideia do fornecimento da informação para efeito de maior controle do cidadão sobre os negócios do Estado[5], e, recentemente, foi aprovada a Lei de Acesso à Informação (Lei nº 12.527/2011) que estabelece elementos definidores de uma cultura da informação, entendida como o compromisso do Estado com a transparência, com os procedimentos que geram *accountability,* com o direito ao conhecimento da verdade, com práticas que buscam inibir a corrupção e fortalecer a democracia.

4 Reside nessa perspectiva uma abordagem importante sobre os limites da democracia representativa. Não é objetivo deste texto aprofundar esse debate. Sobre isso, ver Bobbio, 2007.

5 Podem ser mencionadas as seguintes leis: Lei nº 8.159/1991 - Política Nacional de arquivos públicos e privados; Lei nº 9.507/1997 - Rito processual do habeas data; Lei nº 9.784/1999: Lei do Processo Administrativo; Lei Complementar nº 101 - Lei de Responsabilidade Fiscal;.

A Lei de Acesso à Informação estabelece um conjunto de princípios relacionados à máxima divulgação da atuação governamental, obrigação de publicar, promoção de um Governo Aberto e acesso fácil e rápido às informações públicas (CGU, 2014). Com base nesses princípios, a lei define o que entende por transparência ativa – aquela em que a Administração Pública divulga a informação sem precisar ser questionada – e a transparência passiva – aquela que administração pública divulga a informação a partir da provocação do cidadão.

Sob essa perspectiva, tem-se uma progressiva estratégia de incorporação da informação como um valor necessário a uma cultura política de transparência e deve-se destacar o papel que a tecnologia assume na sociedade atual, fortalecendo e ampliando os mecanismos de divulgação que proporcionam maior transparência das ações do Estado. Trata-se da utilização de instrumentos, os quais possibilitam rapidez no acesso e na divulgação da informação – seja ela pública ou privada.

Na literatura, esse movimento é analisado por Lojkne (1995) como um movimento onde as relações sociais de produção, organizadas não somente sobre o espaço fabril, apresentam a perspectiva da informação como elemento que possui valor no âmbito destas relações. Assim, se o processo industrial pautou-se no fornecimento de bens de consumo duráveis, o período seguinte, marcado pela flexibilização da produção, vai pautar-se no conhecimento e na informação como medidas importantes no processo produtivo.

Esse novo modelo ganha forma efetiva, na Administração Pública, nas ideias apresentadas pela corrente intitulada *New Public Management*, que emerge na Inglaterra do final dos anos 1970. A formulação, nesse caso, apela para um conjunto de procedimentos que deveriam orientar a ação do Estado no sentido de responder às demandas de uma sociedade, cujo processo de organização deixa de ser a hierarquia formal – característica do fordismo do pós-guerra – para responder à circulação da informação, à flexibilização das relações de produção e ao redesenho do estatuto dos direitos sociais.

Nesse contexto, a importância de desenvolver mecanismos que possibilitem a dimensão da agilidade, flexibilidade e informação produzida passa a ser o requerimento colocado na agenda pública dos governos. Como fazer isso? Que mecanismos desenvolver? Como é possível fazer com que tais mecanismos fortaleçam a ação do Estado, que, conforme destacado por Castels (1999), amplia suas interações, mas precisa manter sua

posição de autoridade central em um processo que envolve a coordenação de vários agentes envolvidos no fornecimento de serviços públicos?

Assim, a discussão proposta por esse trabalho busca destacar aspectos que conectam o papel da tecnologia com uma cultura da informação, da transparência e da participação. Por essa razão, a análise destaca a forma como o Ministério da Saúde vem utilizando as redes sociais para a implementação da Lei nº 12.527/2011.

Cabe destacar qual o sentido da informação a ser divulgada nesse contexto. O direito à informação está relacionado ao controle da ação pública. Essa perspectiva denota o sentido de um termo importante no debate atual, trata-se do estabelecimento de uma *cultura da informação*.

Essa cultura da informação consiste em instrumentos que apontam uma preocupação com a transparência e com a divulgação da atuação do Estado. A cultura da informação fortalece uma perspectiva de aprofundamento da democracia, pois pode possibilitar que a atuação dos cidadãos não se restrinja apenas ao ato de votar e ser votado. Trata-se de uma perspectiva de fiscalização, conhecimento, acompanhamento e possibilidade de decisão que, essencialmente, não delega ao agente público o poder de escolha, mas faz com que esse tenha de prestar conta dos seus atos.

Do ponto de vista internacional, o Direito à Informação vem construindo uma trajetória no sentido de ser reconhecido como um direito humano fundamental. Inúmeras declarações e documentos internacionais têm discutido essa perspectiva e apontado uma mudança no sentido de incorporar esse direito ao ordenamento jurídico nas Nações. Mendel (2009, p. 3) aponta que

> Nos últimos anos, houve uma verdadeira revolução no direito à informação, que é comumente compreendido como o direito de acesso à informação mantida por órgãos públicos. Enquanto, em 1990, apenas 13 países haviam adotado leis nacionais de direito à informação, hoje mais de 70 dessas leis já foram adotadas em nível global, e estão sendo consideradas ativamente em outros 20 ou 30 países. Em 1990, nenhuma organização intergovernamental reconhecia o direito à informação. Agora, todos os bancos multilaterais de desenvolvi-

> mento e uma série de outras instituições financeiras internacionais adotaram políticas de divulgação da informação. Em 1990, havia uma visão predominante do direito à informação como uma medida de governança administrativa, ao passo que hoje este direito é cada vez mais considerado como um direito fundamental.

Nesse sentido, implementar regimes de direito à informação contribui sob muitos perspectivas para o fortalecimento da democracia, possibilitando transparência e participação e, acima de tudo, criando elementos de uma cultura de acompanhamento das ações do Estado, o que pode viabilizar melhores escolhas e decisões em torno de políticas públicas e mantém acesa a ideia de *cidadania ativa*, presente em Tocqueville (1984), e que aponta uma persistente atuação do cidadão no sentido de limitar os excessos e abusos do poder governamental.

Sob essa perspectiva, vale destacar, a partir da análise de Mendel (2009), os princípios que devem fundamentar uma estrutura de direito à informação. São eles:

a) Princípio da Máxima Divulgação – "a legislação sobre informação deve ser guiada pelo princípio da máxima divulgação".
b) Princípio da Obrigação de Publicar – "os órgãos públicos devem ter a obrigação de publicar as informações essenciais".
c) Princípios da Promoção de um Governo Aberto – "os órgãos públicos precisam promover ativamente a abertura do governo".
d) Princípio da Limitação das Abrangências das Exceções – "as exceções devem ser claras e restritamente definidas e sujeitas a rigorosos testes de 'dano' e 'interesse público'".
e) Princípio dos Procedimentos que facilitem o acesso – "os pedidos de interesse público devem ser processados com rapidez e justiça, com possibilidade de um exame independentemente em caso de recusa".
f) Princípio dos Custos – "as pessoas não devem ser impedidas de fazer pedidos em razão dos altos custos envolvidos".
g) Princípio das Reuniões Abertas – "as reuniões de órgãos públicos devem ser abertas ao público".

h) Princípio da Precedência – "as leis que não estejam de acordo com o princípio da máxima divulgação devem ser revisadas ou revogadas".
i) Princípio da proteção dos denunciantes – "os indivíduos que trazem a público informações sobre atos ilícitos – os denunciantes – precisam ser protegidos" (MANDEL, 2009, p. 39-42).

Esse arcabouço aparece descrito na formulação da Lei nº 12.527/11, denominada Lei de Acesso à Informação, conforme destaca-se a seguir.

Lei 12.527/11: a Lei de Acesso à Informação Brasileira

No contexto de uma Administração Pública mais transparente, bem como em consonância com as previsões constitucionais brasileiras de acesso à informação, em 18 de novembro de 2011 foi publicada a Lei nº 12.527, que versa acerca do acesso a informações governamentais pelo cidadão.

Dividida em seis capítulos e quarenta e sete artigos, a Lei traz, em termos gerais, a quem é direcionada, como se dá o acesso e a divulgação das informações, a forma como requerê-las perante os órgãos e entidades, os documentos sigilosos não passíveis de requerimento e as responsabilidades em caso de negativa de informações ou de tratamento indevido de informações sigilosas ou pessoais (BRASIL, 2011).

Já em seus primeiros artigos define-se que a Lei é aplicada aos órgãos públicos integrantes da administração direta e indireta em todas as esferas federativas[6] (União, Estados, Municípios e Distrito Federal), relativas aos três poderes, Executivo, Judiciário e Legislativo, além das empresas estatais e do Ministério Público. É interessante observar que também se submetem à Lei as entidades que recebem verbas governamentais, não se restringindo o acesso à informação apenas de entidades públicas, mas também as que do governo dependem (BRASIL, 2011).

6 Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do § 3º do artigo 37 e no § 2º do artigo 216 da Constituição Federal. [...] II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios (BRASIL, 2011).

No artigo 3º, a lei destaca importantes diretrizes acerca do acesso à informação no Brasil. Inicialmente, cita-se que a observância da publicidade é preceito geral e o sigilo é a exceção (BRASIL, 2011), sendo que apenas os documentos expressamente elencados como sigilosos são protegidos do acesso público. Além disso, tem-se como inovação o fato de que ao Estado cabe a divulgação de informações de relevante interesse social sem prévio requerimento (BRASIL, 2011), o que se tem entendido como transparência ativa (SANTOS; BERNARDES; ROVER, 2012, p. 47). Esta proatividade do Estado deve garantir as informações mínimas acerca dos temas em questão, sendo que o artigo 8º[7] define o que é essencial. Ainda, está posto na Lei que na realização destas atividades, deverão ser utilizados os meios de comunicação oportunizados pelas novas tecnologias da informação, como é o caso da Internet[8]. Neste ponto em específico insere-se a questão do Governo Eletrônico, importante "ferramenta" utilizada pelo governo brasileiro nos últimos anos.

Ainda como diretrizes do artigo 3º, tem-se o incentivo ao desenvolvimento da cultura de transparência na administração pública, bem como o do seu controle social, uma vez que, sendo transparentes, as ações do Governo poderão ser observadas, questionadas, discutidas e até mesmo confrontadas por quem interessar[9] (qualquer cidadão).

7 O artigo 8º, §1º define como informações mínimas em locais de fácil acesso à população: registros de competências e estrutura organizacional, endereços, telefones e horários de atendimento; registros de repasses ou transferências de recursos financeiros; registros de despesas; informações acerca de procedimentos licitatórios (editais, resultados e contratos); dados para acompanhamento de programas, ações, projetos e obras; respostas a perguntas frequentes da sociedade (BRASIL, 2011).

8 No artigo 8º, §2º determina que todas as informações ditas mínimas devem estar divulgadas nos sítios oficiais da rede mundial de computadores (à exceção de municípios com menos de dez mil habitantes, de acordo com o parágrafo quarto do mesmo artigo), sendo obrigatórios os seguintes pontos, de acordo com o parágrafo terceiro: conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão; possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações; possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina; divulgar em detalhes os formatos utilizados para estruturação da informação; garantir a autenticidade e a integridade das informações disponíveis para acesso; manter atualizadas as informações disponíveis para acesso; indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência (BRASIL, 2011).

9 Dispõe o artigo 10: "Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida" (BRASIL, 2011). Deste artigo depreende-se que também podem requerer informações pessoas jurídicas (SANTOS; BERGER; ROVER, 2012, p. 50-51).

No cumprimento da Lei, devem ser assegurados pelos órgãos e entidades do Poder Público: a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso (BRASIL, 2011).

Quanto à transparência passiva, refere-se às informações que, apesar de não serem espontaneamente apresentadas pelo governo, podem ser requeridas pelo cidadão, mediante identificação do requerente e dispensada a motivação (BRASIL, 2011). A Lei determina que o pedido deve ser possibilitado no portal oficial do órgão ou entidade e, se não for possível a entrega imediata do que é requerido, define o prazo máximo de vinte dias (prorrogáveis por mais dez) para que seja realizada. Se o documento estiver em forma digital, será entregue ao requerente da mesma forma, e se a informação estiver disponível "universalmente", será informado o local onde pode ser obtida. Se o documento estiver impresso e forem necessárias cópias, apesar do serviço de busca e fornecimento da informação ser gratuito, será cobrado o valor relativo à reprodução, salvo se o requerente for pobre nas acepções legais[10] (BRASIL, 2011).

Da atuação do governo brasileiro perante as TICs, em específico no que concerne à LAI, verifica-se que há a perspectiva de busca pela ampliação e aprofundamento da democracia, utilizando-se para isso as redes sociais digitais (*Facebook, Youtube, Instagram, Twitter*)[11]. Essa afirmação pode ser demonstrada nos diversos perfis dos Ministérios e órgãos federais existentes nessas redes. Considerando a problemática já levantada na introdução deste trabalho (informação X intimidade), apresenta-se a seguir os recursos eletrônicos *on-line* utilizados pelo Ministério da Saúde Brasileiro, destacando a forma como o órgão acessa o cidadão, bem como de que forma estes vêm sendo utilizados.

10 Conceito definido pela Lei nº 7.115/83 (BRASIL, 1983).

11 Segundo levantamento em fevereiro de 2013, 18 Ministérios possuíam *fanpages* no *Facebook* (Farranha, 2013). Levantamento mais recente (Cerquinho, 2014) mostra que em outubro de 2013 esse universo era constituído por 38 órgãos entre Presidência e Ministérios. Dentre as redes sociais identificadas, além do Facebook e do Twitter têm-se também o *Flickr, Youtube, Orkut, Formspring, Google+, Slideshare.*

Ministério da Saúde e implementação do acesso à informação: primeiras análises

Diante das importantes modificações que a Lei de Acesso à Informação Brasileira implica ao Governo e ao Estado Brasileiro, e tendo em vista que sua entrada em vigor ocorreu há mais de dois anos, no mês de maio de 2012, realizou-se o acompanhamento de um órgão federal em três de seus ambientes *on-line* para a averiguação das diretrizes impostas pela Lei nº 12.527/11, pelo comportamento da Administração e sua compatibilidade com as características de governo aberto e da interação e adesão dos cidadãos a estas novas ferramentas.

O objeto desta averiguação foi o Ministério da Saúde, órgão federal diretamente ligado à Presidência da República e responsável por um tema de grande interesse social, quase sempre presente entre as demandas da população: a saúde. Por este motivo, o *Blog*, a página no *Facebook* e o Portal Oficial deste Ministério foram visitados e as informações constantes nestes ambientes foram analisadas.

O primeiro item a ser avaliado foi a Página do Ministério da Saúde no *Facebook*, hospedado na rede social *on-line* de maior adesão no Brasil atualmente (CONSCORE, 2014). A página do Ministério da Saúde foi criada no dia 1º de janeiro de 2008. De acordo com o item "sobre", presente em todas as páginas do *site*, a missão da utilização desta ferramenta é a "Qualificação do SUS por meio do diálogo com a população" (BRASIL, 2014b). Com este objetivo, observa-se que o canal foi criado com o intuito de atender à demanda social de maior participação popular, além de abrir possibilidades para que o internauta que escolhe esta via de comunicação possa contribuir com melhorias para o Ministério. Não há maiores especificações acerca desta missão, mas dela se depreende que o objetivo inicial é a abertura da administração ao cidadão.

No mesmo item "Sobre" está disponível a descrição da página, na qual consta: "Página oficial de relacionamento com os usuários, atendimento à população e divulgação de campanhas, agendas, programas e ações do Ministério da Saúde". Com isto, pode-se inferir que a Página do Ministério da Saúde no *Facebook* intenta fornecer ao menos alguns pon-

tos básicos previstos no art. 8º da Lei nº 12.527/11, como previsto em seu parágrafo primeiro (especificamente no inciso V), em que os órgãos públicos são obrigados a informar ao cidadão, de forma ativa e pelos meios mais eficazes, as principais atividades realizadas.

A primeira imagem da página é seu "cabeçalho", que se manteve em um padrão ao longo do período analisado. Como "foto de capa" sempre eram escolhidas algumas campanhas promovidas pelo órgão, sendo modificadas a cada 10 (dez) ou 15 (quinze) dias. Além disso, ficam visíveis as fotos postadas pelo órgão, o número de curtidas (ou de fãs) e o número de "pessoas falando sobre isso" e opções de campanhas específicas em aplicativos, que podem ser escolhidos pelo usuário e nos quais, dentro da página do Ministério, serão abertos ambientes com cartazes e informações específicas do tema.

Abaixo do topo fixo da página *on-line* estão os *posts* criados pela equipe gestora da página, do mais recente ao mais antigo, que pode ser visualizado ao rolar o cursor para baixo. De forma geral, os *posts* cumprem os objetivos descritos no item "Sobre", pois versam acerca de campanhas, informações à população no pertinente à saúde e a doenças e divulgação de programas e ações do Ministério.

O segundo ambiente digital do Ministério da Saúde observado foi o "*Blog* da Saúde". Referida página distingue-se da Página do *Facebook* por não ser passível de receber curtidas e por não chegar diretamente ao cidadão, pois é necessário ingressar em seu endereço para acessar as informações disponibilizadas. O *blog* oferece a opção de envio de *feeds* de notícia no *e-mail* do internauta interessado e possibilita que sejam realizados comentários, além de ser possível, por meio do link da postagem, o compartilhamento do texto em outras redes (é possível enviar o *post*, por exemplo, no *Facebook,* no *Twitter,* etc.). O próprio *blog* possui a opção de compartilhamento na rede, na qual há a oferta material das campanhas para que o usuário também contribua na propagação das informações.

Abaixo destes ícones e do mecanismo de busca no Blog (obrigatório pelo art. 8º, §3º, I da Lei 12.527/11), encontram-se abas temáticas, em que, além dos destaques (normalmente as notícias mais recentes), estão a agenda do Ministério e do Ministro da Saúde, os programas e campanhas, o espaço para o profissional da saúde, o campo "saúde em dia", o cam-

po específico para o programa "Mais Médicos"e o espaço "SUS e você" (BRASIL, 2014a). O primeiro dos ambientes publica todas as postagens do *blog*, sendo os demais específicos do título que possuem. Desta forma, os interessados nestes assuntos podem acessar diretamente os conteúdos que desejam, sendo desnecessária uma busca entre todas as postagens.

O terceiro ambiente utilizado pelo Ministério da Saúde a ser analisado é o Portal da Saúde, que constitui o sítio oficial do órgão. Por ser um *site*, o ambiente deve obrigatoriamente seguir a Lei de Acesso à Informação, principalmente os expressos nos incisos do artigo oitavo.

O portal da saúde segue o *layout* de grande parte dos sítios oficiais (BRASIL, 2014c). Em seu topo, no canto direito, detém os ícones "Acesso à informação" e "Brasil", sendo que ambos remetem ao já referido "Portal Brasil", *site* administrado pela administração federal. Logo abaixo, está o nome "Portal da Saúde - SUS", que vem acompanhado de uma foto. Ao lado, está um campo para pesquisa no *site*, acompanhado do "Mapa do Site", "Fale conosco" e "Links de interesse" e, abaixo disto, os *links* para acesso aos demais espaços do Ministério da Saúde na *Internet* (exatamente como está disponibilizado no *blog*).

O *menu* principal do *site* é composto por seis itens: "Cidadão", "Profissional e Gestor", "O ministério", "Serviços", "Biblioteca" e "Acesso à informação". Cada uma das opções oferece diferentes itens de acordo com o interesse do internauta. Como no *blog*, cada um dos títulos traz as publicações de acordo com seu título, sendo que a página principal é a que aborda todos os tópicos, além de ser a única que oferece modificações constantes, em seu lado esquerdo da tela, local onde ficam as notícias do Ministério. As notícias, os vídeos e as imagens são os únicos elementos que se modificam com maior frequência em todo o site, visto que os outros itens do *menu* permanecem inalterados a maior parte do tempo.

No *site* destaca-se a grande quantidade de assuntos e conteúdos disponibilizados, em que além de alguns "serviços" prestados pelo Ministério, também estão estampadas as campanhas, informações de cada estado do país e o ícone "Transparência". Neste item, estão disponíveis o "Acesso à Informação", que direciona a um espaço do *site* em que está disponível a Lei nº 12.527/11, as principais dúvidas e respostas sobre ela, e um menu com algumas possibilidades de acesso.

Cada um dos itens do *menu* apresenta informações de extrema relevância ao cidadão que deseja manter-se atualizado sobre as iniciativas do Ministério, respeitando inúmeros pontos da Lei de Acesso à Informação. É o caso de todos os itens elencados, que estão previstos no art. 8º da Lei nº 12.527/11.

Além disto, nesta parte do *site* está o *link* para o portal da "Transparência da Saúde", na qual todos os orçamentos do Ministério da Saúde estão separados por Estado-membro do país. Ao escolher um deles, as informações (BRASIL, 2014c) apresentadas dizem respeito aos valores investidos em "Atenção Básica", "Média e Alta Complexidade", "Assistência Farmacêutica", "Gestão do SUS", "Vigilância em Saúde", "Investimentos" e "Diversos". Ainda, estão expostos os Convênios vigentes, os relatórios de gestão e Estaduais, unidades de saúde, agentes comunitários, equipes de saúde bucal e farmácias conveniadas ao "Programa Farmácia Popular" e as legislações pertinentes aos repasses financeiros e afins[12].

Apresentados os três ambientes *on-line*, reitera-se que por serem plataformas diferentes, cada um deles possui pontos positivos e negativos. Por exemplo, cita-se a restrita participação popular proporcionada pelo Portal Oficial, que é maior no *blog*, pela possibilidade de serem realizados comentários a cada postagem, e na página do *Facebook*, em que a informação chega ao cidadão em suas próprias páginas, ou seja, as movimentações na página da rede social *on-line* são visualizadas por todos que a curtiram/seguem em sua própria página inicial. Outras diferenças entre os três objetos analisados podem ser visualizados, como, por exemplo, as grandes modificações que ocorrem em um *blog* e na página do *Facebook* em um dia em comparação com aquelas realizadas em portais/*sites*. De forma geral, se observa que há maiores participação e facilidade naqueles espaços em que o internauta pode interagir sem passar por filtros ou ter que buscar a informação. Assim, se o Portal e o *Blog* da Saúde necessitam ser acessados em seus endereços *on-line*, a página do *Facebook* sequer isto requer, visto que é o Ministério que acessa o cidadão.

Sobre os temas publicados, todas as campanhas relatadas na página do *Facebook* do Ministério da Saúde também são veiculadas no *blog* e no *site* oficiais. De fato, a iniciativa de conscientização e difusão da informação dos Programas Governamentais não mudam na comparação entre os

12 Estes dados dizem respeito especificamente aos resultados da consulta no Estado do Rio Grande do Sul.

três ambientes *on-line*; no entanto, a forma como eles são abordados varia, como se observa, por exemplo, quando se analisa o *blog* e suas postagens.

Uma importante diferença, por exemplo, é a total ausência de participação popular/internauta nos conteúdos postados no *blog*. Apesar de trazerem mais informações, durante todo o período analisado o número de comentários foi zero. Por ser um ambiente que proporciona esta interatividade, ainda que em menor grau que a rede social *on-line* do *Facebook*, é com surpresa que se concluiu não interação no *Blog da Saúde*.

Ao analisar as poucas modificações ocorridas no Portal da Saúde, observou-se que as notícias presentes no *site* estavam em consonância com as Campanhas realizadas, mas permaneciam por dias inalteradas, modificando-se muito pouco e sem muita frequência. Sendo esta a característica de *sites*, no sentido de manterem-se mais fechados e sem muitas modificações por causa da maior dificuldade e controle no repasse de informações, e, aliado a este fato, a natureza mais parecida com um grande banco de dados para acesso da população ao que lhe convém, observa-se que o Portal da Saúde possui um objetivo muito maior de fornecimento passivo de informações do que de interação com o cidadão. Isto porque facilita o requerimento de informações dos interessados ao invés de expô-lo, que seria um posicionamento mais ativo na construção da transparência.

Considerações finais: notas sobre intimidade e direito à informação

Na experiência do Ministério da Saúde observa-se um esforço em publicizar dados e oferecer canais aos cidadãos, os quais possibilitem conhecer o que o Estado faz no tema saúde. Assim, cumprem-se, em parte, alguns dos requisitos legais quanto ao acesso à informação e a importância dele enquanto um pilar na tomada de decisão. Entretanto, por outro lado, não há muita interatividade cidadãos/internautas e Ministério. Os canais apresentados mostram que se tratam mais da realização da transparência passiva do que efetivamente de uma prática que ouça o cidadão, recolha informações e trate essa informação de maneira a criar, além da cultura da informação, uma atitude de cidadania ativa.

Nesse aspecto, um questionamento que pode vir desta discussão é se a prática da divulgação da informação aponta para a divulgação de dados pessoais, que estão consolidados em banco que contém prontuários de usuários dos sistemas de saúde (SUS). Em que medida interesse público se coloca acima do direito à intimidade?

Na análise apresentada verifica-se que os canais das mídias sociais apresentados nesse texto não parecem se propor à divulgação de informação pessoal. Verifica-se que trata-se de informações que pretendem dar publicidade à ação do Ministério. De toda forma, é preciso destacar quais os desafios na continuidade da implementação da Lei nº 12.527/11. Sob essa perspectiva, a literatura recente sobre o tema demonstra que "a violação à intimidade deve ser analisada ante o princípio da publicidade" (...). Em outras palavras, "a questão consiste em saber se o princípio da publicidade, mesmo com a armadura do interesse público, poderia ocasionar a visualização irrestrita de dados pertencentes à esfera íntima de um indivíduo" (NASCIMENTO & RODRIGUES, 2013, p. 170). Nesse caso, o movimento de publicização das ações do Estado, identificado no início deste texto, demonstra que as mudanças em torno da construção de uma esfera mais coletiva, correlaciona a tutela à intimidade à defesa do interesse público, havendo exclusões que colocam exceções, mas não podem (nem devem) obstaculizar a defesa de um regime de acesso à informação, constituído como articulador de mais transparência, participação e democracia.

Entretanto, ainda que o acesso à informação esteja alicerçado sobre a noção de interesse público, não se pode ignorar a necessidade de algum grau de regulamentação sobre dados pessoais. Nesse sentido, recentemente (janeiro/2015), o Ministério da Justiça lançou debate público com vistas a ampliar a discussão sobre o tema.

Para finalizar, vale destacar que a Lei de Acesso à Informação já menciona, em seu artigo 31, aspectos que enfrentam essa discussão. Apontando que no que concerne ao objeto da lei, a informação deve ser tratada com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como no que tange às liberdades e garantias individuais. Destaca que as informações relativas à intimidade, vida privada, honra e imagem têm acesso restrito aos agentes públicos e às pessoas que a ela se referirem. Destaca que poderão ter sua divulgação autorizada, mediante previsão legal ou con-

sentimento expresso da pessoa a quem se referir. No tema consentimento a Lei estabelece que este não será exigido nas seguintes hipóteses:

a) Prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
b) Realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
c) Ao cumprimento de ordem judicial;
d) À defesa de direitos humanos; ou
e) À proteção do interesse público e geral preponderante (art. 31, II, parágrafo 3º).

Diante destas considerações, parece que o próximo período no que concerne ao tema abordado neste artigo requer duas direções: a) ampliação do acesso à informação pública, de forma a contribuir para processos mais transparentes e democráticos no tema da saúde; e b) regulamentação do trato das informações pessoais de forma a ponderar os princípios relativos ao acesso à informação e à proteção da intimidade.

Referências

BOBBIO, Norberto; NOGUEIRA, Marco Aurélio. **O futuro da democracia**: uma defesa das regras do jogo. Rio de Janeiro: Paz e Terra, 1997.

BRASIL. Blog da Saúde. Disponível em: <http://www.blog.saude.gov.br/>. Acesso em: 1 abr. 2014a.

BRASIL. Controladoria Geral da União. **Manual da Lei de Acesso à Informação para Estados e Municípios.** Brasília, D.F., 2013. Disponível em: <http://www.cgu.gov.br/publicacoes/BrasilTransparente/Manual_LAI_EstadosMunicipios.pdf>. Acesso em: 15 jun. 2014.

BRASIL. Lei nº 7.115, de 29 de agosto de 1983. Dispõe sobre prova documental nos casos que indica, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L7115.htm>. Acesso em: 5 nov. 2014.

BRASIL. Lei 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 nov. 2014.

BRASIL. Ministério da Saúde. Página do Ministério da Saúde no Facebook. Disponível em: <https://www.facebook.com/minsaude/info>. Acesso em: 20 jun. 2014b.

BRASIL. Ministério da Saúde. **Portal da Saúde.** Disponível em: <http://portalsaude.saude.gov.br/>. Acesso em: 1 abr. 2014c.

CASTELLS, Manuel. **Um Estado destituído de poder? O Poder da Identidade**. São Paulo: Paz e Terra, 1999.

CONSCORE. Brazil digital future. 22 de maio de 2014. Disponível em: <http://pt.slideshare.net/jacquelinee/2014-brazil-digitalfutureinfocuspt>. Acesso em: 11 jun. 2014. p. 28.

BRASIL. Controladoria Geral da União. **Rumo a uma cultura de acesso à informação**: Lei 12.527/2012. Brasília, D.F., 2014. [Curso Nacional de Qualificação de Auditorias e Ouvidorias do SUS]

DUVERGER, M. **Los partidos políticos**. México, D.F., Fondo de Cultura Economica, 1957.

LOJKINE, J. **A revolução informacional**. São Paulo: Cortez, 1995.

MACPHERSON, Crawford Brough. **A democracia liberal**: origens e evolução. Rio de Janeiro: Zahar, 1977

MENDEL, T. **Liberdade de informação**: um estudo de direito comparado. 2.ed. Brasília, D.F.: UNESCO, 2009.

NASCIMENTO, V. R. do; RODRIGUES, M. S. A sociedade informacional em xeque: Princípio da publicidade versus direito à intimidade e a Lei nº 12.527/11. In: OLIVEIRA, R.; BUDÓ, M. **Mídias e direitos da Sociedade em Rede**. Ijui, RS:Unijuí, 2013. p. 159-180.

SANTOS, P. M.; BERNARDES, M. B.; ROVER, A. J. **Teoria e prática de governo aberto:** lei de acesso à informação nos executivos municipais da Região Sul. Florianópolis: Funjab, 2012.

17

Movimentos sociais em redes sociais virtuais: possibilidades de organização de ações coletivas no ciberespaço[1]

Wellington Tavares[2]
Ana Paula Paes de Paula[3]

Introdução

A tradição das relações sociais parece estar perdendo sua força continuamente nos últimos tempos. As estruturas socialmente construídas com base em relações de subordinação e dominação por vezes são defendidas como necessárias para permitir maior coesão social, sendo assumidas como fruto da hereditariedade e levando os indivíduos a aceitá-la. A defesa dessa continuidade é realizada tanto por representantes do poder público, em razão do tipo de política e seus regimes políticos adotados, quanto por meio de grupos sociais hegemônicos que se colocam em posições de elite.

Visto tal contexto e a crescente desaprovação das estruturas sociais vigentes, vários tipos de ações coletivas têm levado os indivíduos a ma-

1 Texto originalmente publicado em: TAVARES, W.; PAULA, A. P. P. Movimentos sociais em redes sociais virtuais: Possibilidades de Organização de Ações Coletivas no Ciberespaço. *Revista Interdisciplinar de Gestão Social*, v.4, n.1, p.209-230, jan./mar. 2015.

2 Wellington Tavares (emaildotom12@yahoo.com.br) é graduado em Administração, Doutor em Administração pela Universidade Federal de Minas Gerais (UFMG) e Professor Adjunto na Universidade Federal de Ouro Preto (UFOP).

3 Ana Paula Paes de Paula é Bacharel em Administração de Empresas pela Universidade de São Paulo, Pós-Doutora em Administração pela Fundação Getúlio Vargas - SP e Professora Titular e pesquisadora da Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais.

nifestarem suas demandas sociais e insatisfações diversas por meio de movimentos sociais. Tais movimentos muitas vezes se estabelecem por meio de redes de mobilização que englobam demandas e objetivos semelhantes e compartilhados entre os manifestantes e favorecem a atuação em favor de causas coletivas. As bases deste tipo de ação são bem fundamentadas na história por meio de órgãos de classes - tais como sindicatos -, bem como por meio de revoltas populares e movimentos sociais diversos. Contudo, o que chama a atenção nos tempos atuais é a utilização de diferentes formas de ações coletivas e a utilização de novos espaços e recursos que possibilitam aos indivíduos se (re)conhecerem em grupos, se organizarem e agirem coletivamente.

No entendimento de Scherer-Warren (2005), os movimentos sociais apresentam uma diferente configuração na sociedade da informação, marcadamente alterada em decorrência do desenvolvimento das tecnologias da informação e comunicação. Nesta direção importa considerar três dimensões para a análise de tais movimentos: temporalidade, diante da possibilidade de análises de tempos sociais distintos; espacialidade, diante do surgimento de novos espaços ou territórios - virtuais e reais -, bem como suas interações; e sociabilidade, diante de novas formas de relações sociais em termos de intensidade, alcance, intenções e conectividade com dimensões da esfera pública.

Já as redes sociais resultam de um tipo de conjugação de três elementos: ações orientadas a determinados fins, acaso e heranças de padrões de vínculos anteriores. Tal visão parece apontar para dimensões distintas das redes, sendo estas pautadas por organização, processos políticos e contexto histórico-cultural (MARQUES, 2007). A análise que se pretende realizar neste artigo está voltada para as redes sociais virtuais, em especial por estas propiciarem o desenvolvimento de ações coletivas dos movimentos sociais. Alguns destes movimentos têm desenvolvido capacidades de articulação em redes virtuais, objetivando o aumento do compartilhamento de conhecimentos e experiências, bem como o aumento da amplitude da mobilização, da influência e da interlocução em relação às amplitudes de poder (AGUIAR, 2007b).

A partir daí, e em virtude das recentes inovações nos processos comunicacionais e organizacionais, bem como dos desafios e das pos-

sibilidades inerentes a tais, várias questões surgem como forma de permitir melhores análises e entendimentos sobre estes fenômenos sociais, especialmente em relação às possibilidades de ação para os indivíduos ao possibilitar maior aproximação, integração e cooperação virtuais; ao estabelecimento de organização e coesão entre os grupos e seus movimentos; aos impactos das redes virtuais na cultura e democracia.

Neste sentido, este ensaio teórico se propõe a responder à seguinte argumentação: Quais possibilidades de relações e organizações de ações coletivas e ativistas de movimentos sociais surgem a partir das redes sociais virtuais? A principal proposição levantada aqui é a de que as redes sociais virtuais se constituem como importantes espaços que permitem ampliar as potencialidades dos indivíduos se agruparem e agirem coletivamente diante de transformações ocorridas na tecnologia, cultura e sociedade. Desta forma, para se compreender esta dinâmica social, sua organização e seus processos, o objetivo geral deste estudo é analisar o surgimento, as possibilidades e a dinâmica de ações coletivas e ativistas de movimentos sociais estabelecidas em redes sociais virtuais, bem como refletir sobre a utilização destas redes como espaço para formação e organização de grupos e ações coletivas.

Como forma de melhor esclarecer o objetivo geral deste estudo, foram elaborados os seguintes objetivos específicos: a) identificar e analisar as transformações tecnológicas e sociais que possibilitaram as alterações nas formas de comunicação e organização de grupos e ações coletivas no ciberespaço; b) discutir o surgimento, desenvolvimento e influência das redes sociais virtuais na formação/fortalecimento de grupos sociais; c) analisar a evolução das discussões sobre movimentos sociais, bem como suas relações com as redes sociais; e d) discutir as possibilidades de organização de movimentos sociais nas redes sociais virtuais, as ações coletivas e ativistas.

Para o alcance dos objetivos definidos acima, este ensaio teórico apresenta discussões acerca de movimentos sociais e redes sociais virtuais, organizadas conforme segue. A partir desta primeira seção introdutória, na segunda seção realiza-se uma explanação sobre o desenvolvimento tecnológico que propiciou o aparecimento e fortalecimento de recursos informacionais e comunicacionais, em especial os *softwares* sociais. Na terceira seção são apresentados conceitos sobre as redes sociais e, em especial, sobre tais redes que se desenvolvem no ambiente virtual propiciado pela internet:

as redes sociais virtuais. Já na quarta seção são apresentadas algumas definições sobre movimentos sociais e sobre as relações destes com as redes sociais que possibilitam seu desenvolvimento na sociedade. Na quinta seção são apresentadas discussões acerca da organização de movimentos sociais nas redes sociais virtuais, que é o objetivo central deste ensaio. Por fim, na sexta seção são apresentadas as principais considerações deste ensaio.

Desenvolvimento tecnológico e softwares sociais

O desenvolvimento dos sistemas eletrônicos é um dos principais responsáveis pelas grandes transformações que a economia e a sociedade têm passado. Na economia, o impacto das tecnologias nos processos e na interação entre organizações demonstra o grande impacto sobre o capitalismo, transformado em função da era da informação. Já na sociedade há mudanças em termos das novas formas de comunicação, da redução das distâncias, dos novos modos de se relacionar e da própria mudança cultural, denominada como "cultura internet" (CASTELLS, 1999).

A partir de uma comparação da era industrial e com a era da informação, torna-se perceptível que nesta última há semelhante preocupação com as economias de escala da primeira, porém menos preocupações com o espaço e o tempo. Nota-se o surgimento de uma nova dinâmica de vida e de relações, a qual "exigirá cada vez menos que você esteja num determinado lugar em determinada hora, e a transmissão do próprio lugar vai começar a se tornar realidade" (NEGROPONTE, 1995, p. 159). De forma saudosista, Baudrillard (1997) chama a atenção para as mudanças que o desenvolvimento da tecnologia trouxe para o cotidiano das pessoas e também para as consequências da virtualidade para a identidade dos indivíduos, visto que esta "implica a possibilidade da dissimulação, do desaparecimento no espaço impalpável do virtual, e de assim não ser mais localizável, inclusive por si mesmo" (BAUDRILLARD, 1997, p. 149).

Por outro lado, e de forma mais receptiva e positiva em relação ao desenvolvimento tecnológico, Rheingold (1996) discute a importância da Comunicação Mediada por Computador (CMC) para a democratização da informação e aumento da liberdade de expressão. Ainda neste sentido,

Castells (1999) argumenta que a busca de identificação e sociabilidade expuseram o surgimento de uma nova cultura ocasionada pela expansão dos ciberespaços que eclodiram a partir do desenvolvimento das TICs (Tecnologias da Informação e Comunicação) e da CMC, e que dão base para as formas atuais de relações, trabalho e comunicação das pessoas.

No início da década de 1970, Alan Kay criou o *Research Learning Groupe* no laboratório PARC, da Xerox, que objetivava integrar usuários, tendo levado os demais pesquisadores deste laboratório a se encorajarem para criar o ALTO, um computador pessoal e experimental que funcionava em redes locais (LAN, Ethernet). Esta invenção possibilitou a continuidade do desenvolvimento de máquinas que viriam a constituir os primeiros microcomputadores (LEMOS, 2004). Já as redes sociais na internet se originaram das denominadas comunidades de interesse temático a partir dos BBSes e *newsgroups* da Usenet, criados em 1979 na *Duke University* nos EUA e que permitia o compartilhamento e organização temática de mensagens por várias instituições no mundo. Os BBSes foram sistemas de comunicação muito utilizados nas décadas de 1970 a 1990, nos quais havia troca de mensagens por conexões discadas. Os *newsgroups* eram grupos de discussão que antecederam os grupos de interação por e-mails e redes fechadas que prevalecem nos dias atuais. Ambos os grupos permitiam a interação entre desconhecidos que passavam a se relacionar em virtude de interesses comuns. Já as redes sociais da atualidade, em grande parte, favorecem contatos virtuais de indivíduos que já se conhecem nos espaços reais e que tornam, preferencial ou exclusivamente, a plataforma virtual em espaço de interação e trocas (AGUIAR, 2007a).

Cerca de três décadas depois, em meados de 2002, surgiram novas redes sociais virtuais que atualmente fazem parte do que se denomina de nova geração das redes de relacionamento. A primeira rede baseada em "círculo de amigos" foi o *Friendster* desenvolvido pelo cientista da computação britânico Jonathan Bishop. Nesta rede, os usuários criavam seus perfis públicos e passavam a associar-se a demais perfis, tais como os de amigos, amigos de amigos, entre outros. Após alcançar uma enorme quantidade de usuários em pouco menos de um ano, cerca de 3,3 milhões, outras redes sociais virtuais foram surgindo, tais como os mais conhecidos *MySpace*, *Orkut* e *Facebook*. Após esta propagação de *sites* de

relacionamentos sociais uma série de outros novos tem surgido na atualidade buscando mercados relacionados a grupos específicos, tais como adolescentes, pessoas interessadas por músicas, etc. (AGUIAR, 2007a).

Atualmente nota-se uma expansão do número e variedade dos tipos de *softwares* sociais oferecendo recursos diversos, mas com focos semelhantes e normalmente voltados para a agregação de pessoas do círculo de relacionamentos e na construção de elos. Contudo, há que se esclarecer que o *software* social não é propriamente uma comunidade virtual, mas contém várias delas ao se constituir como o espaço no qual estas se estabelecem. Machado e Tijiboy (2005) enumeram alguns destes *softwares* que dão ou deram nome às redes sociais virtuais que formam, entre os quais pode-se destacar o *Orkut*, *Wallop Tribe*, *Hi5*, *Friendster* e *Dogster*.

Em um breve histórico sobre o desenvolvimento e popularização dos *softwares* sociais podem-se enumerar alguns principais em uma linha histórica, de acordo com Boyd e Ellison (2007). O precursor é o *SixDegrees.com*, lançado no ano de 1997. Após isto, até meados de 2001, uma série de sites surgiu com diferentes possibilidades para formar as redes sociais, conforme anos de surgimento e nomes a seguir: 1999 – *LiveJournal*, *AsianAvenue*, *BlackPlanet*; 2000 – *MiGente*; 2001- *Cyworld* e *Ryze*; 2002 – *Fotolog* e *Friendster*; 2003 – *LinkedIn*, *MySpace*, *Tribe.net*, *Last.FM* e *Hi5*; 2004 – *Orkut*, *Flickr* e *Piczo*; 2005 – *Yahoo! 360* e *YouTube*; e 2006 – *Windows Live Spaces*, *Twitter* e *Facebook*. Apesar de o *Facebook* ter se popularizado a partir de 2006, ele já podia ser utilizado em 2004 apenas por um grupo restrito em Harvard, além de uma versão para redes corporativas lançada no início de 2006. Atualmente, outra rede que tem crescido em popularidade e membros é a *Google+*, lançada pela *Google* em meados de junho de 2011 para fazer frente ao crescimento do *Facebook* e, em especial, diante da queda no número de usuários do *Orkut*, sua outra rede social. Mais recentemente, outra rede social entrou neste cenário no final de 2012, a *Socl*, desenvolvida pela *Microsoft*.

O termo *software* social foi (re)afirmado por Clay Shirky em 2002 buscando abranger uma vasta possibilidade de utilizações, definindo-o como "*all uses of software that supported interacting groups, even if the interaction was offline*", por meio da *Web* 2.0. O termo *software* social por vezes é substituído por outros com os quais mantém semelhanças concei-

tuais, tais como: *groupware*; *computer-mediated communication* (CMC); *social computing*; e *sociable media* (BOYD, 2007a, p. 15).

Na definição de Boyd e Ellison, sites de redes sociais (*social network sites - SNS*) são classificados, em geral, como

> web-based services that allow individuals to (1)construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (BOYD e ELLISON, 2007, p. 211).

A visibilidade dos perfis dos usuários varia de acordo com *software* social utilizado e com a descrição do usuário. Normalmente os *sites* oferecem diversas opções para que o usuário configure seu perfil e escolha o que se torna público para todos os usuários ou privado para os grupos de "amigos" que desejar selecionar para visualizar, desde informações gerais a fotografias, postagens, etc. (BOYD e ELLISON, 2007). Além destes recursos, Cogo e Brignol (2011) ressaltam a importância do hipertexto (formado por texto, som e imagem) na construção de mensagens e conteúdos a partir de fluxos heterogêneos, possibilitando a hibridização de diferentes formas discursivas na CMC. Este fato apontou novas possibilidades para a reestruturação dos processos comunicacionais a partir da lógica de redes.

As repercussões dos sites de redes sociais são um fenômeno global, em especial na expansão de comunidades (BOYD e ELLISON, 2007). Boyd (2007b) discute as questões relacionadas à identidade e participação na rede *Friendster*, defendendo que as relações sociais na rede virtual não equivalem às relações fora dela. Harrison e Tomas (2009) recorrem a um estudo para expor a influência de uma rede social virtual, a *Livemocha*, na aprendizagem de idiomas. Szell e Thurner (2010) apresentam um estudo com uma rede virtual estabelecida por meio de jogadores de *games* procurando mensurar a dinâmica das relações e aspectos estruturais da rede, tal como a densidade. Gosling *et al.* (2011) apresentam estudos comparativos do comportamento relatado e dos dados descritos em perfis de usuários no *Facebook*. Takhteyev, Gruzd e Wellman (2012) compa-

ram a formação de laços sociais no *Twitter* com a proximidade geográfica, linguagem, fronteiras nacionais e outros elementos.

Há também alguns estudos realizados e publicados no Brasil que realizaram análises em redes sociais virtuais, a exemplo do trabalho de Recuero (2004b) ao analisar aspectos da Teoria de Redes no *Orkut*, em *weblogs* e *fotologs*. Em outro estudo, Recuero (2006) faz relações do capital social e de sua relação com a dinâmica sociais observadas no *Orkut*. Já Santos Júnior e Mantovani (2010) procuraram compreender alguns aspectos da comunicação estabelecida em comunidades do *Orkut*. No Brasil nota-se uma preponderância de estudos com foco nesta rede social, visto que até meados de 2010 possivelmente era o *software* social mais utilizado no país, tendo perdido espaço para outros, tais como *Twitter* e *Facebook*.

A partir do aprofundamento dos aspectos tecnológicos e do histórico de desenvolvimento dos *softwares* sociais, na próxima seção é apresentado o contexto virtual das redes sociais nas quais os integrantes de movimentos sociais encontram ferramentas e condições de realizar ações coletivas, organização dos grupos e, especialmente, desenvolver a consciência política a partir do dinâmico contexto ideológico e cultural formado.

Redes sociais virtuais

As redes sociais são quaisquer relações entre pessoas, mediadas ou não por sistemas informatizados. Tais relações podem ser efetivadas por interações que intentam mudanças na vida das pessoas, para o coletivo ou ainda para organizações, visto que tais interações podem ser estabelecidas em razão de interesses particulares, em defesa de outros ou em nome de organizações. Além destas motivações, as redes podem ser estabelecidas em função de movimentos sociais com finalidades sociopolíticas (AGUIAR, 2007a).

Entre as variações ou especificidades de redes sociais estão as denominadas 'redes sociais na internet' ou 'redes sociais virtuais', que se referem aos formatos de sociabilidade e de relações sociais virtuais,

que se diferenciam das relações reais em termos de objetivos e dinâmica. A exemplo das ações sociopolíticas, muitas relações estabelecidas no 'mundo real' passam a utilizar a internet como um ambiente adicional de interação, figurando como um espaço público complementar (AGUIAR, 2007a). Há uma necessidade dos indivíduos em se integrarem a grupos sociais específicos que tenham interesses comuns, o que expõe a intenção de se reconhecerem quando buscam conectar-se às redes com as quais se identifiquem. Além disso, este espaço de interação social, em especial os virtuais, possibilita a comunicação entre os usuários e favorece a desnacionalização e desestatização da informação, a partir da conectividade mundial estabelecida pela internet (CASTELLS, 1999).

Assim, pode-se compreender a existência das redes sociais a partir de análises sobre o prisma das relações sociais e das trocas efetuadas entre os membros dos agrupamentos sociais e não meramente em termos da territorialidade. Para Wellman e Berkowitz (1988), as redes sociais na internet são mais que a simples definição e denominação de elementos que permitem criar uma metáfora para compreender um agrupamento, elas são baseadas em relações que sustentam uma estrutura em rede. Por exemplo, os *nós* não são apenas indivíduos, mas podem representar agrupamentos, os laços entre os membros não são apenas uma representação de um elemento da estrutura da rede, mas representam as relações entre os membros por onde as trocas fluem.

Neste sentido, e diante das possibilidades configuradas por um novo conceito de tempo-espaço, as pessoas têm passado a se estabelecer em redes no ciberespaço. Este fato é reforçado em Rheingold (1996), visto que as redes virtuais foram possíveis a partir da redução das possibilidades de encontros reais entre as pessoas, possibilitando se criar laços emotivos por meio da internet e discussões virtuais duradouras.

Para Lévy (2000, p. 127), uma rede virtual "é construída sobre as afinidades de interesses, de conhecimentos, sobre projetos mútuos, em um processo de cooperação ou de troca, tudo isso independentemente das proximidades geográficas e das filiações institucionais". Elas "constituem o fundamento social do ciberespaço e a chave da ciberdemocracia" (LÉVY, 2002, p. 67). Já no entendimento de Rheingold (1996, p. 18) redes virtuais são conceituadas como "agregados sociais surgidos na Rede,

quando os intervenientes de um debate o levam por diante em número e sentimento suficientes para formarem teias de relações pessoais no ciberespaço". Já ciberespaço, considerando o avanço no desenvolvimento da Comunicação Mediada por Computador (CMC), pode ser compreendido como "espaço conceptual onde se manifestam palavras, relações humanas, dados, riqueza e poder dos utilizadores da tecnologia de CMC".

No entendimento de Recuero (2004a), o fluxo de informações interfere no formato do ciberespaço, visto que a cada nova postagem, comentário ou disseminação de links, a internet e as redes são alteradas, dando origem a novas relações e modificando os *nós* da rede. São ações como estas ocorridas entre os indivíduos que permitem que, assim como na "realidade real", as redes virtuais sejam dinâmicas e alterem suas configurações. Apesar de por um lado parecerem ameaçar a sociabilidade, as redes sociais virtuais se mostram úteis sob o ponto de vista do dinamismo e vitalidade social, e por permitirem um espaço que potencializa as conexões entre os indivíduos (PRIMO, 1997).

Nas relações estabelecidas nas redes os indivíduos têm a possibilidade de escolher o outro com quem deseja se relacionar, diferentemente das relações estabelecidas com a família e comunidade que se dão no primeiro processo de socialização. Além disso, as redes suportam não apenas laços relacionais fracos, mas laços fortes e íntimos, e podem permitir que laços estabelecidos nas redes virtuais tenham também presença na "vida real" dos envolvidos (WELLMAN, 1999; 2002; WELLMAN e GULIA, 1999).

Schlemmer *et al.* (2006) defendem que os espaços de convivência digital ampliam as possibilidades de interação, de comunicação e acesso a informações aos indivíduos, possibilitando a criação de redes complexas, nas quais a estrutura não segue um padrão regular e, por isso, as informações se propagam além do raio de ação direta. Diante disso, uma das principais características deste tipo de rede é a falta de controle e previsão quanto ao direcionamento das informações que provocam constantes mudanças na rede em termos de tempo e espaço.

Outra importante contribuição das redes sociais virtuais é discutida por Costa (2005) ao analisar o papel destas como importantes meios para a geração e aprimoramento do capital social, bem como do capital

cultural. Além disso, são nestas que o indivíduo encontra possibilidades de compartilhar ideias, informações e conhecimentos, o que poderia ser impossível com os próximos em redes locais em virtude das restrições de tempo e espaço.

No que diz respeito à identidade, as redes sociais virtuais podem ser compreendidas como a apropriação de um espaço no ciberespaço por um indivíduo que deseja ser visto e constrói sua identidade, dando origem a um "eu" na rede (RECUERO, 2004). Para Sibilia (2003) citada por Recuero (2004a), existe um imperativo da visibilidade na sociedade que decorre de uma ligação entre os âmbitos público e privado do indivíduo. Para existir no espaço dos fluxos é necessário ser visto e se tornar parte da rede.

No mesmo sentido, Rheingold (1996) analisa o papel das redes sociais virtuais na atualidade e afirma que estas não apenas possibilitam a interação e encontro de pessoas, mas se tornaram um ambiente no qual se pode alcançar objetivos definidos pela coletividade, além da possibilidade de se criar e obter informações relevantes que constituem a inteligência coletiva. Machado e Tijiboy (2005, p. 8) também defendem que as redes sociais virtuais podem ser úteis como espaços de aprendizado coletivo e de trocas cooperativas de conhecimento, contribuindo para "a mobilização dos saberes, o reconhecimento das diferentes identidades e a articulação dos pensamentos que compõem a coletividade".

Até aqui foi possível compreender o quadro conceitual e prático dos estudos de redes sociais, enfocando especialmente na tipologia de redes sociais virtuais, as quais são a base deste estudo, pois é o meio no qual os movimentos sociais serão analisados. A partir daí, torna-se necessário primeiramente elencar as formas pelas quais os movimentos sociais na atualidade se formam e se desenvolvem, conforme se verá na próxima seção.

Movimentos sociais e redes sociais

Na ótica marxista estruturalista, os movimentos sociais eram identificados por meio da ação histórica da sociedade em relação às contradições do capitalismo. Contudo, esta abordagem se tornou antiquada, visto

o crescimento dos movimentos sociais e de lutas direcionadas a diferentes causas. Esses fatos deram origem ao conceito de novos movimentos sociais (NMS), sendo este distante dos tradicionais conceitos de caráter classista dos movimentos camponeses e sindicais. Os novos movimentos foram identificados inicialmente por meio de ações de caráter predominantemente urbanos, tais como os movimentos pacifistas, das mulheres, pelos direitos civis, ambientalistas, etc., sendo que hoje existe uma enorme diversidade, especialmente alguns movimentos específicos de dados contextos sociais, históricos e culturais (MACHADO, 2007). Os novos movimentos sociais têm duas vantagens específicas se comparados aos movimentos sociais marxistas: colocam o ator no centro da análise e capturam características inovadoras destes movimentos que não se definem exclusivamente em relação ao sistema de produção (DELLA PORTA e DIANI, 2006).

As ações coletivas apresentam-se de forma múltipla e variável na contemporaneidade, sendo possível observá-las em diferentes níveis do sistema social. Nas análises atuais destes movimentos busca-se conceituar campos de conflito e, a partir daí, conhecer como os grupos sociais agem nestes. Já no passado, buscava-se analisar a condição social dos grupos e, posteriormente, as ações dos indivíduos decorrentes deste contexto. Isso se justifica em virtude da mudança do foco dos movimentos sociais que deixou de se basear em classes, raças e questões políticas tradicionais, voltando-se para o campo cultural, em virtude da complexidade da sociedade, das mudanças culturais e práticas sociais (MELUCCI, 1996).

Entendida a complexidade das sociedades contemporâneas, tais articulações podem se dar de forma plural, sendo que as lutas por cidadania envolvem várias dimensões: "de gênero, étnica, de classe, regional, mas também dimensões de afinidades ou de opções políticas e de valores: pela igualdade, pela liberdade, pela paz, pelo ecologicamente correto, pela sustentabilidade social e ambiental, pelo respeito à diversidade e às diferenças culturais, etc." (SCHERER-WARREN, 2006, p. 115).

Na visão de Melucci (1996, p. 36) houve uma transformação dos movimentos sociais a partir do final da década de 1970, deixando de existir apenas movimentos de atores políticos ou organizacionais e dando

origem a formas compreendidas como "movimentos como meio" (*movements as media*). Tal diferenciação é dada em função dos papéis e comportamentos assumidos pelos atores, bem como diante do foco assumido nas ações, sendo que por um lado os atores podem engajar-se em ações voltadas para reforma, inclusão, novos direitos, redefinição de regras políticas, e, por outro lado, atores que direcionam suas ações e questionamentos para formas ou condições culturais puras, que expressam conflitos e dilemas de orientações básicas da sociedade.

O descentramento do sujeito e o surgimento de uma pluralidade de atores possibilitaram o fortalecimento do conceito de cidadania a partir da década de 1990 no Brasil, da mesma forma que o conceito de autonomia vigorava na década de 1980. Esta cidadania se liga aos novos movimentos, em lutas pelo "reconhecimento de direitos sociais e culturais modernos", direcionados para causas ligadas a "raça, gênero, sexo, qualidade de vida, meio ambiente, segurança, direitos humanos, etc." (GOHN, 2004, p. 22). Para Edwards e McCarthy (2004), os novos movimentos se tornaram possíveis em virtude do surgimento de uma "nova classe média", atuando como "motores principais" destes.

De acordo com Aguiar (2007a, p. 12), outro público específico das redes de movimentos sociais têm sido os indivíduos com interesses em questões ambientais e desenvolvimento social, que passaram a se inserir em redes sociais temáticas, especialmente a partir da conferência da ONU sobre Meio Ambiente e Desenvolvimento (ECO-92). Estas redes possibilitam criar e manter uma "extensa rede invisível que caracteriza as articulações sociopolíticas no Brasil", que permitem construir debates e acordos à distância por meio das tecnologias da informação envolvidas".

Marteleto (2001, p. 73-74) chama a atenção para o fato de que muitos estudos têm apontado importantes "mudanças no perfil e na dinâmica dos movimentos sociais", sendo que um dos principais aspectos alterados foi o foco das mobilizações e reivindicações, que passou a ser direcionado para as "condições de vida da população" e não mais direcionado à "esfera da produção e do trabalho", visto que as lutas são baseadas na "ampliação do acesso ao espaço público".

Nos movimentos contemporâneos, os atores direcionam suas atenções para as diferenças entre sexos, idades e culturas. Considerando os

distintos focos dos movimentos e as especificidades dos modelos de organização e sistemas políticos, as ações tornam-se intimamente relacionadas com a vida cotidiana e a experiência individual, o que possibilita compreender a variedade de formas dos movimentos e de significados das ações coletivas (MELUCCI, 1996). Para Scherer-Warren (2006), o ativismo embasado nos valores da democracia, da solidariedade e da cooperação vem crescendo de forma significativa nos últimos anos, sendo orientado "aos mais excluídos, mais discriminados, mais carentes e mais dominados".

Os movimentos sociais são formados por agrupamentos heterogêneos, apesar de à primeira vista parecerem homogêneos. Além disso, guardam a característica de serem contínuos, visto que transcendem os episódios. A partir daí, pode-se compreendê-los como um sistema de ações coletivas, nos quais a continuidade das ações molda e forma os movimentos (MELUCCI, 1996). Também para Della Porta e Diani (2006, p. 2), não se pode pensar que os novos movimentos sociais, tais como o "*global justice movement*", são homogêneos. Desta forma, movimentos com bandeiras globais, como os sustentados por iniciativas contra a globalização neoliberal, se diferenciam em relação aos focos de manifestações (trabalho infantil, desmatamento, entre outros), das formas como os indivíduos se comportam nos eventos coletivos, dos pontos de vista assumidos, entre outros.

Os movimentos sociais contemporâneos assumem um formato de rede solidária com importantes significados culturais, e podem ser definidos como "*systems of action, complex networks among the different levels and meanings of social action*" (MELUCCI, 1996, p. 4). Além disso, Melucci (1996) os compara com a metáfora "profetas do presente", que exercem influência não por força de aparatos, mas por meio do poder da palavra, anunciando o início de mudanças.

Neste sentido, Scherer Warren (2005) argumenta que para melhor compreensão dos movimentos sociais contemporâneos é necessário se entender como os indivíduos se tornam sujeitos de seus destinos pessoais e como os sujeitos se transformam em atores políticos por meio de seus envolvimentos em redes. E, vistas as novas possibilidades disponíveis para os movimentos sociais, a autora informa alguns aspectos que as análises

neste campo podem buscar esclarecer: a) a forma pela qual os atores e organizações locais interagem com agentes coletivos nos planos regionais, nacionais e transnacionais; b) quais organizações, atores e movimentos são integrados ou excluídos pelas redes e quais as razões que levam à formação de tal estrutura; c) qual a forma que as interações assumem nas redes de informação e quais seus resultados, tais como o tipo de solidariedade, de estratégia, os mecanismos de negociação, representações simbólicas, interculturalismo, entre outros.

Kraemer, Whiteman e Banerjee (2013) reforçam a ideia da transnacionalidade e da estratégia de movimentos sociais, demonstrando, por meio de um caso ocorrido na Índia, que um movimento local se expandiu e se fortaleceu além das fronteiras daquele país a partir de ações e estratégias iniciadas por um indivíduo que se tornou porta-voz do movimento. Neste caso, foi possível se constatar a importância das redes para efetivar coalisões e para a formação dos processos de mobilização nos âmbitos nacional e internacional.

As redes sociais passaram a ser aplicadas na análise dos movimentos sociais a partir dos anos 1970, a partir do *boom* desta área na sociologia, em especial na abordagem dos novos movimentos sociais. A existência de redes de indivíduos e organizações que formam um coletivo em rede pode ser compreendida como o surgimento de segmentos que formam um movimento social. Há também a possibilidade de formação de redes de movimentos sociais que se formam de modo complexo e transcendem a delimitação de organizações, conectando indivíduos e atores coletivos de forma simbólica, solidária ou estratégica (SCHERER-WARREN, 2005). No caso brasileiro, Sherer-Warren (2005) informa alguns exemplos de redes de movimentos, tais como: redes estratégicas de denúncias - Diretas Já, Caras Pintadas, Gritos dos Excluídos; redes de estratégias de desobediência civil – Movimento dos Sem-Terra, Movimentos dos Sem-Teto; redes de luta contra a exclusão – Ação da Cidadania, Economia Solidária; e redes de negociação na esfera pública – Agenda 21, Conselhos Setoriais, Orçamento Participativo.

Ao se falar em redes de movimentos sociais, deve-se assumir que mesmo neste tipo de redes há distintas formas e intensidades de poder, visto que os centros de poder são democratizados, mas ainda assim pode

haver elos mais fortes, com maior poder de influência e decisão (SCHERER-WARREN, 2006). Para Cogo e Brignol (2011), as redes possuem relações de poder que são expressas em disputas e assimetrias nas esferas de comunicação e cultura. A partir daí compreende-se que a forma como o poder se apresenta e é exercido tem relação com o modo como as relações se estruturam e com a intensidade e tipos de participação dos indivíduos na rede.

Além disso, as redes sociais afetam a participação na ação coletiva e podem ampliar as oportunidades dos indivíduos para se envolverem e fortalecerem o ativismo. Contudo, as redes não são apenas facilitadoras da ação coletiva, mas são também produto resultante destas, visto que a participação possibilita a formação de novas ligações/relações. Contudo, as redes não são o fator mais importante para o estabelecimento de laços nos movimentos sociais, visto que a capacidade de motivar pessoas pode ser realizada por meio de movimentos já fortalecidos e não pelas conexões em rede. Assim, pode-se compreender a capacidade anônima de certos movimentos ao encorajar a participação de outros indivíduos pelo simples fato de se mostrarem maduros e fortalecidos. Além disso, em muitos casos, os laços entre redes, ao invés de encorajar, acabam por desencorajar a participação de outros indivíduos e grupos (DELLA PORTA e DIANI, 2006).

Há uma tendência contemporânea de agregação social, com base em uma nova cultura política, tendendo ao aumento da participação popular quando se está em discussão a busca por justiça social e a construção de uma sociedade mais solidária. O que dá sustentação para este tipo de ação coletiva é a busca de interesses comuns e uma maior conscientização dos indivíduos sobre o contexto no qual estão inseridos. Para isto, o ciberespaço se mostra como um ambiente propício para a troca de informações, sendo que as ações não se situam apenas no campo virtual e nem se esgotem nele. Normalmente, os movimentos sociais são advindos de práticas fora do ambiente virtual e encontram no ciberespaço um local de confluência dos interesses da coletividade (PERUZZO, 2002).

É neste espaço que são ofertados aos usuários formas e tempos diferenciados de tempo e de espaço por meio de diferentes artefatos digitais. Por meio destes artefatos o ciberespaço se torna um instrumento de cone-

xão de forma a catalisar e potencializar ações, o que o torna interesse para estudos antropológicos e sociológicos, por causa de sua possibilidade de canalizar o vitalismo social (LÉVY, 2002; LEMOS, 2004). Para Haug (2013), os movimentos sociais se encontram em uma arena na qual são encontradas três formas de ordenamento social em relação aos grupos de ações coletivas, sendo estes a ordem da organização, a da instituição e a de rede, de acordo com os interesses dos organizadores dos movimentos. Para o autor, as redes se constituem como uma infraestrutura que objetiva atender ao movimento e às mobilizações buscando criar formas de sincronizar as atividades dos indivíduos dispersos em relação ao tempo e espaço.

De forma geral, e em concordância com pensamento de Chua, Madej e Wellman (2011, p. 106), os *sites* de redes sociais apenas incrementam as relações na vida real, visto que "*such social networking sites do not suppress offline social contact, but they are integrated with it, as many relationships are migratory: moving from being online only to combining online with offline contact*". As redes sociais colaboram com o recrutamento e inserção das pessoas nas ações coletivas dos movimentos sociais, além de favorecerem a partir de ações iniciais, que se desenvolva posteriormente uma consciência política (GAMSON, 1992).

As ligações estabelecidas entre grupos estabelecem um canal de comunicação que possibilita promover iniciativas conjuntas, ampliando os laços de solidariedade e confiança entre os grupos, bem como a continuidade das ações ao longo do tempo. O capital social estabelecido nas relações entre grupos favorece o desenvolvimento ou descoberta de oportunidades para os indivíduos e a coletividade. Desta forma, as redes fornecem condições para que a predisposição se transforme em ações, também influenciadas pelos laços estabelecidos e pelos canais de comunicação (DELLA PORTA e DIANI, 2006).

O desenvolvimento da CMC e da internet tem possibilitado a formação e desenvolvimento deste tipo de rede. Para Frey (2003, p. 177), a internet pode possibilitar "modos de relacionamento transversais e estruturas mais fluidos, em maior sintonia com as estruturas de redes, que caracterizam os processos sociais e políticos nas sociedades democráticas modernas". Além disso, Frey destaca as possibilidades de acesso à informação independentemente da distância espacial, podendo ser

transmitida em tempo real, fatos estes que colaboram com as demandas e expectativas de cidadãos envolvidos em processos de decisão e participação democrática. Para Della Porta e Diani (2006), o desenvolvimento da CMC favorece a realização de ações coletivas, reforçando e facilitando o ativismo, visto sua capacidade de possibilitar a manutenção de laços estabelecidos nos espaços reais/físicos e por dar suporte técnico para as atividades dos grupos.

Organização de movimentos sociais nas redes sociais virtuais

As características de interatividade, cooperação e descentralização da internet abriram espaço para as lutas sociais a partir da segunda metade da década de 1990, hajam vista as possibilidades de difusão de reivindicações, disseminação de ideias e estabelecimento de contatos, e sem ter a necessidade de passar pelos filtros ideológicos da grande mídia. Desta forma, "a militância *on-line* vem alargar a teia comunicacional planetária, usufruindo de uma das singularidades do ciberespaço: a capacidade de disponibilizar, em qualquer espaço-tempo, variadas atividades, formas e expressões de vida." (MORAES, 2000, p. 142).

O ciberespaço e a dinâmica propiciada por este em termos de aproximação de diferentes tempos culturais resulta em uma sinergia entre as redes presenciais e redes virtuais. Além das articulações entre as redes virtuais e presenciais, novas possibilidades de articulações podem ser vislumbradas, seja na relação entre legados históricos e projetos de transformações ou mesmo na relação entre escalas locais e globais dos movimentos (SCHERER-WARREN, 2005).

Há uma importância nas mudanças em relação aos modos como a informação passou a circular nas mídias, passando de uma "lógica hegemônica de transmissão das informações de forma massiva e generalizada, de um pequeno grupo produtor a um coletivo indiscriminado" para uma forma na qual há "possibilidade de produção de informação e estabelecimento de comunicação de uma forma mais descentralizada e distribuída para públicos segmentados". Embora a interatividade possa

ser vista em outras mídias, é na internet que ela apresenta maior predominância e força (COGO e BRIGNOL, 2011, p. 83).

Como o ciberespaço se constitui em um "universal indeterminado", a falta de controle e de hierarquias aparentes possibilita que as partes possam se reinventar em densidades e extensões distintas sem se sobreporem ou subjugarem as demais. Por estas características, pode ser denominada de "Babel cultural", visto a constante mutação e desordem saudável dos espaços disponíveis (MORAES, 2000, p. 143). Edwards e McCarthy (2004) apontam a importância da internet para os movimentos sociais em virtude das possibilidades disponibilizadas para disseminar informações e coordenar atividades em diferentes grupos sociais. No entendimento de Klandermans e Staggenborg (2002, p. 332), a internet pode se configurar como uma rica fonte de dados para se analisar tais movimentos em virtude da crescente difusão de informações em seu espaço.

A internet serve, portanto, como importante complemento para as ações políticas, engajamento cívico e participação democrática, o que não significa que os processos tradicionais se encerrem em virtude desta nova dinâmica de participação, mas que os indivíduos têm à disposição novos espaços para diferentes tipos de deliberações democráticas (FREY, 2003). Para Scherer-Warren (2005, p. 83), as redes virtuais resultantes do ciberativismo são intencionais e "*transciendem las fronteras espaciales de las redes presenciales, creando, por lo tanto, territorios virtuales cuyas configuraciones se definen por las adhesiones a uma causa o por afinidades políticas, culturales o ideológicas*". Desta forma, há um deslocamento das fronteiras comunitárias e locais tradicionais, podendo se verificar o desenvolvimento de um potencial de ações coletivas na era da informação.

O ciberespaço se coloca como um ambiente com capacidade de revitalizar lutas e movimentos civis, já que constantemente aumenta o número de indivíduos que procuram tais espaços ansiando por expressar-se. Apesar de anárquica, a internet se mostra bem mais democrática que as mídias de massa, característica esta que se fortalece ainda mais quando se consideram o barateamento dos custos, o aumento do raio de abrangência global e a rápida velocidade de circulação de informações

(MORAES, 2000). Com apenas um clique, uma pessoa pode fortalecer um movimento, como, por exemplo, assinando um abaixo-assinado, o que nos remete a um novo conceito de 'cliqueativismo'. Este fato ainda colabora com o entendimento das chamadas "forças dormentes" que Machado (2007, p. 278) argumenta serem importantes para os movimentos sociais nas redes virtuais, visto que estas forças são relacionadas a pessoas que fazem parte da rede e, apesar de não muito engajadas, podem se identificar com certas causas e ações, e fortalecê-las em dados momentos.

Machado (2007) alerta para a existência de movimentos sociais que ocorrem em zonas cinzas de descontrole, nas quais se torna difícil estabelecer controle e responsabilidades. A exemplo desses movimentos, o autor aponta para o "hacktivismo" e o "ciberterrorismo", os quais se utilizam de ataques virtuais a *sites* e sistemas diversos de organizações. Nos dias atuais, um movimento que tem ganhado força neste contexto advém de ações do grupo intitulado como *Anonymous*.

Apesar das diversas possibilidades para o desenvolvimento de movimentos sociais, Moraes (2000, p. 153) argumenta que alguns fatores requerem melhor análise do quadro de expectativas que a internet pode propiciar. Para o autor, "a cibermilitância necessita aprofundar experiências de comunicação eletrônica" e, além disso, ao mesmo tempo em que o fenômeno dos movimentos se torna muito rápido graças à tecnologia, também se mostra muito lento devido aos hábitos culturais e políticos. Além dos aspectos mencionados, a internet pode dar maior visibilidade para certos movimentos, mas isso não retira o poder predominante de determinadas mídias de massa que são bem perceptíveis na atualidade.

Desta forma, as redes sociais virtuais se mostram como um importante espaço de interação, reconhecimento e ação, mas podem requerer, em certos casos, outros tipos de recursos e ambientes para desenvolver os movimentos sociais. Para Scherer-Warren (2006, p. 112), por exemplo, as mobilizações contemporâneas na esfera pública resultam de articulações entre "atores dos movimentos sociais localizados, das ONGs, dos fóruns e redes de redes, mas buscam transcendê-los por meio de grandes manifestações na praça pública, incluindo a participação de simpatizantes,

com a finalidade de produzir visibilidade através da mídia e efeitos simbólicos para os próprios manifestantes (no sentido político-pedagógico) e para a sociedade em geral".

Uma importante discussão a respeito das redes de movimentos sociais reside no fato das múltiplas participações em movimentos sociais, possibilidade esta que se eleva quando se leva em consideração as ações no ambiente virtual. Conforme esclarecido por Della Porta e Diani (2006), alguns tipos de grupos exigem afiliação exclusiva, tal como organizações políticas, enquanto outros possibilitam múltiplas afiliações, como no caso de grande parte dos movimentos sociais. A múltipla afiliação possibilita aos indivíduos e grupos acessarem diferentes áreas e estabeleceram relações de confiança com demais grupos que podem apoiar as ações desenvolvidas, se tornando um importante canal para a articulação de iniciativas. Ao estudar a participação política de jovens brasileiros, Mische (1997, p. 145) argumenta que o contexto brasileiro apresenta uma característica de "militância múltipla", podendo ser observado por meio da participação dos indivíduos em uma série de movimentos (estudantis, políticos, religiosos), o que leva a crer que as redes de movimentos são extremamente interligadas.

Mesmo tendo clara a grande possibilidade que as redes virtuais oferecem para a integração e articulação dos movimentos sociais, Machado (2007) argumenta que ainda não se pode definir a exatidão dos impactos destas para os movimentos, até mesmo porque os estudos neste campo são insuficientes. Contudo, pode-se afirmar que as redes sociais virtuais são um importante marco em relação à atuação dos/nos movimentos sociais, provocando consideráveis alterações na forma como as relações e as ações coletivas se estabelecem e se desenvolvem, bem como no impacto de tais redes para os resultados esperados. Além disso, fatores como a motivação, significados e organização das ações coletivas dos movimentos sociais não se mostram tão claros, mas, de certo modo, intrigantes e desafiadores.

Vistas as possibilidades e desafios de estudos no campo dos movimentos sociais a partir de sua presença e estruturação nas redes sociais virtuais, a próxima seção procura apresentar as principais considerações a que se pôde chegar nesta discussão teórica.

Considerações finais

Como se propôs na discussão acima, uma forma de promover a emancipação do indivíduo pode ser encontrada na criação e ampliação dos espaços que promovam maiores possibilidades de interação entre eles e de seus grupos como forma de participarem de discussões e ações para o alcance de objetivos, anseios e demandas coletivas. Neste sentido, as redes sociais virtuais parecem despontar como importantes espaços nos quais as demandas individuais possam ser identificadas e reconhecidas como coletivas e permitir que a cooperação dê maiores condições de ação aos indivíduos, especialmente se comparadas às ações individualizadas.

A busca por emancipação, igualdade e/ou tipos de reconhecimento passa a ser realizada exclusivamente em espaços virtuais de interação ou como extensão dos espaços reais/físicos disponíveis. Estes espaços virtuais denominados de ciberespaços e estruturados na internet têm permitido novos formatos de organização social e a criação, estabelecimento e repercussão de movimentos sociais em várias partes do mundo, em especial pelo que se conhece como "redes sociais virtuais" ou "redes sociais na internet". Estas redes, baseadas no desenvolvimento da *Web* 2.0 e de *softwares* sociais, têm ganhado espaço na sociedade permitindo uma maior interação entre as pessoas.

Como resultado e exemplo das mudanças, há constantes repercussões na mídia mundial em relação às ações coletivas que se desenvolvem nestas redes, especialmente nos casos de alguns regimes autoritários que foram desestabilizados ou ruíram a partir de movimentos iniciados e/ou organizados em redes como *Facebook* e *Twitter*, sendo alguns dos casos mais recentes os relacionados com regimes autoritários de países como Egito e Líbia, por meio do que se denomina de Primavera Árabe. Além disso, outros vários eventos têm sido abrigados nas redes sociais, tais como movimentos contra a corrupção, formas de autoritarismo e opressão, violência, homofobia, racismo, entre outros dos contextos sociais e econômicos. No Brasil, por exemplo, tem-se deparado atualmente com constantes movimentos abrigados nas redes sociais virtuais, em especial os direcio-

nados a questões políticas, como nos casos do "Fora Renan" direcionados a manifestações pela saída do Senador Renan Calheiros da presidência do Senado Federal e no movimento a favor da saída do deputado federal Marcos Feliciano da presidência da Comissão de Direitos Humanos e Minorias da Câmara (CDHM). Além disso, impacto maior pôde ser observado no Brasil nas manifestações de Junho de 2013 que encontraram muitas possibilidades de organização de ações em redes sociais virtuais como o Facebook e *Twitter*, bem como um espaço para divulgação de ações e para a criação e divulgação de ideias e comportamentos políticos.

Estas redes têm desempenhado um papel importante nos mais diversos países e com os mais distintos propósitos a partir da (re)definição da dinâmica relacional entre grupos sociais com a sociedade de forma mais ampla ou relacionados diretamente ao Estado, ainda que influenciados por grupos políticos. A relevância destas redes para a organização social já se mostra latente e tem ocasionado importantes mudanças nas formas como a democracia é realizada *na* e *por meio* da internet, configurando o que se se denomina de 'ciberdemocracia' por intermédio do desenvolvimento da 'cibercultura'. Contudo, este contexto ainda é repleto de questionamentos e necessidades de esclarecimentos quanto às interações sociais e à organização dos grupos e de suas ações. Várias discussões têm vindo à tona quanto às formas virtuais de ações que se configuram como ativismo virtual e ações baseadas em 'simples' compartilhamentos de informações por meio do que se pode definir de 'cliqueativismo', isto é, possibilidades de ação apenas no espaço virtual por meio do compartilhamento e disseminação de informações entre os grupos sociais dos quais se faz parte.

Como contribuição teórica, este ensaio permitiu a organização de conceitos e o esclarecimento de contextos relacionados aos movimentos sociais organizados em redes, especialmente nas chamadas redes sociais virtuais, fato que colabora com a produção científica em uma área que se encontra em desenvolvimento. Desta forma, o enfoque sobre estes dinâmicos espaços e movimentos pode propiciar novos olhares de pesquisadores sobre a influência dos novos aparatos de comunicação e interação sobre as ações coletivas de movimentos sociais, bem como sobre a importância da computação social na contemporaneidade ao permitir

a aproximação dos indivíduos e a busca de objetivos comuns e compartilhados, o estabelecimento de novos arranjos organizacionais para os movimentos e a concessão de novas possibilidades relacionais nos movimentos que acompanhem os dinâmicos contextos dos relacionamentos na sociedade.

Este estudo apresenta como limitação a própria natureza dos objetos discutidos e suas formações conceituais recentes que, por serem demasiadamente fluidos e dinâmicos, requerem cuidado em termos de definições precisas e de julgamentos sobre suas influências na sociedade contemporânea. Além disso, outra limitação se encontra na não aplicação dos conceitos em casos reais de forma aprofundada e apenas o uso de citações de casos recentes nos quais os objetos em discussão podem ser encontrados, o que se justifica em função da natureza deste como um ensaio teórico.

Por fim, aponta-se como possibilidade de estudos que se investiguem os conceitos relacionados ao ciberespaço das redes sociais virtuais e as ações coletivas de movimentos sociais em casos reais ocorridos desde o nível nacional ao local, especialmente buscando verificar a influência da rede de relacionamentos virtuais sobre este contexto. Desta forma, talvez seja possível verificar as relações entre movimentos sociais distintos nas redes e suas ligações, bem como a integração de ativistas de diferentes localizações em um mesmo movimento, buscando ressaltar a importância das redes virtuais e de suas ferramentas para a aproximação destes e do alinhamento de ideias e ações. Outros estudos podem buscar discutir como a formação de redes sociopolíticas virtuais são formadas independemente da proximidade geográfica, bem como as possibilidades de organização e acompanhamento das ações coletivas por meio do ciberespaço das redes.

Referências

AGUIAR, S. Redes sociais na internet: desafios à pesquisa. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 30., Santos – 29 ago. a 2 set. 2007. Anais... Santos: Intercom, 2007a. Disponível em: <http://www.

sitedaescola.com/downloads/portal_aluno/Maio/Redes%20sociais%20na%20internet-%20desafios%20%E0%20pesquisa.pdf>. Acesso em: 12 jan. 2012.

AGUIAR, S. Formas de organização e enredamento para ações sociopolíticas. **Informação & Informação**, v. 12, ed. esp., 2007b. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/viewFile/1776/1514>. Acesso em: 29 fev. 2012.

BAUDRILLARD, J. **Tela total**: mito-ironias da era do virtual e da imagem. Trad. Juremir Machado da Silva. Porto Alegre: Sulina, 1997.

BOYD, D. The significance of social software. In: BURG, T. N.; SCHMIDT, J. (Ed.) **BlogTalks reloaded**: social software research & cases. Norderstedt: Books on Demand, 2007a. p.15-30. Disponível em: <http://www.danah.org/papers/BlogTalkReloaded.pdf>. Acesso em: 27 fev. 2012.

BOYD, D. None of this is real: identity and participation in Friendster. In: KARAGANIS, J. (Ed.) **Structures of Participation in Digital Culture**. New York: Social Science Research Council, 2007b. p. 132-57.

BOYD, D. M.; ELLISON, N. B. Social network sites: definition, history, and scholarship. **Journal of Computer-Mediated Communication**, v.13, n.1, 2007. p.210-230. Disponível em: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>. Acesso em: 27 fev. 2012.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CHUA, V.; MADEJ, J.; WELLMAN, B. Personal communities: The world according to me. In: CARRINGTON, P.; SCOTT, J. (Ed.) **Handbook of Social Network Analysis**. Thousand Oaks, CA: Sage, 2011. pp. 101-115. Disponível em: <http://homes.chass.utoronto.ca/~wellman/publications/personal/Personal%20Communities%20-%20The%20World%20According%20to%20Me.pdf>. Acesso em: 28 fev. 2012.

COGO, D.; BRIGNOL, L. D. Redes sociais e os estudos de recepção na Internet. **Revista Matrizes**, São Paulo, v.4, n. 2, p. 75-92, jan./jun., 2011.

COSTA, R. Por um novo conceito de comunidade: redes sociais, comunidades pessoais, inteligência coletiva. **Interface - Comunicação, Saúde, Educação**, v.9, n.17, p.235-48, mar/ago 2005. Disponível em: <http://www.scielo.br/pdf/icse/v9n17/v9n17a03.pdf>. Acesso em: 19 jan. 2012.

DELLA PORTA, D.; DIANI, M. **Social movements**: an introduction. 2.ed. Oxford: Blackwell Publishing, 2006.

EDWARDS, B.; McCARTHY, J. D. Resources and social movement mobilization. In: SNOW, D. A.; SOULE, S. A.; KRIESI, H. (Org.) **The blackwell companion to social movements**. Oxford: Blackwell. 2004.

FREY, K. Desenvolvimento sustentável local na sociedade em rede: O potencial das novas tecnologias de informação e comunicação. **Revista de Sociologia e Política**, Curitiba, n.21, p. 165-185, nov. 2003.

GAMSON, W. A. **Talking Politics**. New York: Cambridge University Press, 1992. 272p.

GOHN, M. G. Empoderamento e participação da comunidade em políticas sociais. **Saúde e Sociedade**, v.13, n.2, p.20-31, 2004.

GOSLING, S.; AUGUSTINE, A.; VARZIRE, S. et al. Manifestations of personality in online social networks: self-reported Facebook-related behaviors and observable profile information. **Cyberpsychology, Behavior, and Social Networking**, v.14, n.9, 2011. p. 483-488.

HAUG, C. Organizing spaces: Meeting arenas as a social movement infrastructure between organization, network, and institution. **Organization Studies**, v.34, n.5-6, 2013. p. 705-732.

KLANDERMANS, B.; STAGGENBORG, S. Introduction. In: KLANDERMANS, B.; STAGGENBORG, S. (Org.) **Methods of social movement research. Social movements, protest, and contention**. Minneapolis: University of Minnesota , 2002. v.16.

KRAEMER, R.; WHITEMAN, G.; BANERJEE, B. Conflict and astroturfing in Niyamgiri: the importance of national advocacy networks in anti-corporate social movements. **Organization Studies**, v.34, n.5-6, 2013. p. 823-852.

LEMOS, A. **Cibercultura**: tecnologia e vida social na cultura contemporânea. 2. ed. Porto Alegre: Sulina, 2004. 295p.

LÉVY, P. **Cibercultura**. Trad. Carlos Irineu da Costa. 2. ed. São Paulo: Editora 34, 2000. 260p.

LÉVY, P. **Ciberdemocracia**. Trad. Alexandre Emílio. Lisboa: Instituto Piaget, 2002. 249p.

MACHADO, J. A. Ativismo em rede e conexões identitárias: Novas perspectivas para os movimentos sociais. **Sociologias**, Porto Alegre, v, 9, n, 18, p. 248-285, jul./dez., 207.

MACHADO, J. R.; TIJIBOY, A. V. Redes Sociais Virtuais: Um espaço para efetivação da aprendizagem cooperativa. Novas Tecnologias na Educação.Porto Alegre, v.3, n.1, mai., 2005. Disponível em: <http://seer.ufrgs.br/renote/article/view/13798/7994>. Acesso em: 25 jan. 2012.

MARQUES, E. Os mecanismos relacionais. **Revista Brasileira de Ciências Sociais**, São Paulo, v. 22, n. 64, p. 157-161, 2007.

MARTELETO, R. M. Análise das redes sociais: Aplicação nos estudos de transferência da informação. **Ciência da Informação**, Brasília, v. 30, n. 1, p.71-81, jan./abr. 2001. Disponível em: <http://www.scielo.br/pdf/%0D/ci/v30n1/a09v30n1.pdf>. Acesso: 18 jan. 2012.

MELUCCI, A. **Challenging codes**: collective action in the information age. New York: Cambridge University, 1996.

MISCHE, A. **De estudantes a cidadãos**: Redes de jovens e participação política. **Revista Brasileira de Educação**, São Paulo, n. 5/6, p. 134-50, 1997.

MORAES, D. Comunicação virtual e cidadania: Movimentos sociais e políticos na Internet. **Revista Brasileira de Ciências da Comunicação**, São Paulo,v. 23, n. 2, p. 142-155, 2000.

NEGROPONTE, N. **Vida digital**. Trad. Sérgio Tellaroli. 2.ed. São Paulo: Companhia das Letras, 1995.

PERUZZO, C. M. K. Comunidade em tempo de redes. In: PERUZZO, C. M. K.; COGO, D.; KAPLÚN, G. (Org.) **Comunicação e movimentos populares**: quais redes? São Leopoldo: Unisinos, 2002. p. 275-298. Disponível em: <http://www.ciciliaperuzzo.pro.br/artigos/comunidades_em_tempos_de_redes.pdf>. Acesso em 13 fev. 2012.

PRIMO, A. F. T. A emergência das comunidades virtuais. In: INTERCOM - CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 20., Santos,1997.Anais... Santos, 1997. Disponível em: <http://www.sitedaescola.com/downloads/portal_aluno/Maio/A%20emerg%EAncia%20das%20comunidades%20virtuais.pdf>. Acesso em: 18 jan. 2012.

RECUERO, R. C. Webrings: As Redes de Sociabilidade e os Weblogs. **Revista Sessões do Imaginário**, Porto Alegre, v.11, p.19-27, 2004a. Disponível em: <http://www6.ufrgs.br/limc/PDFs/webrings.pdf>.Acesso em: 18 jan. 2012.

RECUERO, R. C. Teoria das Redes e Redes Sociais na Internet: Considerações sobre o Orkut, os weblogs e os fotologs. In: INTERCOM - CON-

GRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 27., Porto Alegre, 2004b. Anais... Disponível em: < http://galaxy.intercom.org.br:8180/dspace/bitstream/1904/17792/1/R0625-1.pdf>. Acesso em: 18 jan. 2012.

RECUERO, R. C. Dinâmicas de Redes Sociais no Orkut e Capital Social. **UNIRevista Uni Sinos**, São Leopoldo, v.1, n.3, jul. 2006. Disponível em: <http://www.unirevista.unisinos.br/_pdf/UNIrev_daCunha.PDF>. Acesso em: 25 jan. 2012.

RHEINGOLD, H. **Comunidade virtual**. Trad. Helder Aranha. Lisboa: Gradiva, 1996.

SANTOS JÚNIOR, D. L.; MANTOVANI, D. M. N. Comunicação nas redes sociais: Um estudo com usuários das comunidades do Orkut. **Análise**. Porto Alegre, v.21, n.1, p.30-41, jan./jun., 2010. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/face/article/viewFile/8235/5905>. Acesso em: 17 jan. 2012.

SCHERER-WARREN, I. Redes sociales y de movimientos en la sociedad de la información. **Revista Nueva Sociedad**, Caracas, n.196, mar-abr, p. 77-92, 2005.

SCHERER-WARREN, I. Das mobilizações às redes de movimentos sociais. **Revista Sociedade e Estado**. Brasília-DF, v.21, p. 109-130, 2006.

SCHLEMMER, E.; BACKES, L.; FRANK, P. S. S. et al. A criação de um Espaço de Convivências Digital Virtual. In: SIMPÓSIO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO , 17., Brasília, 2006. Disponível em: <http://www.br-ie.org/pub/index.php/sbie/article/view/507/493>. Acesso em: 10 jan. 2012.

SZELL, S.; THURNER, S. Measuring social dynamics in a massive multiplayer online game. **Social Networks**, v.32, 2010. p. 313-329.

WELLMAN, B. Network analysis: from method and metaphor to theory and substance. In: WELLMAN, B.; BERKOWITZ, S. D. (Ed.). **Social structures**: a network approach. New York: Cambridge University , 1988. p.19-61. Disponível em: < http://homepage.ntu.edu.tw/~khsu/network/reading/wellman2.pdf>. Acesso em: 09 fev. 2012.

WELLMAN, B. From little boxes to loosely-bounded networks: the privatization and domestication of community. In: ABU-LUGHOD (Ed.) **Sociology for the twenty-first**: century: continuities and cutting edges. Chigaco: University of Chicago, 1999. p.94-114. Disponível em: <http://homes.chass.utoronto.ca/~wellman/publications/littleboxes1/littleboxes1.pdf>. Acesso em: 10 fev. 2012.

WELLMAN, B. Little Boxes, Glocalization, and Networked Individualism. In TANABE, M., BESSELAAR, P. V. D.; ISHIDA, T. (Ed.) **Digital Cities II**: computational and sociological approaches. Berlin: Springer-Verlag, 2002. p. 11-25. Disponível em: <http://homes.chass.utoronto.ca/~wellman/publications/littleboxes/littlebox.PDF>. Acesso em: 10 fev. 2012.

WELLMAN, B.; BERKOWITZ, S. D. **Social structures**: a network approach. New York: Cambridge University, 1988.

WELLMAN, B.; GULIA, M. Net surfers don't ride alone: virtual communities as communities. In: KOLLOCK, P.; SMITH, M. (Ed.) **Communities and Cyberspace**. New York: Routledge, 1999. Disponível em: <http://homes.chass.utoronto.ca/~wellman/publications/netsurfers/netsurfers.pdf>. Acesso em: 09 fev. 2012.

VI

Privacidade e confidencialidade das informações em saúde: voluntariado, documentação e ética

18

Voluntários em serviços de saúde: implicações para a privacidade dos pacientes

Siomara Roberta de Siqueira[1]
Elma Lourdes Campos Pavone Zoboli[2]

Introdução

Neste capítulo discute-se aspectos do voluntariado na área da saúde com foco nas questões de privacidade e confidencialidade das informações de pacientes que emergem nesse contexto e na relação entre voluntários, usuários/família e profissionais.

Voluntariado é uma palavra polissêmica. Há várias definições para voluntariado, associadas à filantropia, solidariedade, caridade e fraternidade com fundo religioso que traduz contextos e aspectos históricos, culturais, políticos e ideológicos. Nas formas de definir voluntariado alguns pontos em comum podem ser destacados: conjunto de atividades sociais realizada sem recompensa financeira; prática que traduz um conjunto de crenças e valores de determinado grupo ou cultura; atividade orientada para responder a situações de exclusão e sofrimento; atuação direcionada para o desenvolvimento e fortalecimento do tecido social; forma de inserção precária no mercado de trabalho; atividade humanística realizada por empatia e compaixão com o sofrimento de semelhantes; estratégia de

1 Siomara Roberta de Siqueira (siomara@isaude.sp.gov.br) é Psicóloga e Enfermeira, Mestre em Ciências da Saúde pela Coordenadoria de Controle de Doenças da Secretaria de Estado da Saúde de São Paulo (SES/SP) e Assistente Técnica de pesquisa científica e tecnológica – nível V do Instituto de Saúde da SES/SP.
2 Elma Lourdes Campos Pavone Zoboli é graduada em Enfermagem, Doutora em Saúde Pública pela Universidade de São Paulo e Docente da Escola de Enfermagem da Universidade de São Paulo.

apoio a comunidades carentes (BRASIL, 1998; MARQUES, 2006; SELLI et. al, 2008; SOUZA et. al, 2010).

O trabalho voluntário teve influência de princípios religiosos e da Igreja Católica de maneira especial com a prática da benemerência e da evangelização. No século XX quando guerras mundiais espalharam miséria e orfandade, houve ação conjunta de governos e de organizações religiosas para dar atenção aos "pobres" e "mais necessitados" vítimas desses conflitos (KISNERMAN, 1983; THOMPSON et. al, 2000).

Segundo a UNV (Voluntários da Nações Unidas), o voluntariado engaja pessoas no enfrentamento de desafios da pobreza e subdesenvolvimento dos países e é capaz de transformar o ritmo do seu desenvolvimento. O voluntariado beneficia tanto a sociedade em geral quanto o indivíduo voluntário, ao fortalecer a confiança, solidariedade e reciprocidade entre os cidadãos, e ao criar propositadamente oportunidades para a participação (CIVICUS, 2008).

Na Europa, após a Segunda Guerra Mundial, com o Estado de bem-estar social, se desenvolvem as associações de voluntários. Aumentam o voluntariado e a participação dos cidadãos em espaços de atenção aos indivíduos e famílias, às organizações sociais e nas iniciativas por mudanças positivas no âmbito dos direitos humanos e sociais, por meio de planejamento, gestão e avaliação de políticas públicas e ação humanitária (SIQUEIRA, 2008).

A atividade do voluntário na saúde, considerada como atividade social, tem seu reconhecimento por meio de programas de Voluntários das Nações Unidas (UNV) vinculado à Organização das Nações Unidas (ONU). A atividade do voluntário contribui para a paz e para o desenvolvimento em todo o mundo (CIVICUS, 2008).

Existente há algumas décadas na saúde, as ações do voluntariado podem reduzir o impacto da exclusão social das formas avançadas de capitalismo, contribuindo para criar novas formas de solidariedade sustentável (SELLI et. al, 2008).

Existem diversas formas de exercer o voluntariado, que variam de acordo com o contexto, o foco e os propósitos das ações. No Brasil, a tradição do voluntariado esteve mais presente na forma de doação de dinheiro ou de tempo de trabalho (PORTAL DO VOLUNTÁRIO, 2014).

Merhy (1997), ao analisar o processo de trabalho em saúde em suas dimensões tecnológicas, explicita as categorias: tecnologias duras, repre-

sentadas pelas máquinas, normas, estruturas organizacionais, tecnologias leve-duras, representadas pelos saberes estruturados, normas e rotinas (como a clínica médica, a epidemiologia, etc.), e tecnologias leves (tecnologias de relações do tipo produção de vínculo, autonomização, acolhimento, gestão como forma de governar processos de trabalho). Nessa visão, o voluntariado se insere no âmbito da tecnologia leve. Pode criar espaço de acolhimento, ampliando e humanizando o apoio oferecido pelas instituições.

A vulnerabilidade diante do processo de adoecimento e morte favorece a necessidade de interação e compartilhamento das histórias pessoais na convivência e na relação de apoio e auxilio entre o voluntário, a família e a equipe. Cria-se aí a contradição com as questões pessoais e íntimas, o que justifica a preocupação com as questões referentes à privacidade (BERRY e PLANALP, 2009; GRIEP et. al, 2015).

Apesar do voluntariado já estar presente há muito tempo nas unidades de saúde, ele ainda é pouco conhecido quanto às atividades que realizam. No intuito de conhecê-lo melhor, o Instituto de Saúde desenvolveu em 2008-2009, com apoio da FAPESP (Processo: 07/51663-9), uma pesquisa intitulada "Humanização e voluntariado: um estudo em hospitais da Coordenadoria de Serviços de Saúde, da Secretaria de Estado da Saúde de São Paulo" (NOGUEIRA-MARTINS et. al, 2009; 2010).

A partir de recortes desta pesquisa, discute-se questões éticas no âmbito da privacidade e confidencialidade que requerem reflexão crítica sobre a relação entre voluntários que atuam em contato com pacientes, familiares e cuidadores. Trata-se de questões éticas no âmbito das relações de cuidado exercidas por voluntários a pacientes/usuários, familiares e cuidadores na ambiência de serviços de saúde.

Natureza das informações compartilhadas entre pacientes e voluntários

É da natureza das informações clínicas fornecidas na anamnese, história clínica e da evolução dos pacientes que sejam relatadas, entrelaçadas na confiança e sigilo profissional das informações. Entretanto, esta informação pode ser compartilhada por necessidade do paciente com vá-

rios outros profissionais que interagem entre si e entre os colaboradores que atuam na relação de cuidado (ALIU et. al, 2014).

Os dados fornecidos e colhidos nesse âmbito são sensíveis e a manipulação desses pode significar benefícios indevidos, tal como a venda de banco de dados para a indústria farmacêutica e uso de informação para campanhas promocionais (BRENT, 2005).

O respeito à privacidade é valor central da moral comum anglo-americana. O modelo da lei de privacidade na saúde estadunidense considera que as informações de saúde identificável são dignas de tutela jurídica. A "Lei Modelo" aplica-se a todas as "informações de saúde protegidas", por agências de saúde pública. Estas informações, sejam orais, escritas, eletrônicas, ou visuais, relacionam-se com o passado de um indivíduo, presente ou futuro estatuto de saúde física ou mental, condição, tratamento, serviço, compras de produtos ou prestação de cuidados. Esta definição ampla de informações de saúde protegidas reconhece que quaisquer dados identificáveis podem ser sensíveis e necessitam de proteção (LAWRENCE, 2001).

A última década assistiu a um rápido aumento do interesse e preocupação em relação à proteção da privacidade das informações pessoais. Alguns países dispõem de legislação relacionada à privacidade, outros não (ALIU et. al, 2014; BAHATI et. al, 2010). A proteção da privacidade das informações pessoais é geralmente aceita como um direito civil fundamental. O incumprimento deste direito é mais associado a regimes opressivos e totalitários do que relacionados a sociedades democráticas as quais respeitam os direitos humanos (JACOB, 1982).

Confidencialidade de informações no âmbito dos serviços de saúde

As informações fornecidas em âmbito hospitalar são potencialmente sensíveis, nos aspectos da sua confidencialidade, sigilo e manutenção de privacidade do paciente e familiares (BHARUCHA et. al, 2015).

Na abertura da privacidade é necessário que se estabeleça um acordo de confidencialidade, um pacto. A privacidade e a confidencialidade são princípios complexos que se correlacionam entre si. A privacidade consiste

no conjunto de informações sobre uma pessoa, que pode decidir mantê-las sob seu exclusivo controle, ou comunicar, decidindo em que medida e a quem, quando, onde e em que condições o outro poderá acessar as informações. Já a confidencialidade se relaciona na garantia (no sentido de confiança) de que as informações confiadas não serão reveladas sem prévia autorização da pessoa em questão. Ou seja, a privacidade das informações é um direito dos usuários do serviço, ao mesmo tempo em que a confidencialidade é um dever dos profissionais em relação às informações geradas e confiadas no relacionamento profissional/usuário (MASSAROLLO et. al, 2006).

Petrônio et. al (2004) indicam que o desrespeito ao aspecto da confidencialidade na área da saúde é situação potencialmente arriscada sob o ponto de vista ético-legal. Em seu artigo apresenta-se como fundamental explorar não só o papel informal do advogado, mas considerar as partes do jogo do paciente e do médico neste sistema comunicativo complicado. Uma vez que todos os três membros dessa tríade forem examinados, podemos ter uma ideia melhor de como informalmente advogados, médicos e pacientes podem navegar pelo terreno complexo de limites de privacidade em torno de confidencialidade médica.

Diante de situações de doença, os princípios como o da dignidade, igualdade, confiança, lealdade, vulnerabilidade, entre outros, inclui em situações que envolvem direitos e relações privadas que podem demandar inclusão de pessoas ao serviço de saúde; entre elas, estão o advogado e voluntários de diversas áreas de atuação (PETRONIO et. al, 2004).

Em quase nenhum outro âmbito da vida humana esta questão é trazida com tanta ênfase como no caso da informação de saúde, talvez porque os dados dessa área acabem se relacionando com outros também de cunho íntimo (vida sexual) ou pelos riscos que a violação da confidencialidade pode impor à pessoa (perda de emprego, seguro de saúde ou de vida). Pacientes esperam que a informação que eles compartilham com o seu médico e no entorno hospitalar sejam respeitadas e mantidas em sigilo (FULLBROOK, 2007).

A equipe de saúde, os prestadores de serviços de cuidados, os serviços de assistência, ao ter acesso à informação, precisam manter sigilo compatível com princípios de respeito à pessoa autônoma e da privacidade (MILNES et. al, 2012; HERTZMAN et. al, 2013).

Dentre as interações no hospital está aquela entre equipes, "pacientes" e o voluntariado. O voluntariado ocorre na áreas da medicina, da enfermagem e de outras formações universitárias através da prestação de serviços em países em desenvolvimento, situações de crise e conflitos. No sistema educacional americano, a adesão ao trabalho voluntário é um dos componentes educacionais na formação de carreiras na área da social e de saúde (KORKMAZ et. al, 2009).

Não só no hospital circulam informações de saúde de caráter sigilosas, íntimas e privadas, também nos serviços de atenção básica é comum ocorrer estas trocas. No Brasil, em São Paulo, pesquisa com enfermeiros e médicos do Programa Saúde da Família (PSF) demonstra sutileza no escopo dos problemas éticos vividos na atenção básica. Aborda preocupações do cotidiano da atenção à saúde (SILVA et. al, 2006). A equipe de saúde pode encontrar dilemas éticos em vários atos. Como, por exemplo, o resultado positivo de um exame de uma gravidez indesejada, não revelada à família por pedido da mulher. Para evitar danos, tomou-se todos os cuidados para cercar a grávida de toda a assistência possível, mas o caso culminou em morte por hemorragia, causada por aborto. A família, após o óbito, procurou a unidade básica de saúde para saber o que estava acontecendo, pois encontraram o cartão de matrícula da gestante nos seus pertences (ZOBOLI, 2010). A presença de voluntários na Atenção Básica é bem menor que nos hospitais, entretanto, a comunidade, como agentes de saúde, amigos, vizinhos e parentes estão no mesmo ambiente de convivência que o usuário, ou seja, utilizam o mesmo serviço; muitas vezes, compartilham até o prontuário/família.

A disseminação das informações pessoais sobre as condições de saúde, tais como lepra, HIV, tuberculose, entre outras, pode vir carregada de estigma sobre a condição de saúde da pessoa fora do contexto dos serviços de saúde (MATSUBA et. al, 2007).

No âmbito hospitalar, relacionados à confidencialidade e à privacidade de suas informações, Kobayashi (2007) relata que:

> "A área da segurança da informação em saúde ainda é bastante incipiente, permitindo pesquisas maiores e mais aprofundadas. Em particular, praticamente não há pesquisa nesta

> área dentro do Brasil, o que a torna uma linha promissora tanto em termos acadêmicos quanto em termos de mercado".

Voluntários e profissionais em estabelecimentos de saúde têm acesso a dados pessoais de pacientes, mesmo que indiretamente (pelo fato de frequentarem este ou aquele a serviço de saúde), trazendo questões relacionadas à eficiência e à interoperabilidade de um lado, e a confidencialidade e a privacidade, do outro, na balança da segurança das informações em saúde (MASSAD et. al, 2003; BOCCHI et. al, 2010).

Aspectos legais do voluntariado e a proteção à privacidade

A questão da segurança está incluída nas preocupações das organizações internacionais de saúde. Segundo a Organização Pan-Americana de Saúde (OPAS, 1999):

> "Os Sistemas de Informações em Saúde (SIS) armazenam dados identificados sobre saúde dos indivíduos, e essas informações são muito sensíveis. Dados médicos inserem-se na esfera mais íntima do indivíduo. Conteúdo dos prontuários pode causar danos ao paciente, se for utilizado fora da relação médico-paciente. Divulgação não autorizada de dados pessoais médicos pode, portanto, levar a várias formas de discriminação, à incriminação, e até mesmo à violação de direitos fundamentais".

Segundo o Programa Voluntário do Brasil Conselho da Comunidade, lançado pelo Governo Brasileiro em 1997, "voluntário é o cidadão que, motivado pelos valores de participação e solidariedade, doa seu tempo, trabalho e talento, de maneira espontânea e não remunerada, para causas de interesse social e comunitário" (COMUNIDADE SOLIDÁRIA, 2014).

O arcabouço legal do voluntariado é fundamentado na Lei n 9.608, de fevereiro de 1998 (BRASIL, 1998), a qual dispõe sobre o serviço voluntário, e dá outras providências:

> "Art. 1: Considera-se serviço voluntário, para fins desta Lei, a atividade não remunerada, prestada por pessoa física à entidade pública de qualquer natureza ou instituição privada de fins não lucrativos, que tenha objetivos cívicos, culturais, educacionais, científicos, recreativos ou de assistência social, inclusive, mutualidade".

A legislação brasileira de 1988, Capítulo I, artigo 5º, inciso LXXII, alíneas *a* e *b*, contempla o "habeas-data", ação que garante ao interessado o acesso a informações atinentes à sua pessoa, constante de registro ou bancos de dados de entidades governamentais ou de caráter público, bem como de retificação desses dados. Intenta assegurar a proteção da informação sob sua responsabilidade, e garantir o direito dos cidadãos de acesso (confidencial e privado) às informações de seu interesse (BRASIL, 1998).

Proteção da privacidade e voluntariado em serviços de saúde

O voluntário frequenta o âmbito hospitalar e até ao lado dos leitos podem ocorrer atos de observação e/ou escuta involuntária de discussão entre equipes, familiares e cuidadores podendo ocorrer conflitos éticos a partir desta convivência. O voluntariado presente nos hospitais tem diferentes níveis de escolaridade, indo desde pessoas de origem simples, analfabetas ou mal alfabetizadas a profissionais de nível universitário ou pós-graduados. Nesta perspectiva, a literatura demonstra a necessidade de delimitar os "limites admissíveis" de exposições durante o trabalho voluntário, pois as situações podem ser nocivas ao paciente. É essencial para qualificar o trabalho voluntário na saúde, lidar com os desafios da educação técnica e clínica no desenvolvimento de atividades/habilidades diárias dos voluntários (BERLINGUER et. al, 1996).

Ramificações éticas do sigilo e da privacidade têm se preocupado em mediar inúmeros conflitos advindos do cotidiano das práticas de saúde, surgem questões para as quais normas, leis e regulamentos adminis-

trativos não fornecem todas as respostas, deixando considerável margem de liberdade para tomadas de decisão tanto do coordenador de voluntariado quanto do voluntário (CLAMERS, 2003).

Numa era digital onde existe a superexposição é de se esperar que dentre os princípios éticos que têm sofrido grande impacto neste início de milênio podem ser destacadas a privacidade e a confidencialidade das informações. Tais princípios estão relacionados à ideia de respeito à autonomia da pessoa. Ao invés de uma ética de evitar danos - uma noção paternalista de proteção, pode o voluntariado em âmbito hospitalar atuar através de uma ética do cuidado (DALY e LEWIS, 2000).

O voluntariado tem perfil variado de idade, escolaridade e situação econômica tanto no Brasil quanto no exterior, tendo como eixo comum a determinação de realizar trabalho em prol de grupo de pessoas ou de organizações voltadas para temas os mais diversos possíveis (educação, saúde sexual, envelhecimento saudável) (NOGUEIRA-MARTINS et. al, 2010).

Além de conhecer vários aspectos do paciente, o voluntariado no contato direto com o paciente, devido naturalmente à sua proximidade, terá acesso direto ou indiretamente a uma série de atributos pessoais, tais como orientação sexual, etnia, opiniões políticas e religiosas, traços de personalidade, inteligência, felicidade, uso de substâncias ilícitas, situação matrimonial e/ou separação dos pais, a idade e a identidade de gênero (CALLEJA et. al, 2011).

Sobre o acesso à informação, estudo na África subsaariana aborda os desafios de familiares na continuidade de cuidados a pacientes de Aids em domicílio. No contexto da confidencialidade, quando foi respeitado, os cuidadores foram frustrados por falta de informação, tratamento interrompido, a exclusão de suas perspectivas em cuidados médicos, bem como a falta de hospitalização segura (BAHATI et. al, 2010).

Um outro estudo revela que voluntários com pessoas em cuidados paliativos gostariam de saber mais sobre os pacientes antes que eles realmente se encontrassem pela primeira vez. A metade destes voluntários relatou que a sua coordenadora lhes forneceu as informações do paciente: apoio do paciente relacionado à organização familiar, diagnóstico/doença do paciente, idade, localização (endereço residencial ou leito hospitalar).

Os voluntários ficaram muito satisfeitos com a informação repassada - informação médica (diagnóstico do paciente) e informações de relacionamento (estado civil do paciente). Esta última informação apareceu como sendo a mais importante das informações pessoais (à frente de interesses e hobbies do paciente). Os voluntários relatam como fonte de informação o próprio paciente, seus familiares e o coordenador do voluntariado. Alguns voluntários mencionam questões de privacidade em seu trabalho, como, por exemplo, ser um voluntário em uma cidade pequena, onde as pessoas sabem o que você está fazendo, o que em certa medida pode contribuir para publicizar determinadas condições da população atendida (CLAXTON-OLDFIELD et. al, 2006).

As questões éticas de voluntários de hospitais dos Estados Unidos versam sobre o dilema de aceitar ou não presentes, a assistência ao paciente, preocupações familiares, papéis e limites, o suicídio e a antecipação da morte. Os voluntários também confrontam questões éticas na negociação de seu papel desconfortável posicionado entre profissional de saúde e amigo. Esta ambiguidade pode criar uma variedade de dilemas éticos e outros problemas não comumente vividos por outros profissionais de saúde. A literatura acadêmica sugere neste tema a necessidade de mais extensa investigação. De mais de 500 voluntários do hospital de Kentucky, 4% relataram terem sido convidados a ajudar um paciente a pôr termo à sua vida. Com meio milhão de voluntários de hospitais ativos nos Estados Unidos, esta proporção pode extrapolar a dezenas de milhares de voluntários provavelmente confrontados com pedidos para ajudar com o suicídio de um paciente hospitalar. O estudo conclui que na formação voluntária devem ser incluídas as discussões de ética (BERRY e PLANALP, 2009).

Desafios éticos vivenciados pelos voluntários nos serviços de saúde

Quatro principais tipos de desafios éticos foram identificados por voluntários canadenses de cuidados paliativos. O primeiro foi a comunicação, especialmente a respeito de quem deve saber o prognóstico de um

paciente. Como exemplo a pergunta de uma menina de 6 anos "E a minha mãe, vai morrer?".

O segundo conflito envolve situações onde os voluntários foram convidados a "tomar partido" ou opiniões sobre os cuidados e opções funerárias.

O terceiro, a confidencialidade. Um voluntário foi questionado por um estranho sobre uma pessoa que estava sendo cuidada pelo hospital e seu status.

O quarto tipo versou sobre o cuidado comprometido. O voluntário acreditava que o paciente estava sofrendo por causa da medicação inadequada. Os problemas de comunicação observados e experimentados por voluntários sugerem enfrentar questões éticas.

Outros exemplos incluídos: postura ao enfrentar perguntas do paciente se está morrendo e ao mesmo tempo respeitando a vontade da família que ela não seja dita; se ao ajudar um paciente a ir para a sua garagem (em algum risco físico e com grande dificuldade) para destruir materiais que ele fez, mas não quer que sua esposa veja, ou para escrever uma carta pelo paciente a alguém que o cuidador não aprovaria (FRY, 1984).

Voluntariado diante de situações de confidencialidade

Como lidar com o voluntário que acredita que o paciente foi excessivamente medicado? E como lidar com questões de moralidade de uma paciente sobre uma gravidez antes de seu casamento? Os voluntários de hospitais têm de treinar as habilidades de escuta, as necessidades especiais dos moribundos, autocuidado, gestão do estresse, o cuidado espiritual, cuidando do (s) cuidador (es), o manejo da dor da família e tristeza, todos os temas em que as questões de privacidade podem surgir. A confidencialidade ética, como seguro de vida, as restrições sobre suas próprias crenças, a confidencialidade, os pedidos de assistência, e outras questões-limites (CLAXTON-OLDFIELD et. al, 2006).

Pesquisa americana ilustra o ambíguo papel de voluntários e os problemas que os acompanham. Para profissionais provavelmente não

são oferecidos presentes. Amigos provavelmente não recusam recebê-los, mas os voluntários são colocados na incômoda posição de não serem nenhum dos dois. Verificou-se que foi comum para os voluntários chamar seus coordenadores para saber como lidar com esta questão. O tema do cuidado e da família relacionado às questões do paciente também reflete a ambiguidade dos papéis. Os voluntários têm condições de observar o cuidado dos pacientes, mas não são cuidadores, seja profissional, seja familiar. Voluntários frequentemente relataram tentativa de intervir indiretamente através de outros membros da equipe de cuidados paliativos ou a família, mas de vez em quando relatam tomar o assunto em suas próprias mãos (BERRY e PLANALP, 2009).

Ao voluntário é solicitado a permanecer por mais horas com o paciente/cliente (como se poderia pedir de um amigo), mas não de um profissional. Relatos de voluntários expressam entendimento das diretrizes de cuidados paliativos para a distribuição de medicamentos. Entretanto, estavam angustiados por ter que assistir o paciente sofrer. Os voluntários relataram que geralmente mantinham suas funções circunscritas às diretrizes do hospital, mas na ocasião de fim de vida fizeram o que o paciente ou a família queriam. Os voluntários relataram pedidos de suicídio assistido, mas não aparecia angústia sobre esses pedidos; ao contrário, eles reconheceram claramente que isto era além de suas funções como voluntários de cuidados paliativos. Ao responder perguntas que abordam suas ações, os voluntários indicaram que iriam chamar o coordenador do voluntariado, outros funcionários da equipe de cuidados paliativos (enfermeira, assistente social e capelão), ou a família. É um dilema revelar desejo de morte, suicídio ou eutanásia à família. Os voluntários, em sua maioria, referiam que, além de pedirem ajuda ou conselho, eles "apenas ouviram" (CLAXTON-OLDFIELD et. al, 2006).

Os voluntários tendem a utilizar os seus próprios juízos éticos. Por exemplo, se reconhecem o suicídio assistido como ato que atenta contra a moral e a ética, não o encorajam ou o assistem (CLAXTON-OLDFIELD et. al, 2006).

As sugestões para lidar com a ética, privacidade e confidencialidade do voluntariado foram: incluir as questões éticas no treinamento inicial de forma eficaz; sugerir acompanhamento em grupos por vários

meses de experiência; uso de cenários simulados para que os voluntários pudessem discutir e trabalhar com preocupações éticas em situações específicas (ROTOLO et. al, 2014).

Estudos anteriores revelam preocupação dos voluntários para cuidados inadequados enquanto voluntários. Estavam preocupados com cuidados desnecessários que podiam ter causado sofrimento aos pacientes. O dilema de aceitar um presente e violar as regras do hospital, ou recusar e ofender o doador. Se fossem amigos, eles poderiam ter aceitado o presente; se profissionais, não poderiam ter sido oferecidos. Além disso, as violações de limites, como pedir aos voluntários para ficarem mais tempo tratando-os como amigos ou pedindo-lhes para administrar a medicação necessária tratando-os como profissionais. Há várias implicações para educar e apoiar os voluntários na orientação e de forma contínua ao longo da sua experiência de voluntariado (AUSTAD et. al, 1998).

Dilemas éticos vivenciados por voluntários em serviços de saúde

Identificaram-se diversas situações ou dilemas éticos vivenciados por voluntários na área da saúde que sugerem a urgente necessidade de capacitação do voluntário em questões de ética e respeito à privacidade dos pacientes e seus familiares.

É importante preparar e apoiar os voluntários na abordagem de questões éticas em seu valioso trabalho à saúde. No treinamento oferecido ao voluntariado, quando iniciam sua atuação, convém apresentar a ambiguidade que viverão nesse papel: "*não muito cuidador profissional de saúde*" e "*não é bem amigo*". Há consequências práticas destas questões pertinentes ao âmbito do trabalho voluntário intra e extra-hospitalar.

O atendimento dos voluntários aos pacientes potencialmente incorre em acesso a informações pessoais, privadas, de cunho íntimo, que têm de ser respeitadas com sigilo e confidencialidade.

Os principais desafios propostos seria otimizar uma revisão da jurisprudência internacional que explora os princípios jurídicos fundamentais que sustentam a confidencialidade, o paciente e o voluntariado.

Esta revisão das orientações poderia concentrar documentação regulamentar voluntária que deveria ser encontrada com facilidade perante a temática apresentada.

Reforçar as razões subjacentes da diretriz do serviço de saúde relacionadas à aceitação de presentes, à não intervenção em assistência médica, enfermagem, circunscrevendo o papel voluntário às funções que lhes são circunscritas pelos serviços em seus regulamentos.

Normas relacionadas à aceitação de presentes, que deveriam estar expostas em cada instituição e a diretriz circunscrita ao papel voluntário dos que ali exercem suas atividades.

Considerações finais

Na discussão foram apontados conflitos de privacidade e sigilo relacionados a diferentes aspectos: terminalidade, desejo de morte, condutas a respeito de aceitar presentes, tratamentos e critérios medicamentosos, critérios de conduta profissional, interferência familiar, respeito às necessidades do paciente.

O conflito entre ser amigo e confidente de situações íntimas (estado gestacional, doença), demanda familiar (para revelação de estado de saúde), segredos do paciente (demanda por cumplicidade na realização de tarefas e desejos de cunho pessoal, polifarmácia e abuso de fármacos).

Outro tema recorrente apresentado foi aceitar ou não presentes, que é um dilema quando o serviço de saúde não tem uma conduta estabelecida para o voluntário(a). No mesmo mote, discutir melhor a relação comercial e a relação afetiva, principalmente em cuidados paliativos.

As pesquisas sugerem que voluntários de hospitais e serviços de saúde em geral são comumente confrontados com problemas éticos, mas pouco se sabe sobre a natureza dessas situações ou como são manejadas pelos voluntários, serviços, familiares e pacientes. As virtudes da compaixão, da empatia, fidelidade, justiça, solidariedade, cidadania, proteção, defesa e sabedoria prática podem servir como base para a tomada de decisão do voluntariado em situações eticamente problemáticas.

Todas as questões e proposições acima expostas prestam-se a ser consideradas na atuação dos conselhos de saúde, na sociedade civil, em representações de entidades de classe, trabalhadores de saúde, no Estado, em órgãos oficiais deliberativos criados por Lei e pertencentes à estrutura do poder Executivo, na gestão das instituições e sistemas de saúde.

Como sugestões gostaríamos de propor:

- A criação de grupos de estudos de questões pertinentes ao trabalho voluntário entre diferentes segmentos da sociedade.
- Vivência do relacionamento voluntariado-cliente-hospital durante o treinamento do voluntário. Em sua formação para o trabalho voluntário, utilizar cenários típicos que os voluntários possam encontrar e opções para lidar com eles.

Os princípios de confidencialidade são de suma importância. Regras, protocolos e diretrizes precisam ser formuladas e quiçá órgãos reguladores, códigos de conduta dos voluntários. O sigilo deve ser colocado como item da maior importância, especialmente na arena da prestação de cuidados de saúde.

Referências

ALIU, O.; CORLEW, S. D.; HEILES, M. E. et al.. Building Surgical Capacity in low-Resource Countries. A qualitative analysis of task shifting from surgeon volunteers´perspectives. **Annals of plastic surgery,** v.72, n.1, p.108-12, jan.2014.

AUSTAD, C. S.; HUNTER, R. D. A.; MORGAN, T. C. Managed health care, ethics, and psychoterapy. **Clinical Psychology-Science and Practice,** v.5, n.1, p.67-76, 1998.

BAHATI, P. N.; KIDEGA, W.; OGUTU, H. et al. Ensuring quality of services in HIV prevention research settings: findings from a multi-center quality improvement pilot in East Africa. **Aids Care,** v.22, n.1, p.119-25, jan.2010.

BHARUCHA, T.; TRAIANOU, A.; KENIGER, M. et al.. Volunteering to improve health worldwide. Current trends in Out of Programme Experience/Training in the UK 2014. **Journal of Epidemiolog and Global Health**, 2015. [No prelo].

BERLINGUER, G.; FALZI, G.; FIGA-TALAMANCA, I. Ethical problems in the relationship between health and work. **International Journal of Health Services,** v.26, n.1, p.147-71, 1996.

BERRY, P.; PLANALP, S. Ethical issues for hospice volunteers. **Am J Hosp Palliat Care,** v.25, n.6, p.458-62, 2009.

BRASIL. Lei nº 9.608/98, 19 de fevereiro, 1998. Dispõe sobre o serviço voluntário, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9608.htm>.

BRENT, N. J. The Use and Misuse of Electronic Patient Data. **Journal of Infusion Nursing,** v.28, n.4, p.251-58, 2005.

BOCCHI, S. C. M.; ANDRADE, J.; JULIANI, C. M. C. M. et al. Entre o fortalecimento e o declínio do vínculo voluntário-idoso dependente em um Centro-Dia. **Esc. Anna Nery,** v.14, n.4, p.757-764, 2010.

CALLEJA, P.; FORREST, L. Improving patient privacy and confidentiality in one regional Emergency Department: a quality project. **Australasian Emergency Nursing Journal,** v.14, n.4, p. 251-256, 2011.

CIVICUS: World Alliance for Citizen Participation, International Association for Volunteer Effort (IAVE) & United Nations Volunteers (UNV). 2006. Partnership pledges to promote volunteer´s role in social activism. Disponível em: <http:www.worldvolunteerweb.org.br.org/browse/sectors/activism/doc/partnershippledges-to-promote.html>. Acesso em: 5 dez 2014.

CLAMERS, J. Patient privacy and confidentiality. **BMJ,** n.5, p.326, 2003.

CLAXTON-OLDFIELD, S.; MACDONALD, J. B. S.; CLAXTON-OLDFIELD, J. What Palliative Care Volunteers Would Like to Know About the Patients They Are Being Asked to Support. **American Journal Hospital Palliative Care,** n.23, p.192-96, 2006.

COMUNIDADE SOLIDÁRIA. Programa Voluntários do Conselho da Comunidade Solidária. Disponível em: <http://portaldovoluntario.org.br/blogs/54329/posts/146>. Acesso em: fev. 2014.

COREY, G.; COREY, M. S.; CALLANAN, P. **Issues and ethics in the helping professions.** 6.ed. Pacif Grove, California: Brooks/ColeKuhse , 1998.

DALY, M.; LEWIS, J. The concept of social care and the analysis of contemporary welfare states. **Br. J. Sociol.,** v.51, n.2, p.281-98, 2000.

FRY, S. T. Confidentiality in health care: a decrepit concept? **Nursing Economic**, v.2, n.6, p. 413-8, nov/dez. 1984.

FULLBROOK, S. Legal principles of confidentiality and other public interests. **British Journal of Nursing,** v. 6, n.14, p. 874-75, 2007.

GRIEP, Y.; HYDE, M.; VANTILBORGJ, T. et al.. Voluntary work and the relationship with unemployment, health, and well-being: A two-year follow--up study contrasting a materialistic and psychosocial pathway perspective. **Journal of Occupational Health Psychology**, v. 20, n.2, p.190-204. 2015.

JACOB, J. M. Confidentiality – the dangers of anything weaker than the meedical ethic – commentary. **Journal of Medical Ethic**, v.8, n.1, p.18-21, 1982.

HERTZMAN, C. P.; MEAGHER, N.; MCGRAIL, K. M. Privacy by Designat Population Data Base: a case study scribing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. **J. Am. Med. Assoc. Informe,** v. 20, n. 1, p. 25-28, jan.2013.

KISNERMAN, N. **Introdução ao trabalho social**. São Paulo: Moraes; 1983.

KORKMAZ, F.; ERDIL, F. Ethical problems observed by student nurses. **Nursing Ethics,**v.16, n.5, p. 589-98, 2009.

KOBAYASHI, L.O.M.; FURIE, S.S. Segurança em informações médicas: visão introdutória e panorama atual. **Revista Brasileira de Engenharia Biomédica**. v.23, n. 1, p. 53-77, 2007.

LAWRENCE, O.; GOSTIN, L. O.; HODGE JR., J. G. et al. Informational privacy and the public's health: the model state public health privacy act. **Am. J. Public Health**. v. 91, n.9, p.1386-92, set. 2001.

MARQUES, V.L. Voluntariado: motivos e repercussões na vida social e acadêmica dos alunos de graduação de medicina, voluntários em programas na área da saúde. 2006. (Dissertação de Mestrado) – Escola Paulista de Medicina, Universidade Federal de São Paulo. São Paulo, 2006.

MATSUBA, M. K.; HART, S.; ATKINS, R. Psychological and social-structural on commiteng. **Journal of Research of Personality**, v. 41, p. 889-907, 2007.

MASSAD, E.; MARIN, H.F.; AZEVEDO, N.R. **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico**. São Paulo; FMUSP/UNIFESP/OPAS, 2003.

MASSAROLLO, M.K.B., et al. Autonomia, privacidade e confidencialidade. In: OGUISSO, T.; ZOBOLI E. L.C.P. (Org.). **Ética e bioética**: desafios para a enfermagem e a saúde. São Paulo: Manolle, 2006. p.136-152.

MERHY, E.E. Um ensaio sobre o médico e suas valises tecnológicas: contribuições para compreender as reestruturações produtivas do setor saúde. **Interface: Comunicação, Saúde, Educação.** v.6, p.109-16, 1997.

MILNES, L.; KENDAL, S. Ethical challenges of conducting health research in UK school setting. **British Journal of Nursing,** v.21, n.5, p.294-48, 2012.

NOGUEIRA-MARTINS, M.C.F.; BERSUSA, A.P.S.; SIQUEIRA, S.R. Características sociodemográficas dos voluntários de hospitais públicos estaduais. **Boletim Epidemiológico Paulista,** v.70, p. 13-9, 2009.

NOGUEIRA-MARTINS, M.C.F.; BERSUSA, A.P.S.; SIQUEIRA, S.R. Humanização e voluntariado: estudo qualitativo em hospitais públicos. **Rev. Saúde Pública,** São Paulo. v. 44, n.5, p. 942-49, 2010a.

NOGUEIRA-MARTINS, M.C.F.; BERSUSA, A.P.S.; SIQUEIRA, S.R. Voluntariado nos Hospitais Públicos Estaduais: o papel do Coordenador de Voluntários. **Revista Prática Hospitalar**, v.68, p.114-77, 2010b.

ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE (OPAS). **Cyberspace law and ethics**: a health sector perspective. Washington, D.C: OPAS, 1999.

PETRONIO, S.I.; SARGENT, J.; ANDEA, L. et al.. Family and friends as healthcare advocates: Dilemmas of confidentiality and privacy. **Journal of Social and Personal Relationships,** v.21, n.1, p. 33–52, 2004.

PORTAL DO VOLUNTÁRIO. Disponível em: <http://portaldovoluntario.org.br/documents/0000/0118/121450315821.doc>. Acesso em: maio 2014.

ROTOLO, T.; WILSON, J. Social heterogeneity and volunteering in U.S. Cities. **Sociological Forum,** v.29, n.2, p.429-52, 2014.

SILVA, L.T.; ZOBOLI, E.L.C.P.; BORGES, A.L.V. Bioética e atenção básica: um estudo exploratório dos problemas éticos vividos por enfermeiro e médicos no PSF. **Cogitare Enfermagem**, v.11, n.2, p. 133-42, mai/ago.2006.

SIQUEIRA, U. Entre sindicatos, clubes e botequins: identidades, associações e lazer dos trabalhadores paulistanos (1890-1920). 2008. Tese Universidade Estadual de Campinas. Campinas, 2008.

SELLI, L.; GARRAFA, V.; JUNGES, J. R. Beneficiários do trabalho voluntário: uma leitura a partir da bioética. **Revista de Saúde Pública,** v.42, n. 6, p.1085-9, 2008.

SOUZA, L. M.; LAUTERT, L.; HILLESHEIN, E. F. Trabalho voluntário, características demográficas, socioeconômicas e autopercepção da saúde de idosos de Porto Alegre. **Rev. Esc. Enferm.,** v.44, n.3 p.561-9, 2010.

THOMPSON, A.A.; TORO, O.L. El voluntariado social em America Latina: tendências, influencias, espacios, y leciones aprendidas. Disponível em: <http://new.lasociedadcivil.org/docs/ciberteca/thompsontoro_copy4.pdf>.

ZOBOLI, E. L. C. P. Deliberação: leque de possibilidades para compreender os conflitos de valores na prática clínica da atenção básica. 2010. Tese (Livre Docência) - Escola de Enfermagem. Universidade de São Paulo. São Paulo, 2010.

19

Arquivos de prontuários e a preservação das informações privadas dos usuários de serviço de saúde

Teresa Cristina Gioia Schimidt[1]
Antonio Victor Rodrigues Botão[2]

Introdução

Os arquivos existem desde os tempos mais remotos de nossa história e surgiram com a finalidade de guardar os documentos considerados fontes de provas de atos administrativos, jurídicos, históricos e culturais, como também fontes de registro dos direitos e deveres dos cidadãos.

As mudanças tecnológicas no campo da informação em saúde no país e no mundo, ainda que defasadas em relação a outros campos, repercutem na forma de registrar, armazenar, preservar e tratar os arquivos com as informações de saúde dos prontuários, de forma a que seja preservada a privacidade e garantida sua disponibilidade de forma oportuna e precisa.

A importância do registro em saúde teve seu início na prática clínica, na qual os profissionais de saúde identificaram a necessidade de recorrer à história clínica e evolutiva para acompanhamento dos problemas de saúde que acometiam os pacientes. Os registros são estratégicos para a

1 Teresa Cristina Gioia Schimidt (tschimidt@saude.sp.gov.br) é Enfermeira, Doutora em Ciências pela USP, atua na Secretaria de Estado da Saúde de São Paulo junto ao Gabinete do Secretário.
2 Antonio Victor Rodrigues Botão é Arquivista, Mestre em Ciência da Informação IBICT/UFRJ e Professor Assistente na área de Gestão Documental do Curso de Biblioteconomia e Gestão de Unidade de Informação da UFRJ.

decisão clínica e gerencial e para o apoio à pesquisa e formação profissional, e na atualidade são considerados como um dos critérios de avaliação da qualidade da prestação de serviço de saúde, ou seja, a qualidade dos registros efetuados é reflexo da qualidade da assistência prestada, sendo ponto-chave para informar acerca do processo de trabalho e de condutas terapêuticas. O prontuário é o documento no qual se deposita o conjunto de dados sobre o paciente e sobre seu processo de atendimento, um documento que é utilizado por todos os profissionais envolvidos no atendimento. O prontuário é do paciente e as informações registradas nesse documento devem obedecer a uma norma, assim também a sua guarda com segurança, as formas de requisitá-lo e os limites de circulação desse documento dentro dos serviços (VASCONCELOS et al,2008).

Os registros técnicos e administrativos oriundos da assistência nos serviços de saúde são importantes e utilizados para pagamentos da assistência à saúde prestada ao paciente, e a análise dos prontuários tem sido uma estratégia aplicada para garantir justa cobrança. Além disso, é um instrumento que pode e deve ser consultado em situações que envolvam aspectos legais e/ou éticos, científicos, educacionais e da qualidade do cuidado (MOTTA,2003).

Como forma de garantir a continuidade e a segurança do diagnóstico e da terapêutica proposta, o registro deve ser realizado em impressos devidamente identificados com dados do paciente, data e horários específicos, ser claro e objetivo, com identificação do autor feita de forma legível e sem rasuras, favorecendo o uso dos elementos administrativos e clínicos, inclusive os ligados à auditoria.

Interessante citar que os profissionais diretamente envolvidos na prestação do cuidado e na gestão, tais como pesquisadores, docentes, alunos do campo da saúde e o próprio paciente, são usuários dos registros de saúde, devendo estes serem preenchidos e organizados de forma a permitir sua localização, leitura e identificação de autoria e, ainda, serem completos, acurados, objetivos e concisos.

Apesar das considerações sobre a importância dos aspectos legais e assistenciais, com muita frequência os registros não contêm todas as informações necessárias que atendam aos requisitos ético-legais relativos ao processo de trabalho dos profissionais de saúde que prestam assistência direta ao usuário, nem da instituição. Acrescenta-se o desconheci-

mento sobre os aspectos arquivistas que merecem a devida atenção e que constituem o principal foco deste capítulo.

Origem e evolução dos arquivos nos serviços de saúde

Com relação aos aspectos históricos dos registros em saúde, os mesmos estão relacionados à história da medicina, na qual os registros podem ser formais (escritos) ou informais, com o uso de símbolos. A cronologia dos registros médicos é dividida da seguinte forma (EPSJV, 2005):

- **Medicina primitiva** – com origem na pré-história, onde se verifica práticas de trepanação, que consiste na abertura do crânio para libertar os espíritos;
- **Medicina na antiguidade** – com indícios no **Egito** que, por intermédio de Ilhote, preconizava o registro de informações considerando os seguintes elementos: título, diagnóstico provisório, exame físico, lista de sintomas, diagnóstico definitivo, prognóstico e tratamento. Na **Mesopotâmia**, o Código de Hamurábi instituía o conceito legal dos registros médicos e incluía leis civis e religiosas, definia princípios para o exercício legal da medicina apresentando conceitos de boa e má prática médica e regras de olho por olho e dente por dente. Havia estudo de sintomas, dietas, receitas e repouso e usavam-se plantas medicinais, vegetais e minerais, que hoje são as bases da farmacologia moderna. As primeiras foram escritas em tábua de barro. Na **Grécia**, os registros tinham fundamentos baseados na mitologia e surgia nesse momento o Esculápio, que é a história dos pacientes escrita nas paredes dos templos, considerando como dados o nome, breve resumo do caso e resultado. Porém, não se tinha a ideia de continuidade do tratamento. Através de Hipócrates, surgem os princípios da medicina científica, que separou o mistério da magia, liberando os deuses das responsabilidades da prevenção e do tratamento das doenças, e coloca o encargo nas mãos dos homens, afirmando que as doenças

tinham uma causa natural. Em **Roma**, Galeno adota pioneiramente os princípios de higiene e levava estudantes para fazer observação. Os hebreus possuíam técnicas de prevenção das doenças, considerando importantes as práticas de higiene, e instituíram a sistematização do primeiro código de higiene e circuncisão (postectomia). Na **Índia**, o livro Susruta era o referencial em registros de saúde, no qual se verificava a utilização de instrumentos cirúrgicos, bem como determinavam o número de refeições e a quantidade de água a ser consumida em tratamento de saúde. Na **China,** a filosofia do yin/yang considerava a saúde como resultado de equilíbrio. A ingestão de água era fundamental, e havia a prática da acupuntura e a utilização de produtos de origem animal, vegetal e mineral;

- **Medicina da Idade Média** – com a queda do Império Romano, a medicina volta a ser mistério, mas no Oriente Médio as práticas continuavam a se desenvolver;
- **Medicina na Idade Moderna** – começam a surgir hospitais, que tinham finalidade religiosa e de proteção, e não de tratamento. Os doentes eram geralmente anciãos e pobres. No Hospital São Bartolomeu (Inglaterra), instituiu-se no contrato dos médicos o que lhes cabia prescrever aos pacientes.

A Renascença representou o período no qual se desenvolveram a anatomia e a fisiologia, além de técnicas cirúrgicas. Nesse período ocorre a descoberta de novas drogas e novos estudos sobre a causa das doenças. Todavia, a dissecação era proibida e continuava-se utilizando animais para tal.

No período compreendido entre os séculos XVI e XX, a anatomia se moderniza e tem-se a dissecação de cadáveres. Há o desenvolvimento da clínica farmacêutica, que se pautava na idade, sexo e peso, constatação de inter-relações entre coração, pulso e sangue. Há, ainda, o surgimento da histologia e a utilização do microscópio, os estudos estatísticos em saúde, a medicina preventiva, as vacinas, os anestésicos, os serviços de enfermagem, bem como o desenvolvimento dos procedimentos de registros em saúde.

Os três últimos séculos referentes ao período mencionado anteriormente representam importantes descobertas e avanços para a área

de saúde, quando a área de registros de saúde tem contribuições importantes, especificamente no século XVIII, como a descoberta de Benjamin Franklin, primeiro secretário do Hospital Pensilvânia, que institui o preenchimento dos primeiros prontuários. O Hospital de Nova York, aberto em 1771, continha em seu primeiro registro o diagnóstico, idade, data de admissão, ocupação e aparência do paciente, notas de evolução e tratamento realizado. No século XIX, há a organização do primeiro departamento de registros médicos, contendo um arquivo completo de todos os prontuários de forma catalogada. O Hospital Geral de Massachusetts, inaugurado em 1821, organizou em 1877 o primeiro SAME (Serviço de Atendimento Médico e Estatística). O século XX consolidou-se como o período das grandes mudanças e descobertas, época em que surgiram os computadores, elevando a capacidade de processamento e facilitando a obtenção de dados mais selecionados e reais, bem como o uso de novas tecnologias que começam a ser utilizadas, sendo empregados programas de avaliação e auditoria médica para melhorar a qualidade da assistência (EPSJV, 2005).

Arquivos como órgãos de apoio à administração das instituições

Além de se constituir em um direito à informação, que é inerente a todo cidadão, os arquivos tiveram sua evolução pautada no atendimento às necessidades informacionais a partir de exigências advindas do campo da administração, na organização das instituições públicas e privadas e das tecnologias de informação e comunicação.

Cabe ressaltar que o setor de arquivo constitui uma unidade administrativa primordial para a realização das atividades das organizações, pela produção documental, as quais consideram o documento arquivístico como ferramenta de testemunho e autenticidade dos registros de atos da administração e formalização de suas atividades específicas, e sua importância como centro vital de informação e veículo de comunicação, pois serve à garantia e ao resgate de direitos e de apoio à tomada de decisões estratégicas para as organizações.

A finalidade primordial dos arquivos, inerente à sua criação, é de caráter funcional, ou seja, atender às necessidades da administração de órgãos públicos e privados, assim como à vida privada das pessoas, conforme o disposto na Lei 8.159, de 8 de janeiro de 1991, conhecida como Lei de Arquivo e oportunamente aqui abreviada como LARQ:

> *"Art. 2º - Consideram-se arquivos, para os fins desta Lei, os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos".* (BRASIL,1991)

Não obstante a estas considerações, destacamos que a finalidade histórica e cultural dos arquivos fica condicionada secundariamente à atividade de avaliação documental implementada pelas práticas de gestão documental; contudo, tanto pelo uso administrativo-jurídico quanto pelo uso histórico-documental, a responsabilidade dos arquivos consiste em guardar e conservar documentos para prover a recuperação e o acesso às informações contidas neles, conforme será elucidado a seguir.

Arquivos e a dicotomia entre acesso à informação pública e privada

O acesso à informação é um direito fundamental garantido pela Constituição Federal do Brasil (BRASIL,1990) e coincide com a atribuição dos arquivos, que organizam, armazenam, e conservam os documentos para tal propósito, porém há diretrizes que condicionam o acesso, desde a liberação irrestrita, aos casos de restrição ou sigilo em virtude do teor documental.

Há que se distinguir, primeiramente, duas situações: a forma de elucidar melhor as práticas da área arquivística, que é a classificação dos arquivos e a classificação dos documentos, nas quais temos que na primeira situação os arquivos são classificados quanto ao acesso como franqueado, o qual consiste na liberação de acesso ao público em geral às instituições arquivísticas e o de uso restrito, que restringe o acesso aos funcionários da instituição, pois esta documentação ainda não adquiriu uma conotação

que enseje o acesso ao público em geral como nos franqueados, pois ainda são utilizadas sob caráter administrativo-jurídico, servindo aos propósitos organizacionais, apenas, e são confidenciais, onde os documentos apresentam caráter sigiloso em virtude de seu teor, e cuja divulgação indevida representaria risco à segurança da sociedade e do Estado.

A segunda situação contextualiza que os documentos são classificados quanto à natureza do assunto, a qual os classifica como ostensivos, que são aqueles cuja divulgação não representa risco à administração da instituição pública ou à segurança da sociedade e do Estado; e os sigilosos, que apresentam três classificações: reservado, secreto e ultrassecreto, conforme a vigência da Lei 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação, também conhecida como LAI (BRASIL, 2011).

Com relação ao dispositivo legal mencionado anteriormente, o mesmo rege a questão do acesso às informações no país e estabelece diretrizes que liberam ou restringem as condições de acesso aos documentos, assim como prevê sanções para o descumprimento do disposto em seu conteúdo. A LAI, em suas disposições gerais, determina quem está subordinado ao regime de acesso às informações conforme descrito a seguir:

> Art. 1º: Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Os artigos 1º e 2º definem os órgãos públicos e privados; autarquias, fundações e entidades filantrópicas estão incluídas entre as que devem observar as regras de acesso à informação.

A partir do exposto, percebe-se que a questão do acesso às informações no Brasil têm diretrizes estabelecidas tanto para as informações públicas contidas nos documentos armazenados em arquivos públicos, quanto para as informações privadas armazenadas nos mesmos; e os procedimentos previstos na LAI destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes, conforme o artigo 3º:

> I - observância da publicidade como preceito geral e do sigilo como exceção;
> II - divulgação de informações de interesse público, independentemente de solicitações;
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

Verifica-se, a partir das diretrizes inerentes ao acesso às informações públicas, que elas constituem um direito de qualquer cidadão em nosso país, mantendo apenas as ressalvas, conforme o artigo 4º da LARQ:

> *Todas as pessoas possuem o direito de receber dos órgãos públicos informações que sejam do interesse particular ou coletivo, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob a pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.* (BRASIL,1991)

Com relação à questão das informações que se enquadram como privadas, há acordo com a LAI, na seção V, denominada Das Informações Pessoais, a qual estabelece que deve haver transparência no trato de informações privadas, respeito à intimidade das pessoas, sua honra e imagem, bem como às liberdades e garantias individuais. Dentro desse escopo estabelece a restrição de acesso pelo prazo de 100 anos a contar de sua produção, e o acesso a essas informações deverá ser feito por agentes públicos legalmente autorizados e a pessoas que a elas se referirem. A divulgação dessas informações será mediante consentimento expresso da própria pessoa a que se refere a informação. Sobre informações médicas, essas são particularmente sensíveis e exigem um trato mais específico. Nessa categoria estão os registros relativos à prevenção e diagnóstico mé-

dico e quando a pessoa estiver física ou legalmente incapaz. São utilizadas única e exclusivamente para o tratamento médico, pesquisas, ordem judicial, defesa de direitos humanos e proteção de interesse público.

O artigo 5º da LAI determina que "*é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão*". Nesta situação enquadram-se os arquivos de prontuários médicos e os aspectos relacionados a estes, que serão abordados a seguir a partir da sua origem, considerando seus aspectos evolutivos ao longo dos anos no Brasil no que tange às informações de caráter privado dos usuários de serviço de saúde.

Registros de Saúde: SAME e SRIS

De maneira geral, os setores encarregados dos Registros em Saúde estão estruturados em setores de Registro, Arquivo e Estatística. Os aspectos organizacionais dos registros de saúde são caracterizados a partir dos serviços de coleta e armazenamento de informações médicas, que convergem nos setores SAME e SRIS, a saber:

- **SAME** (Serviço de Atendimento Médico e Estatística) é o setor que tem entre seus objetivos principais**:** contribuir para a prestação de melhor assistência possível ao paciente, assegurando que seu prontuário único seja exato, confidencial e acessível; proporcionar à direção da unidade de saúde informações fidedignas e apropriadas para a determinação de necessidades; prover níveis hierárquicos superiores com indicadores de saúde necessários para a gerência e planejamento; providenciar os prontuários e outros registros para estudos e pesquisas; zelar pela proteção aos interesses legais do paciente, da instituição e do corpo clínico e técnico.
- **SRIS** (Serviço de Registro de Informação em Saúde), tem as seguintes funções: realizar procedimentos administrativos relacionados com a matrícula e admissão de pacientes; arquivar,

recuperar e conservar os prontuários dos pacientes; manter o fichário-índice de pacientes e outros registros secundários básicos; coletar, processar e divulgar dados estatísticos sobre a produção de serviços; elaborar indicadores de saúde necessários ao estabelecimento e aos respectivos níveis centrais; fornecer certificados sobre o tratamento prestado aos pacientes; colaborar com o corpo clínico, facilitando o acesso aos prontuários e dados estatísticos para fins de avaliação, ensino e pesquisa.

O SRIS é dividido em**:**

- **Registro/matrícula** - consiste no registro dos pacientes, abertura de prontuário e construção de fichário-índice;
- **Arquivo médico** - responsável pela movimentação, controle e conservação dos prontuários, bem como anexação de laudos de exames complementares e preparação de certidões para pacientes;
- **Estatística/informações** – competência na coleta de dados, processamento e divulgação de informações referentes à produção dos serviços de saúde e pela elaboração dos indicadores de morbimortalidade da população assistida.

Os serviços de saúde comumente apresentam problemas ligados à escassez de recursos humanos ou mesmo à inexistência de profissionais adequadamente qualificados. Além disso, os recursos materiais nem sempre são de boa qualidade, e os espaços físicos são insuficientes. Há dificuldades gerenciais, como a duplicidade de números de registro, métodos inadequados de arquivamento, falha no controle da movimentação e, ainda, indefinição sobre o sistema de informações, ausência de padronização de formulários e duplicidade de dados.

A estrutura organizacional e a administração do SRIS são baseadas em suas funções, conforme exposto anteriormente. A interface com os serviços assistenciais dá-se pela atualização com os termos e expressões da área de registro em saúde, em alinhamento com o Sistema Único de Saúde – SUS, incluindo definições, normas gerais para emergência, internação e serviços de laboratório. Acrescenta-se, ainda, a articulação com

as atividades dos setores de serviço social, nutrição, farmácia, triagem, ambulatório, admissão e alta, emergência, complementares de diagnósticos e exames especiais, comissão de prontuários e serviços gerais.

O planejamento das atividades e recursos das unidades básicas de saúde – ambulatório, internação e emergência – é baseado no SRIS a partir de seus fluxos, que são os caminhos dos usuários do sistema de saúde da referência, ou seja:

- O encaminhamento de um estabelecimento a outro;
- Da contrarreferência, que consiste no retorno do paciente após a resolução da causa pela referência;
- Do fluxo do prontuário, que em caso de encaminhamento ao ambulatório deve retornar ao SRIS no mesmo dia, sendo que, no caso de ausência de prontuário, a orientação é procurar o responsável pela devolução, do estabelecimento de normas de controle e vigilância para evitar o extravio; e
- Do pessoal administrativo do ambulatório, que poderá responsabilizar-se pela coleta de dados das agendas para a realização de estatísticas e envio posterior ao SRIS e também controlar a iniciação à admissão do paciente, entrevistar o paciente e preencher os formulários básicos para internação, obter assinatura do termo de responsabilidade pelo paciente ou responsável, comunicar normas do hospital, notificar internações ou altas aos diferentes serviços, controlar internações ou altas, manter controle dos leitos e da lista de espera, e encaminhar os pacientes às unidades de internação.

A estruturação da atividade de planejamento de um SRIS deve considerar os programas e ações de saúde, o número de habitantes, as principais características do perfil demográfico, o porte da unidade de saúde, a infraestrutura e tipo de unidade de saúde, o tamanho e movimento do ambulatório e as especialidades, o tempo de arquivamento dos prontuários, as funções desempenhadas pelo pessoal. Com relação à sua posição no organograma da unidade de saúde, é subordinado à Divisão Técnica, com chefia, secretaria e setores de registro geral, arquivo médico e estatística/informações e possui as seguintes etapas de planejamento:

identificar propósitos e metas da instituição, que consistem em planos para aumentar leitos, novos serviços, centro de docência, unidade de referência; considerar objetivos como: desenvolver estatísticas, elaborar políticas e diretrizes relacionadas com as normas e procedimentos administrativos; acompanhar movimentação do paciente, atender à clientela, orientar quanto ao tipo de prontuário a ser utilizado, manter prontuários em bom estado, definir horário de funcionamento do serviço, escolher modalidade de agendamento; definir funções a serem desempenhadas; definir fluxos de trabalho; estimar o volume de trabalho anual; determinar agrupamento de funções por área de trabalho; determinar o pessoal necessário para cada atividade; definir espaço, equipamento e material; determinar relação entre áreas internas de trabalho e o SRIS; organizar áreas de trabalho e desenhar esquema de distribuição de espaços.

A localização física de um SRIS deve ser estabelecida em lugar de fácil acesso, deve ter fácil comunicação, acesso facilitado aos profissionais e distribuição, ter área prevista de 12m² para 40 mil prontuários, previsão de áreas de trabalho, de equipamento e de transporte, peso do arquivo entre 200-500 kg/m², pelo menos 4m² para cada funcionário trabalhar, ser estimada a capacidade de arquivamento para 10 anos, considerando 0,25 m² por leito em hospital-geral sem ambulatório, 0,50 m² por leito em hospital-geral com ambulatório e medida que permita arquivamento de três prontuários tamanho carta por centímetro linear em estantes fixas de cinco prateleiras com 30 cm de profundidade.

O arquivo ativo deve ser estabelecido o mais próximo possível das pessoas e setores que os utilizam: ambulatório, emergência e admissão, ou mais próximo da entrada dos pacientes e dos consultórios. Devem ser verificados fatores como temperatura, luminosidade e piso resistente, considerando-se, como parâmetro, que 1 m linear de documentos-carta pesa 37kg.

O procedimento de arquivamento deve ocorrer da esquerda para direita e de cima para baixo. As prateleiras de estantes devem estar em posição perpendicular às janelas e a organização deve ser centralizada e dividida em arquivo ativo e permanente. O ativo para os que estão recebendo atendimento ou que compareceram por um período de 5 anos após o último atendimento, são arquivados com capas individuais e numerados

conforme método adotado. No arquivo permanente são conservados os prontuários antigos com informações de valor científico e os inativados depois de 5 anos após o último atendimento; atenção deve ser dada na realização de auditoria no arquivo para sua seleção, cuidados devem ser tomados para não atribuir novo número aos prontuários e não fornecer a nenhum outro paciente o número de prontuário que tenha sido enviado ao permanente.

O arquivo permanente deve possuir recursos, como espaço necessário para as estantes e localização dos documentos, acesso restrito às pessoas autorizadas e quando não estiver em uso, permanecer trancado. O local deve ser livre de inundações, goteiras e umidade, e de roedores ou insetos, para este arquivo e para o arquivo ativo também, pois é constante a preocupação com infestação, controle de pragas. Os níveis de temperatura e umidade devem ser constantes, daí haver proibição de fazer refeições nestes locais.

Dentre os parâmetros para definição dos equipamentos, são preconizados o uso de estantes abertas com prateleiras, em média 5 a 6, com profundidade de 30 cm possibilitando arquivamento de prontuários de 32 cm facilitando a manipulação, devem ser fechadas nos fundos e nas laterais e contar com divisórias, 4 por prateleira de 90 cm; uso de carrinhos que facilitem o transporte; equipamentos para atividades estatísticas, com uso de pelo menos três tipos de fichário: fichário-índice de pacientes, nosológico e de operações, em fichários verticais com gavetas duplas.

Prontuário: definição, classificação, composição, conservação e arquivamento

O prontuário consiste no conjunto de registros dos cuidados prestados. É um documento único, que contém a história médico-social do paciente e é de acesso restrito amparado por legislação específica, com liberação apenas em casos de fornecimento de dados clínicos para pesquisa, são fontes de informação para agências reguladoras, base para pagamento de serviços prestados e servem como fontes de produção da informação como ferramenta para processo gerencial.

Podem-se identificar quatro tipos de prontuário: **tradicional**, confeccionado nas seções de identificação médica e de enfermagem; **orientado aos problemas**, com informação básica, lista de problemas, plano inicial, notas de evolução; e **integrado,** que contém episódios em ordem cronológica e especiais, que utilizam formulários especiais para casos específicos, como obstetrícia, recém-nascido, paciente com permanência de 24-48 horas, emergência e atendimento ambulatorial. Todos os prontuários devem ser ordenados cronologicamente por seções, para casos de internação/tratamento ambulatorial, ou por sistema integrado, quando se utiliza datas sucessivas.

Os prontuários, por se tratarem de um conjunto de informações relativas ao tratamento de pacientes, são compostos por formulários, sendo estes básicos e específicos. Os formulários básicos podem ser de identificação, de internação e alta, resumo da alta, anamnese e exame físico, solicitação de exames laboratoriais, radiológicos e outros, folhas de evolução e prescrições médicas, registros da Sistematização da Assistência de Enfermagem; pedidos de parecer ou de interconsulta, descrição anestésica e cirúrgica, gráfico de sinais vitais, partogama e outros padronizados conforme cada serviço. Cabe ressaltar que, por se tratarem de documentos arquivísticos, os prontuários passam por criteriosa análise e avaliação por intermédio da Comissão de Prontuários, cujos integrantes são designados pelo diretor da unidade de saúde e procedem a análise qualitativa e quantitativa com o objetivo de levantar o registro de omissões e inconsistências de informações.

Em 2002, o CFM, por meio da Resolução nº. 1.638, estabeleceu a criação das Comissões de Revisão de Prontuários nos estabelecimentos e/ou instituições de saúde onde se presta assistência médica, definindo como competências a observação dos itens que devem constar obrigatoriamente do prontuário confeccionado em qualquer suporte, eletrônico ou papel, sendo obrigatória a legibilidade da letra do profissional que atendeu o paciente, bem como a identificação dos profissionais prestadores do atendimento (CFM,2002). Neste documento, ênfase foi dada para o uso de recursos que assegurem a responsabilidade do preenchimento, guarda e manuseio dos prontuários que cabem ao médico assistente, à chefia da equipe, à chefia da Clínica e à Direção Técnica da unidade.

Com a evolução das tecnologias de informação e comunicação verifica-se, além da produção do prontuário em suporte papel, a confecção do Prontuário Eletrônico do Paciente – PEP – que possibilita a verificação de data e autor dos registros efetuados, diminui a possibilidade de alteração dos dados a níveis seguros, padroniza os dados por tipo para o uso em rede, facilita o acesso aos dados do paciente, diminui a perda de registros, padroniza registros para legibilidade e diminui espaço físico, porém pode apresentar desvantagens com relação a investimento, capacitação de profissionais e resistência por parte dos funcionários.

Algumas recomendações fazem-se necessárias ao tratamento documental dos prontuários e ao seu controle, pois são considerados únicos, sendo o de recém-nascido armazenado com o da mãe e quando ocorrer o primeiro atendimento o outro será anexado a este, a numeração é única e deve-se verificar se já não tem registro. O aspecto relativo ao controle dos prontuários preconiza que a solicitação de prontuário deve ser feita com no mínimo 24 horas de antecedência, elabora-se a ficha de substituição para indicação de empréstimo, procede-se ao controle da devolução e a realização de estatísticas para avaliar eficiência.

A conservação dos prontuários adota procedimentos de microfilmagem, processo no qual se adotam rolos de 16 mm, dos quais cada um tem dimensões de 10 x 2,5 cm e pode conter até 2.500 imagens de tamanho tipo carta, microfichas com tamanho de 15 x 10,5 cm com 192 imagens tamanho carta, proporcional quantitativamente a 5 prontuários por microficha, o que proporciona economia de espaço, acessibilidade, disponibilidade no tempo, proteção, economia de tempo na busca e recuperação das informações. O processo de digitalização também é utilizado na conservação dos prontuários e obedece a critérios legais para sua validação como prova documental, tópico que será oportunamente abordado posteriormente neste trabalho.

O arquivamento dos prontuários obedece a critérios preestabelecidos, como o sistema numérico de ordenação, que pode ser: **seriado**, no qual o paciente recebe um novo número a cada ida ao atendimento; **unitário**, com número único; e, ainda, o **seriado-unitário**, que é uma mescla dos dois anteriores, além de obedecer a métodos de numeração, que

adota números consecutivos, por data de nascimento, por documento de identidade e em ordem alfanumérica ou numeralfa.

Os métodos de arquivamento aplicáveis aos prontuários são os seguintes: alfabético, numérico, alfanumérico e cron-dalfa, que tomam por base a data de nascimento do paciente da seguinte forma: ano registrado com 4 dígitos, por décadas acrescido de 10 cores (0 a 9), sendo duas delas usadas na capa, que servem para desempate por meses. Também usam-se guias divisórias, uma para cada 50 prontuários e consideram-se como tipos de arquivos: o centralizado, que se localiza em uma unidade central; o descentralizado, localizado na unidade onde é gerado; os descentralizados controlados, que são arquivados nas unidades que prestam o serviço; e o satélite, que consiste em um arquivo central para conservar permanentemente nos arquivos até que o serviço seja concluído.

O aspecto legal da utilização dos prontuários não poderia deixar de ser abordado neste capítulo, pois demonstra na contemporaneidade todo o esforço da área de saúde, em parceria com a área arquivista, no sentido de atendimento às necessidades administrativas, jurídicas e informacionais dos usuários de serviços de saúde, que somente é alcançado pela adoção das boas práticas de gestão documental, alinhadas com a legislação brasileira, assunto abordado a seguir.

Aspectos legais do acesso às informações privadas armazenadas em arquivos de saúde

As informações registradas nos prontuários médicos dos pacientes têm seu acesso condicionado a dispositivos legais, incluindo os das áreas médica e de enfermagem e da área arquivística, que determinam o modo como tais informações devem ser preservadas em sentido físico e intelectual, tanto no meio analógico quanto no meio digital, seguindo aspectos éticos de conduta das referidas áreas. Ressalta-se que as áreas médica e de enfermagem alinham a conduta de seus profissionais aos códigos de ética respectivos, e a área arquivística ao seu, estabelecido pelo Conselho Internacional de Arquivos – CIA (CIA,1996).

A partir das considerações sobre a ética arquivística, podem-se destacar alguns dos itens contidos no código publicado pelo CIA (1996), dentre eles:

- "Um código de ética dos Arquivistas tem, por finalidade, fornecer à profissão arquivista regras de conduta de alto nível. Ele deve sensibilizar os novos membros da profissão a essas regras, relembrar os arquivistas experientes suas responsabilidades profissionais e inspirar ao público confiança na profissão".
- "Os arquivistas preservam a autenticidade dos documentos nos trabalhos de tratamento, conservação e pesquisa."
- "Os arquivistas se responsabilizam pelo tratamento dos documentos e justificam a maneira como o fazem."
- "Os arquivistas facilitam o acesso aos arquivos ao maior número possível de usuários, oferecendo seus serviços a todos com imparcialidade."
- "Os arquivistas objetivam encontrar o justo equilíbrio, no quadro da legislação em vigor, entre o direito ao conhecimento e o respeito à vida privada."
- "Os arquivistas servem aos interesses de todos e evitam tirar de sua posição vantagens para eles mesmos ou para quem quer que seja."
- "Os arquivistas trabalham em colaboração com seus colegas e os membros das profissões afins, para assegurar, universalmente, a conservação e a utilização do patrimônio documental."

No que tange à informação contida em prontuário médico, relacionam-se os aspectos legais ao Código de Ética Médica e à Constituição Federal, onde se considera obrigatória a elaboração do prontuário ou registro médico pelo médico, resguardados o respeito às questões de acesso à informação e sigilo, sem, contudo, deixar de considerar que estes aspectos são matéria da área arquivística aplicada em suas práticas, com procedimentos éticos em prol da excelência no exercício da profissão de arquivista e da garantia de direitos aos cidadãos e usuários dos registros em sistemas de saúde.

As Resoluções nº 22 do CONARQ, de 30 de junho de 2002 e nº 1.821 do CFM, de 11 de julho de 2007, são imprescindíveis neste capítulo, pois explicitam o entendimento das práticas de avaliação documental em instituições de saúde no escopo de gestão e na prática da digitalização de prontuários médicos. Estas são formas de preservar e dar celeridade no acesso às informações privadas contidas nesses materiais.

A Resolução nº 22 do CONARQ dispõe sobre as diretrizes para a avaliação de documentos em instituições de saúde e constitui um instrumento legal da área arquivística, baseado em outros dispositivos legais, como o Código Civil Brasileiro, o Estatuto da Criança e do Adolescente, a legislação arquivística que dispõe sobre a constituição de Comissões Permanentes de Avaliação de Documentos nos órgãos e entidades da Administração Pública Federal, a inserção de documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR e legislação pertinente à área médica que instituem e aprovam o regulamento do Conselho Federal e dos Conselhos Regionais de Medicina e o Código de Ética Médica.

De acordo com a referida Resolução, a necessidade de orientar as ações operacionais de avaliação de documentos em instituições de saúde que fazem assistência médica, a relevância das informações constantes dos prontuários médicos para diversos fins, a responsabilidade da instituição de saúde pela guarda, conservação, consulta, controle e acesso aos prontuários médicos para atendimento médico-assistencial em todos os níveis, e que o prontuário é documento único que contém informações de caráter sigiloso sobre situações de atendimento ao paciente e possibilita comunicação entre equipes multiprofissionais e a própria continuidade da assistência prestada ao indivíduo. Assim, o CONARQ recomenda às instituições de saúde a criação da Comissão Permanente de Avaliação de Documentos. Esta comissão deve conhecer os objetivos, estrutura e funcionamento da instituição detentora dos documentos, os conjuntos documentais a serem avaliados, sua classificação e importância para fins de prova, informação, estudos e pesquisas nas áreas de ciências da saúde, humanas e sociais, assim como a terminologia, os procedimentos e especialidades da área médica, como também a legislação pertinente à con-

cessão de direitos relativos aos indivíduos com necessidades especiais e com doenças graves terminais.

A questão relativa à temporalidade e destinação final dos documentos dos prontuários dos pacientes é de competência da comissão supracitada, por meio da análise dos conjuntos documentais para determinação dos prazos de guarda e destinação, da identificação dos valores primário e secundário segundo seu potencial de uso, do estabelecimento de critérios para análise e avaliação documental e sua destinação final, e da elaboração dos instrumentos de destinação e, se for o caso, sua revisão, destacando que a eliminação desses documentos seguirá as diretrizes constantes da Resolução nº 40 do CONARQ, de 9 de dezembro de 2014.

Por fim, cabe ressaltar que, para tais tarefas, a comissão deverá ser composta por representantes do corpo clínico e da equipe de saúde, por arquivista responsável pela guarda da documentação, por servidores das unidades organizacionais e por representantes da comissão de revisão de prontuários e da área jurídica da instituição.

A Resolução nº 1821/2007 do CFM trata da aprovação de normas para a 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 a partir das considerações de que o médico tem que elaborar um prontuário para cada paciente e que o CFM é a autoridade certificadora dos médicos no Brasil e distribuirá o CRM-Digital aos médicos interessados, o qual será certificado pela Infraestrutura de Chaves Públicas - ICP - Brasil.

Deve-se atentar para o fato de que os documentos próprios de todas as unidades de atendimento fazem parte do prontuário, assim como o crescimento do volume documental, o desenvolvimento tecnológico da informação e da comunicação, com a oferta de novos métodos de armazenamento e transmissão de dados. A partir desta perspectiva, o prontuário, em qualquer meio de armazenamento, é de propriedade física da instituição onde o paciente é assistido e os dados ali contidos pertencem a ele e devem estar permanentemente disponíveis, considerando o sigilo profissional, que intenta preservar a intimidade do indivíduo conforme normas legais e éticas.

A partir do exposto no Manual de Certificação de Sistemas de Registro Eletrônico em Saúde, elaborado em convênio com o CFM e Sociedade Brasileira de Informática em Saúde - SBIS, a autorização para eliminar documentos em papel é condicionada ao atendimento das exigências dos sistemas informatizados que atendam aos requisitos com nível de garantia de segurança 2 – NGS2, pois toda a informação em saúde identificada individualmente necessita de proteção em sua confidencialidade, por ser princípio basilar da medicina e pela obrigação do médico de proteger o sigilo profissional.

Tais perspectivas culminaram com a aprovação do referido manual em sua versão 3.0, que autoriza a digitalização de prontuários de pacientes, desde que o modo de armazenamento desses documentos digitalizados obedeça à norma específica de digitalização e após análise obrigatória da Comissão de Revisão de Prontuários e Comissão Permanente de Avaliação de Documentos da unidade médico-hospitalar geradora do arquivo.

Os métodos de digitalização devem reproduzir todas as informações dos documentos originais e os arquivos digitais oriundos da digitalização dos documentos do prontuário dos pacientes, os quais deverão ser controlados por sistema especializado de Gerenciamento Eletrônico de Documentos – GED – que possua as seguintes características mínimas: capacidade de utilizar bases de dados adequadas para armazenamento dos arquivos digitalizados, método de indexação que permita criar arquivamento organizado, propiciando pesquisa simples e eficiente, e obediência aos requisitos do NGS2 estabelecidos no manual citado anteriormente e no que concerne também ao aspecto referente à eliminação, pois esta não é autorizada em NGS1 por falta de amparo legal.

Com relação à preservação das informações, a referida resolução estabelece que os prontuários microfilmados poderão ser eliminados de acordo com legislação específica que regulamenta essa área e após análise obrigatória da Comissão de Revisão de Prontuários, assim como a guarda permanente destes, deve considerar a evolução tecnológica para os prontuários dos pacientes arquivados eletronicamente em meio ótico, microfilmado ou digitalizado, considerando como prazo estabelecido 20

anos a partir do último registro para a preservação dos prontuários dos pacientes em suporte de papel que não foram arquivados das formas citadas anteriormente.

Considerações finais

Os prontuários médicos, como fontes de registros das informações sobre o histórico de atendimento dos pacientes nos sistemas de saúde, revelam-se fontes importantes de informação e têm, nos arquivos médicos, seu ponto de referência para o tratamento documental adequado, com vistas ao atendimento de necessidades administrativas e científicas. Os arquivos têm papel preponderante no armazenamento, conservação e disseminação de informações, atribuições as quais têm seu desenvolvimento prejudicado pela falta de administração e controle de tais rotinas, além de não podermos deixar de considerar os entraves gerados pela legislação arquivística e médica que se confrontam com aspectos de ética e direitos fundamentais.

O estabelecimento de objetivos que culminem com a elaboração dos formulários que tratam de vários aspectos relativos à saúde dos pacientes para a constituição dos prontuários médicos é de suma importância para se estabelecer padrões de informações médicas em sistemas de saúde, alinhados com uma política arquivística condizente com as legislações pertinentes, de forma a atender às necessidades informacionais em todas as instâncias envolvidas nas rotinas de produção, armazenamento, controle, conservação e divulgação de informações médicas.

O avanço tecnológico tem atribuição decisiva na migração do suporte analógico – papel – para o suporte digital – em meio eletrônico – , que, juntamente com a adoção de uma política de padrões dos dados (metadados, que significam descritores de informações), compõem os formulários dos prontuários médicos eletrônicos, além de adoção de recursos de segurança da informação e transmissão das informações em ambientes *web* compatíveis entre sistemas de informações eletrônicas estabelecidos em dispositivos legais, os quais permitem maior agilidade nos trâmites administrativos, nas comunicações e na troca de informa-

ções por meio de sistemas eletrônicos (interoperabilidade) entre profissionais e instituições de saúde.

Verifica-se, portanto, que de acordo com a realidade brasileira na área de registros em saúde, a trajetória a ser percorrida pelos profissionais de informação e as instituições em saúde ainda é longa, em razão da morosidade na compreensão da importância dos registros em saúde que os arquivos armazenam e da contribuição de tais informações para o aprimoramento do tratamento dos pacientes e o desenvolvimento da pesquisa científica em saúde, que vão de encontro a entraves de origem administrativa, política e legal.

A partir do exposto neste capítulo, recomenda-se uma revisão das práticas administrativas, arquivísticas e políticas, no sentido de sensibilizar autoridades e instituições de saúde na adoção de procedimentos que normalizem e padronizem o registro, armazenamento, gestão, conservação e acesso às informações contidas em prontuários médicos concomitantemente com a adoção de técnicas informáticas que permitam a agilidade na produção, circulação e intercâmbio de informações entre as instâncias da área de saúde, representando de fato um verdadeiro avanço científico e social de forma mais ampla, realidade que verifica-se somente em algumas poucas instituições de saúde no país.

Referências

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Organização do texto: Juarez de Oliveira. 4. ed. São Paulo: Saraiva, 1990. 168 p. (Série Legislação Brasileira).

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. **Diário Oficial da União**, Brasília, DF, 18 nov. 2011. Seção 1, Edição Extra, p. 1-4. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 7 abr. 2015.

BRASIL. Lei 8.159 de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm>. Acesso em: 7 abr. 2015.

CASTRO, A. M. ; CASTRO, A. M.; GASPARIAN, D.M. **Arquivística e arquivologia**: arquivística – técnica, arquivologia – ciência. 2.ed. Rio de Janeiro: Ao Livro Técnico, 1988

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº. 1.638, de 10 de julho de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Prontuário nas instituições de saúde. **Diário Oficial da União**, 9 ago, 2002. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução 1821/2007. 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 em: <http://www.diariodasleis.com.br/busca/exibelink.php?numlink=1-178-34-2007-07-11-1821>. Acesso em: 1 out. 2014.

CONSELHO INTERNACIONAL DE ARQUIVOS-CIA. Código de ética arquivística. In: CONGRESSO INTERNACIONAL DE ARQUIVOS, 13. China, 1996. **Anais**... Rio de Janeiro, AAERJ, 1996. Disponível em: <http://www.aaerj.org.br/a-profissao/codigo-de-etica/>. Acesso em: 20 out. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Resolução nº 22, de 30 de junho de 2005. Dispõe sobre as diretrizes para a avaliação de documentos em instituições de saúde. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from_info_index=11&infoid=73&sid=46>. Acesso em: 1 out. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Resolução nº 40, de 9 de dezembro de 2014. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: < http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?infoid=1017&sid=46>. Acesso em: 5 jan. 2015.

ESCOLA POLITÉCNICA DE SAÚDE JOAQUIM VENÂNCIO (EPSIV) (Org.) **Registros de saúde**: textos de apoio. Rio de Janeiro: Fiocruz/OPAS/MS .2005. 244p. (Trabalho e formação em saúde)

MOTTA, A.L.C. **Auditoria de enfermagem nos hospitais e operadoras de planos de saúde.** São Paulo: Iátria, 2003.

PAES, M. L. **Arquivo**: teoria e prática. 3.ed. rev. ampl. Rio de Janeiro: FGV, 2004. 228 p.

POSSARI, J.F. **Prontuário do paciente e os registros de enfermagem**. São Paulo: Iátria, 2005.

VASCONCELLOS, M. M; GRIBEL, E.B. MORAES, I. H. S. de. Registros em saúde: avaliação da qualidade do prontuário do paciente na atenção básica. Rio de Janeiro, Brasil. **Cad. Saúde Pública,** v.24, suppl.1, p.s173-s182, 2008.

INSTITUTO DE SAÚDE

GOVERNO DO ESTADO DE SÃO PAULO