XXIV ENCONTRO NACIONAL DO CONPEDI - UFS

DIREITO E NOVAS TECNOLOGIAS

JOSÉ RENATO GAZIERO CELLA

VALÉRIA RIBAS DO NASCIMENTO

AIRES JOSE ROVER

D598

Direito e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UFS;
Coordenadores: José Renato Gaziero Cella, Aires Jose Rover, Valéria Ribas Do Nascimento – Florianópolis: CONPEDI, 2015.

Inclui bibliografia
ISBN: 978-85-5505-054-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: DIREITO, CONSTITUIÇÃO E CIDADANIA: contribuições para os objetivos de desenvolvimento do Milênio.

1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Encontros. 2. Tecnologia. I. Encontro Nacional do CONPEDI/UFS (24. : 2015 : Aracaju, SE).

CDU: 34

CONPEDI
Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXIV ENCONTRO NACIONAL DO CONPEDI - UFS

DIREITO E NOVAS TECNOLOGIAS

Apresentação

APRESENTAÇÃO

No XXIV Encontro Nacional do CONPEDI, realizado na Universidade Federal de Sergipe - UFS, em Aracaju, de 03 a 06 de junho de 2015, o grupo de trabalho Direito e Novas Tecnologias novamente esteve presente com destaque pela qualidade dos trabalhos apresentados e pelo numeroso público, composto por pesquisadores-expositores e interessados. Esse fato demonstra a inquietude que o tema desperta na seara jurídica, em especial nos programas de pós-graduação em Direito que procuram empreender um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao Direito.

Foram apresentados 22 artigos que foram objeto de um intenso debate e agora fazem parte desta coletânea. Numa tentativa de organizar quantitativa e qualitativamente os artigos e seus temas, segue uma métrica:

Cinco artigos trataram da Internet, em diversos âmbitos.

Quatro artigos discutiram a proteção da privacidade e dos dados pessoais e corporais.

Quatro artigos foram sobre responsabilidade civil e capacidade na internet.

Dois artigos versaram sobre aspectos regulatórios das nanotecnologias.

Dois artigos sobre marco civil da internet.

Dois artigos trataram do processo eletrônico, com enfoque de questões como inclusão, acesso à justiça e nova cultura.

Dois artigos discutiram redes sociais em temas como a violação de direitos e bloqueio de conteúdos ilícitos.

Dois artigos foram sobre o mercado de trabalho, tratando do pleno emprego e do analfabetismo digital.

Dois artigos versaram sobre a democracia eletrônica, envolvendo temas como o voto eletrônico e a democracia direta.

Um artigo sobre inovação e regulação tecnocientífica.

Um artigo sobre o direito de autor e plágio em software.

Um artigo sobre a tutela da honra no âmbito da internet.

Um artigo sobre rádio/tv na sociedade da informação.

Nota-se nessa classificação que o tema tecnológico mais tratado é a internet, mas se discute também redes sociais, nanotecnologias, urnas eletrônicas, software e tv/rádio. Dos temas jurídicos a privacidade e a responsabilidade civil são numericamente majoritários. Processo eletrônico, democracia digital e mercado de trabalho estão em seguida. Com únicos artigos seguem temas diversos, mas em pouco número considerando o total de artigos. Observa-se, portanto, algumas temáticas se tornando focais nessa edição e mantendo o interesse que vem das edições anteriores dessa coletânea.

Enfim, os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema direito e novas tecnologias. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Aires José Rover

Prof. Dr. José Renato Gaziero Cella

Profa. Dra. Valéria Ribas do Nascimento

OS DESAFIOS DA PRESERVAÇÃO DO DIREITO À PRIVACIDADE DE PESSOAS MONITORADAS POR SENSORES CONECTADOS À REDES WBAN (WIRELESS BODY AREA NETWORK) À LUZ DA LEGISLAÇÃO BRASILEIRA E AMERICANA

THE CHALLENGES OF PRESERVATION OF RIGHT TO PRIVACY OF PEOPLE MONITORED FOR SENSORS CONNECTED TO WBAN (WIRELESS BODY AREA NETWORK) FROM THE PERSPECTIVE BRAZILIAN AND AMERICAN LAW

Claudia Regina Grandi
Carlos Roberto De Rolt

Resumo

Com o avanço dos conhecimentos médicos, a mudança do perfil epidemiológico diante do envelhecimento da população e do aumento de doentes crônicos, o setor da saúde tem passado por importantes transformações nos últimos anos em todo o mundo (QUEIROZ e BARBOSA, 2003). As novas demandas do setor tornaram necessária a busca pela implementação de novas formas assistenciais, suportadas pela tecnologia. Uma das soluções que alia a medicina à tecnologia é o WBAN (wireless body area network), uma rede que permite interligar diversos dispositivos e formar uma teia entre sensores vestíveis e dispositivos que monitoram variáveis comportamentais e fisiológicas das pessoas com smartphones ou mesmo ligados direntamente a redes de internet sem fio (wi-fi). Contudo, a garantia da privacidade das informações arquivadas e transmitidas por estes dispositivos é um grande desafio. Este artigo objetiva estudar o direito fundamental à privacidade de indivíduos monitorados por tecnologias conectadas à redes WBAN, considerando os marcos legais brasileiro e americano. Realizou-se levantamento dos aparatos jurídicos do Brasil em relacão ao direito fundamental à privacidade, distinção entre intimidade e vida privada, espécie de dados pessoais, marco civil da internet e proteção de dados pessoais e erguimento da privacidade em e-health (e-saúde) dos dois países. Concluiu-se que a questão ainda carece de ordenamento jurídico adequado, tanto no Brasil como nos Estados Unidos, sendo ainda mais apropriada uma regulamentação internacional para defender os direitos dos monitorados que se desloquem entre países.

Palavras-chave: Privacidade, E-saúde, Computação ubíqua, Wban

Abstract/Resumen/Résumé

With the advancement of medical knowledge, the changing epidemiological profile with the increase of chronically ill and the aging population, the health sector has undergone important changes in recent years around the world. The new demands of the sector the search necessitated by the implementation of new care forms, supported by technology. A type of product that combines the medical technology is the WBAN (Wireless body area network), a type of wearable sensor that monitors vital signs. However, ensuring the privacy of information stored and transmitted by these devices is a major challenge. This article aims

to study the fundamental right to privacy of individuals monitored by WBAN technologies, considering the Brazilian and American legal frameworks. Carried out a survey of the legal apparatus of Brazil in relation to the fundamental right to privacy, distinction between intimacy and privacy, a kind of personal data, civil framework of internet and protection of personal data and uplifting of privacy in e-health (e-health) of the two countries. It was concluded that the issue still lacks adequate legal system, both in Brazil and in the United States, and even more appropriate international regulation to defend the rights of the monitored moving between countries.

Keywords/Palabras-claves/Mots-clés: Privacy, E-health, Ubiquos computing, Wban

1 Introdução

O presente artigo objetiva estudar o direito fundamental à privacidade de indivíduos monitorados por sensores vestíveis conectados à redes do tipo WBAN (*wireless body area network*), considerando os marcos legais brasileiro e americano.

O setor da saúde apresenta novas demandas nos dias de hoje, especialmente por conta do envelhecimento populacional: a expectativa de vida ao nascer do brasileiro aumentou de 62,5 anos em 1980 para 74,9 anos em 2013, um aumento de 12,4 anos[1]. Estima-se que em 2050, 30% da população terá mais de 60 anos (IBGE, 2014).

Duas outras grandes mudanças impactaram muito o segmento da saúde: mudanças demográficas e epidemiológicas. A primeira versa sobre a concentração da população nas cidades e centros urbanos, locais com acesso a internet mais estáveis, que permitem uso de redes de comunicação sem fio. Em 2010, 52% da população mundial morava em cidades, com perspectivas que chegue a 67% em 2050, segundo as Nações Unidas (2014)[2]. No Brasil, ao se analisar a distribuição da população no território, percebe-se uma grande concentração em áreas urbanas: a taxa de urbanização, medida pela proporção de pessoas que viviam em áreas urbanas, foi de 84,8% para o Brasil, em 2013.[3] A Pesquisa Nacional por Amostra de Domicílios (PNAD) 2013[4], realizada pelo IBGE, aponta que 49,4% dos moradores brasileiros possuem acesso à internet.

Já as mudança no perfil epidemiológico denotam o aumento da mortalidade por doenças crônicas não transmissíveis em detrimento das doenças infecto-parasitárias (Ministério da Saúde, 2012)[5] – hoje é comum que pessoas vivam por anos com doenças crônicas, como diabetes, problemas cardíacos, Alzheimer, insuficiência renal, câncer, entre outros. Tais doenças crônicas exigem tratamentos contínuos e, muitas vezes, podem vir acompanhados de disfunções e/ou algum nível de dependência (Nasri, 2008).

---

[1] Conforme Tábua Completa de Mortalidade 2013 divulgada pelo IBGE 01/12/2014, considerando ambos os sexos. Disponível em <ftp://ftp.ibge.gov.br/Tabuas_Completas_de_Mortalidade/Tabuas_Completas_de_Mortalidade_2013/pdf/ambos_pdf.pdf >Acesso em 2 de março de 2015.

[2] Disponível em <http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf >Acesso em 3 de março de 2015.

[3] Disponível em <ftp://ftp.ibge.gov.br/Indicadores_Sociais/Sintese_de_Indicadores_Sociais_2014/SIS_2014.pdf>Acesso em 3 de março de 2015.

[4] Disponível em <http://www.ibge.gov.br/home/estatistica/populacao/trabalhoerendimento/pnad2013/default.shtm >Acesso em 3 de março de 2015.

[5] Confirmados em pesquisa Vigitel Brasil 2011, com estimativas sobre frequência e distribuição sociodemográfica de fatores de risco e proteção para doenças crônicas nas capitais dos 26 estados brasileiros e no distrito federal. Disponível em <http://bvsms.saude.gov.br/bvs/publicacoes/vigitel_brasil_2011_fatores_risco_doencas_cronicas.pdf >Acesso em 2 de março de 2015.

Tanto pacientes crônicos quanto idosos necessitam de acompanhemento e cuidados permanentes, medições de sinais vitais frequentes, acesso rápido ao socorro e ao atendimento de emergência (WILKOWSKA e ZIEFLE, 2011).

Estas mudanças geram impacto direto nos gastos com saúde, tanto públicos quanto privados, bem como na previdência do país (Banco Mundial, 2011). Os custos e despesas do setor são elevados, tornando a busca por soluções de suporte tecnológico um caminho para a sustentabilidade do segmento.

Contudo, a mesma tecnologia que pode solucionar problemas e ajudar na prestação de serviços médicos tão importantes a manutenção da vida humana, principamente em situações de urgência e emergência, pode ameaçar a garantia do direito à privacidade do paciente monitorado por redes WBAN, foco central deste artigo, que está estruturado em seis partes: 1. Introdução; 2. As redes WBAN e o desafio da garantia do direito à privacidade, 2.1 Computação ubíqua; 3. O Direito Fundamental à Privacidade no Brasil, 3.1 Intimidade e vida privada: distinção conceitual pela teoria das esferas, 3.2 A privacidade na sociedade da informação, 3.3 Espécie de dados pessoais, 3.4 Marco civil da internet no Brasil, 3.5 Proteção de dados pessoais – Anteprojeto de Lei; 4. Privacidade em e-saúde (*e-health*), 4.1 No Brasil, 4.2 Nos Estados Unidos; 5. Considerações finais e 6. Referências.

2 As redes WBAN e o desafio da garantia do direiro à privacidade

Dentre as soluções que aliam a medicina à tecnologia estão os produtos tecnológicos vestíveis para medições e monitoramento de dados de saúde conectados via internet – os chamados WBAN (*wireless body area network*), também ditos serviços de e-sáude, objeto deste estudo. Barakah e Ammad-uddin (2012) comentam que o WBAN ganhou muito interesse e tornou-se tecnologia emergente em centros de serviços de saúde devido à sua ampla gama de utilidade e seu papel vital para melhorar a saúde humana.

Wireless body area network é um tipo especial de rede, concebido e desenhado para o corpo humano, para monitorar, gerenciar e comunicar diferentes sinais vitais como a temperatura, pressão arterial, eletrocardiograma etc. Estes sinais vitais podem ser monitorados por meio de um sensor instalado sobre a roupa, ou no corpo, ou mesmo sob a pele. Uma Unidade Central é responsável por estabelecer a comunicação entre sensores, atuadores e telefone celular por meio de rede sem fio. O celular da pessoa monitorada pode ser usado para transmitir toda a informação que está sendo medida no corpo humano para o mundo exterior (médico, emergência). Este tipo de rede pessoal sem fio ao redor e/ou perto do corpo humano

chamado de WBAN atribui para cada "corpo monitorado" um endereço IP (protocolo de internet) (BARAKAH e AMMAD-UDDIN, 2012).

A tecnologia móvel para saúde é promissora em muitos aspectos: permite aos médicos monitorar remotamente a saúde de seus pacientes, melhorando os cuidados com a saúde e permitindo aos próprios pacientes "gerir" a sua saúde com mais facilidade, além de reduzir custos de internações hospitalares e de deslocamento de pacientes, que podem receber auxílio remoto em situações menos complexas (AVANCHA, BAXI e KOTZ, 2012).

O uso de tais dispositivos para monitoramente de saúde vestíveis conectados sem fio permitem um acompanhamento médico contínuo a longo prazo para muitas finalidades (Baker et al, 2007; Boric-Lubecke e Lubecke, 2002; Varshney, 2007): para pacientes ambulatoriais com condições crônicas de saúde, indivíduos que buscam mudanças de comportamento, como a perda de peso, médicos que necessitam quantificar e detectar alterações físicas de pacientes para o diagnóstico precoce e preciso, ou atletas que desejam monitorar sua condição e performance.

Os autores Avancha, Baxi e Kotz (2012) levantam no artigo "*Privacy in Mobile Technology for Personal Healthcare*" diversas interações a partir dos dispositivos de medição que comunicam-se via internet com *smartphones*:

> Os dados resultantes podem ser usados diretamente pelo paciente (AC, 2008; AH, 2008; Wang et al. 2006), ou podem ser compartilhados com os outros: com um médico para o tratamento (SH, 2008), com uma companhia de seguros para a cobertura, com um cientista de pesquisa (DH, 2008), com um treinador para o treinamento atlético (Aylward e Paradiso, 2007), ou com familiares e amigos em comunidades de redes sociais direcionados para a saúde e bem-estar (OW, 2009; DS, 2009, por exemplo) (Pág. 2, tradução livre)

As inovações tecnológicas, o desenvolvimento das TICs (tecnologias da informação e comunicação) e os avanços da telemedicina criam oportunidades aos pacientes que, uma vez monitorados, poderão ter maior e mais rápido acesso à assistência médica. Mas alguns desafios apresentam-se neste contexto: como as pessoas podem ser afetadas em seus direitos à privacidade? Quais direitos dos monitorados podem ser afetados pelo uso de dispositivos do tipo WBAN, no momento em que as informações são repassada a uma rede?

Rindfleisch (1997) previne que "as informações do paciente podem ser utilizadas por um número muito grande de pessoas das mais variadas instituições". Por isso, para que a implantação de medidas de segurança da informação na área da saúde seja eficaz é necessário

conhecer os possíveis caminhos que serão percorridos, seus contextos, e também que seja estabelecida uma aproximação entre os especialistas na área de saúde e os especialistas em segurança da informação, uma vez que há pouco intercâmbio entre as áreas, acarretando que uns possuem poucos conhecimentos da área dos outros (ROSARIO, 2010).

Al Ameen, Liu e Kwak (2010) alertam que como a maioria dos dispositivos e seus aplicativos trafegam informações por rede sem fio, as preocupações de segurança e privacidade estão entre as principais inquietações.

Informações sobre o monitorado podem interessar a Operadoras de Saúde, que poderiam reajustar o valor do plano anualmente considerando as medições do monitorado. Seguradoras também poderiam usar essas informações para aceitar ou reajustar planos. O mercado laboral também poderia ser afetado, uma vez que empresas tenham acesso a medições de um candidato a uma vaga de emprego, balizando uma contratação por critérios "físicos". Portanto, a privacidade dos dados do monitorado pode ser considerada não só um desafio como uma barreira na disceminação dos dispositivos de monitoramento por redes WBAN.

2.1 Computação ubíqua

Os dispositivos conectados por redes WBAN são estudados no contexto da computação ubíqua em saúde (pHealth ou UbiHealth). Ubiquidade significa onipresença, estar em toda parte. O termo "computação ubíqua" foi cunhado pelo cientista e pesquisador do Centro de Pesquisa Xerox PARC Mark Weiser, por meio do artigo "O Computador do Século 21 (*The Computer for the 21st Century*), de 1991 (BOLSONI, CARDOSO, MEDEIROS DE SOUZA, 2009)[6]. Weiser (1991, pág. 19) preveu que no futuro "as tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam com o cotidiano até que se tornem indistinguíveis dele". A ideia da computação ubíqua é que o computador "se esconde" nas coisas, as máquinas e objetos computacionais ficam imersos no dia a dia de forma onipresente, possível graças a era da conexão a internet.

Com uma computação invisível e onipresente, todos os lugares estarão repletos de sensores monitorando o ambiente. Este é um modelo reverso ao da realidade virtual, onde o real é projetado no virtual; na computação ubíqua, também chamada de pervasiva, o virtual é projetado no real, de forma a auxiliar as pessoas em seu cotidiano, com uma computação

[6] Disponível em <http://www.ceped.ufsc.br/wp-content/uploads/2009/01/Artigo-14.pdf>Acesso em 10 de março de 2015.

adaptável ao contexto do usuário (MACHADO, LIBRELOTTO E AUGUSTIN, 2010, PÁG. 317). Os autores consideram ainda que

> O sistema de saúde do futuro prevê o uso de tecnologias da computação pervasiva formando um espaço inteligente, reativo e pró-ativo, onde dispositivos móveis e fixos estão totalmente integrados ao ambiente com objetivo de captar informações do meio físico e transmitir as alterações detectadas para os sistemas de gerenciamento de informações, os quais tomarão decisões e adaptarão às situações detectadas. (Pág. 316)

Christensen e Bardram (2007) afirmam que o trabalho realizado por uma equipe clínica ou hospitalar é um desafio para os pesquisadores da computação pervasiva, uma vez que nestes ambientes é preciso lidar com grandes volumes de dados compartilhados, tais como registros de pacientes (prontuários) e resultados de exames. Nestes lugares, as tecnologias ubíquas têm potencial para apoiar o uso móvel e colaborativo de dispositivos.

A mudança de modelo tecnológico que superou o modelo estático e relativamente previsível, baseado em estações de trabalho, para um modelo dinâmico, móvel e de grande interação faz emergir uma forte discussão sobre a privacidade, uma vez que o usuário pode não querer ser localizado, ou pode não querer compartilhar seus dados a todo o momento (LEITHARDT et al, 2014).

O monitoramento da saúde por meio de computação onipresente WBAN tem mostrado grande potencial na melhoria da qualidade de cuidados de saúde. Ao mesmo tempo, há uma grande preocupação com a privacidade e proteção dos dados coletados, tanto no armazenamento quando na transmissão de informações.

3 O Direito Fundamental à Privacidade no Brasil

No Brasil, a promulgação da Constituição Federal de 1988 representou um grande avanço, visto que não apenas estabeleceu um regime político democrático no Estado Brasileiro, como também propiciou um grande progresso no que diz respeito aos direitos fundamentais.

Direitos fundamentais estão ligados à história e às lutas de uma sociedade, conforme argumenta Norberto Bobbio (1992):

> Os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizados por lutas em defesa de novas liberdades contra velhos poderes, e

> nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas." (pág. 9)

Portanto, o autor considera que não existe direito fundamental por natureza, uma vez que o que é considerado fundamental em dado momento, pode não o ser em outra época.

João Trindade Cavalcante Filho[7] qualifica direitos fundamentais como os direitos considerados básicos para qualquer ser humano, compondo um núcleo intangível de direitos dos seres humanos submetidos a uma determinada ordem jurídica. O autor comenta ainda a característica da eficácia vertical e horizontal dos direitos fundamentais, visto que aplicam-se não só nas relações entre o Estado e o cidadão (eficácia vertical), como também nas relações entre os particulares-cidadãos (eficácia horizontal).

Conquanto alguns autores tratam os termos "direitos humanos" e "direitos fundamentais" como sinônimos (MORAES, 2000), Fábio K. Comparato (2001) preocupa-se em fazer uma distinção entre tais terminologias. Em sua visão, os direitos fundamentais são os Direitos Humanos reconhecidos como tal pelas autoridades. Portanto, são os Direitos Humanos positivados nas Constituições, nas leis, nos tratados internacionais. Exercem também uma função pedagógica, no sentido de fazer prevalecer os grandes valores éticos, que demorariam a se estabelecer na vida coletiva sem tal reconhecimento oficial. "O reconhecimento oficial dos Direitos Humanos pelo ordenamento jurídico dá mais segurança às relações sociais" (ALMEIRA, 2010).

O direito à privacidade, segundo Tatiana Malta Vieira (2007)

> (...) foi sendo incorporado gradualmente às legislações criminais e civis de cada país, até ser reconhecido como direito fundamental previsto na maior parte das constituições modernas. Na área civil, protege-se o direito à privacidade incluindo-o na categoria dos direitos da personalidade juntamente com a proteção do corpo, da honra, da imagem e do nome. (pg. 37).

Tartuce (2005) explica que "Os direitos da personalidade podem ser conceituados como sendo aqueles direitos inerentes à pessoa e sua dignidade. Surgem cinco ícones principais: vida/integridade física, honra, imagem, nome e identidade".

Os direitos da personalidade são absolutos, instransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis e inexpropriáveis (DINIZ, 2007, p.

[7] Disponível em <http://www.stf.jus.br/repositorio/cms/portaltvjustica/portaltvjusticanoticia/anexo/joao_trindadade__teoria_geral_dos_direitos_fundamentais.pdf >Acesso em 2 de março de 2015.

119), ou seja, não podem sofrer qualquer espécie de limitação, nem mesmo voluntária por parte de seu próprio titular.

A importância dos direitos personalíssimos evidencia-se por sua presença tanto na legislação civil (artigos 11 a 21), como também na própria Constituição Federal, no artigo 5º, configurando-se, portanto, como cláusula pétrea, abrangendo o direito à privacidade.

O artigo 5° da Constituição Federal afirma em seus incisos V e X, respectivamente: "Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; X – 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;". O inciso V aborda o direiro de resposta, enquanto o inciso X defende a inviolabilidade.

No Código Civil, o artigo 11 versa que "Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.", enquanto o artigo 21 assegura: "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."

O direito à privacidade, segundo Celso Ribeiro Bastos (1989), consiste: "Na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes 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".

Tatiana Malta Vieira (2007) conclui que

> os direitos fundamentais são eminentemente democráticos, ou seja, configuram-se como mecanismos de defesa da democracia. Seu caráter objetivo relaciona-se intimamente ao fortalecimento dessa forma de governo, aferindo-se dessa estreita relação a relevância dessa garantia. Ao integrarem o conteúdo principal das constituições dos Estados Democráticos de Direito, juntamente com as normas que organizam e estruturam o Estado propriamente dito, funcionam como uma garantia a favor das minorias contra as opressões da maioria, especialmente no que concerne às liberdades públicas, tais como a privacidade; a liberdade de manifestação do pensamento; a liberdade

> de consciência e de crença; a liberdade de expressão e de comunicação; a liberdade de profissão; e a liberdade de associação. (pág. 96)

Desta forma, pode-se concluir que os direitos fundamentais possuem duas dimensão: a) subjetiva, enquanto garantia individual de exigir do Estado e dos demais particulares determinados comportamentos negativos ou positivos; e b) objetiva, na condição de sistema de valores de um Estado Democrático de Direito, ao funcionar simultaneamente como diretriz e como limite ao poder público, estabelecendo-se íntima relação entre direitos fundamentais e democracia (VIEIRA, 2007, pág. 96 e 97).

3.1 Intimidade e vida privada: distinção conceitual pela teoria das esferas

Diversos juristas recorrem à teoria das esferas para diferenciar os conceitos de intimidade e direito à vida privada. Desenvolvida pela doutrina alemã, a teoria das esferas ou círculos concêntricos "(...) se funda no fato de que a sociabilidade da pessoa deve servir de limitação à sua liberdade individual, devendo a intensidade da tutela jurídica da personalidade ser inversamente proporcional à sociabilidade do seu comportamento em questão". (SAMPAIO, 1998 apud Winikes e Camargo, 2012)

Heinrich Hubmann é um dos pioneiros em dividir a personalidade humana em três esferas concêntricas (que tem o mesmo centro, mas raios diferentes), em publicação de 1953 (WINIKES e CAMARGO, 2012). A esfera mais ampla seria a esfera individual na qual se desenvolve a personalidade da pessoa, que abarcaria a pessoa na sua unicidade e identidade. A segunda esfera, menor que a anterior, seria a esfera privada, enquanto a menor e mais restrita das esferas seria a esfera secreta, a que conglomera situações restritas à própria pessoas ou à um círculo limitado de pessoas.

O também alemão Heinrich Henkel publicou na edição de 1957 de tradicional congresso jurídico alemão (*Deutscher Juristentages*, Fórum Jurídico Alemão) posicionamento semelhante ao de Hubmann, classificando a personalidade humana também em três esferas (em grau decrescente de proteção): esfera do segredo, esfera da intimidade e esfera privada. Tal concepção doutrinária tem sido divulgada no Brasil por Paulo José da Costa Júnior desde 1970, quando da publicação de sua monografia "O direito de estar só: tutela penal da intimidade".

Winikes e Camargo (2012) alertam que a diferença entre as propostas dos referidos autores é somente de nomenclatura, sendo que praticamente a mesma amplitude pode ser observada em cada uma das esferas (da mais restrita até a mais larga).

Paulo José da Costa Júnior (1995) esclarece que no círculo externo, da privacidade, estão todos os fatos e comportamentos que o indivíduo deseja resguardar para que não se tornem de domínio público. No segundo círculo, da intimidade ou da confidência, concentram-se as informações compartilhadas apenas com as pessoas com as quais o indivíduo estabelece uma relação de confiança, excluindo-se o público em geral e as pessoas de sua convivência em relação às quais não confia. No círculo menor e central, dito do segredo, guardam-se as informações que devem ser mantidas em sigilo ou em segredo, ou seja, aquelas nunca compartilhadas e aquelas reveladas apenas para as pessoas extremamente íntimas (VIEIRA, 2007, pág. 30).

A teoria das esferas ou círculos concêntricos objetiva "garantir à pessoa uma esfera mínima inviolável, na qual a pessoa é absolutamente livre e não está sujeita a interferências de qualquer ordem" (PONTES DE MIRANDA, op. cit., p. 123, apud WINIKES e CAMARGO, 2012).

Por tratarem-se de aspectos subjetivos do homem, é difícil diferenciar os conceitos intimidade e vida privada, além de serem dinâmicos devido às influências culturais, religiosas, políticas, entre outras, em determinada época na qual se vive (SAMPAIO, 2006 apud ROSSONI e BOLESINA, 2014). O jurista Sampaio (2006) argumenta que a diferença entre esses dois conceitos baseia-se na abrangência do círculo de conhecimento, ou seja, o número de pessoas que tem posse a determinada informação. Fato íntimo está ligado a um conhecimento próprio do indivíduo e revelado apenas a um pequeno grupo de pessoas. Já um fato no qual ultrapassa esses limites, mas não é explícito ao público em geral, é considerado privado (NASCIMENTO, 2009, p. 27).

Apesar de no Brasil, assim como nos países de língua espanhola, os termos intimidade e vida privada serem usados indistintamente, Sampaio defende que por meio da análise do direito comparado e da etimologia das palavras, a intimidade é um extrato mais restrito da vida privada (ROBL FILHO, 2006).

3.2 A privacidade na sociedade da informação

A privacidade na sociedade da informação ganha relevância com a disseminação da internet e das redes sociais, bem como da tecnologia que permite associar e "cruzar" informações de pessoas. A informação tornou-se o grande "ativo" da sociedade contemporânea, portanto houve a necessidade de se buscar uma "gestão mais eficiente das

informações", o que fez surgir uma especialidade denominada segurança da informação[8]. Trata-se da área responsável por assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações.

Segurança da Informação	
Disponibilidade	Possibilidade de acesso e utilização oportunos de informações por indivíduos e sistemas autorizados.
Integridade	Significa que a informação não foi modificada, inclusive quanto à origem e ao destino.
Autenticidade	Quer dizer que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo ou sistema.
Confidencialidade	Significa acesso ou divulgação restritos, ou seja, sigilo[9]

Quadro 1 - Segurança da Informação. Adaptado de Vieira (2007).

Hoje, a segurança da informação está sendo implementada tanto pelo setor privado – como forma de garantir a continuidade do negócio, minimizar os riscos e maximizar os investimentos – como pelo setor público – especialmente para garantir a disponibilidade e a integridade dos documentos públicos, para controlar o acesso às informações sigilosas e para incrementar as atividades de governo eletrônico.

Frente a excessiva acumulação de informações de caráter pessoal, o espaço virtual ao possibilitar a comunicação por meio da tecnologia pode colocar em risco a privacidade dos usuários. Maria Eduarda Gonçalves (2003) alerta que

> poucos serviços prestados pela web dispensam a coleta, o armazenamento, o tratamento e a difusão de dados relacionados com a intimidade e com a vida privada dos internautas. Qualquer acesso à rede deixa gravados registros do usuário, ainda que de forma indireta: o seu espectro de relações, as suas opiniões e gostos, os hábitos de consumo, o nível social, entre outros. O problema reside no fato de a coleta de dados ser feita tanto de forma transparente para finalidades explícitas e autorizadas pelo titular, como também de forma velada e contra os interesses da pessoa em questão (GONÇALVES, 2003, pág. 173-174).

[9] Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm#art60 > inciso XII do artigo 2º, do Decreto nº 7.845, de 14 de novembro de 2012.

O tráfego mundial de dados é muito expressivo se comparado há anos atrás. A todo momento, dados pessoais[10] são armazenados e extraídos da computação em nuvem via internet, portanto a busca pela privacidade é elemento sensível sempre que tais informações são coletadas e transmitidas.

Hoje a sociedade está conectada por *smartphones*, e-mails, chats, comunidades *on line*, SMS, *Voip*, e tem à sua dispoição uma infinidade de ferramentas que até pouco atrás não existiam, e a popularidade de dispositivos móveis com acesso a internet torna viável uma série de tipos de comunicação, especificamente a de produtos conectados à redes WBAN, objeto deste estudo, os quais geram novas formas de relacionamento – do monitorado com o médico, do monitorado com a sua família, do monitorado com pesquisadores, por exemplo, afetando, consequentemente os aspectos que envolverm as relações sociais com foco em saúde.

Ao observar a classificação da privacidade em diferentes categorias, conforme seu âmbito de proteção: física, do domicílio, das comunicações, decisional e informacional (VIEIRA, 2007), é possível relacionar as categorias ligadas à privacidade de dados do monitorado por um dispositivo conectado à rede WBAN, conforme demostrado no quadro abaixo.

Classificação de privacidade

Categoria	**O que é**	**Privacidade em WBAN**
Física	Protege o corpo do indivíduo contra procedimentos invasivos não autorizados pelo próprio indivíduo.	
Do domicílio	"A casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial".[11]	
Das comunicações	"Inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por	✓

[10] Entende-se por dados pessoais qualquer informação tal como um nome, uma fotografia, um número de telefone, um endereço postal ou de correio eletrónico, dados bancários, participações em sítios de redes sociais, informações médicas, dados sobre convicções religiosas ou o endereço IP de um computador (ARAÚJO e OLIVEIRA, 2014)

[11] Artigo 5º da Constituição Federal, inciso XI.

	ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".[12]	
Decisional	Atributo inato ao indivíduo, ao ser humano, de decidir seu próprio destino, de tomar as próprias decisões.	
Informacional	Cinge em seu âmbito de proteção, as informações sobre determinada pessoa, abarcando não só aquelas relacionadas a sua esfera mais íntima, mas também dados pessoais.	✓

Quadro 2 – Classificação de privacidade conforme âmbito de proteção. Adaptado de Vieira (2007).

Uma vez que as informações do monitorado envolvem a comunicação de dados, dados estes pessoais, conclui-se que as categorias "das comunicações" e "informacional" estão diretamente ligadas à privacidade do monitorado por WBAN.

3.3 Espécie de dados pessoais

Após os entendimentos sobre o direito fundamental à privacidade, a distinção dos conceitos da intimidade e vida privada, sob a luz da teoria dos círculos concêntricos, e o olhar da privacidade na era da informação, é importante contextalizar a proteção de dados pessoais.

> Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo). Entende-se por identificado, o indivíduo que já é conhecido; e por identificável, a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros (CASTRO, 2005).

Os dados pessoais podem ser classificados em três espécies: não sensíveis; sensíveis; e de tratamento proibido, e podem ser relacionados diretamente com a já abordada teoria das esferas: dados não sensíveis correspondem a esfera privada, també chamada de *Sphere of privacy* pelos americanos; dados sensíveis são os da esfera da intimidade ou esfera confidencial, cujo acesso é mais restrito, enquanto os de tratamento proibido são os dados da esfera do segreso, da vida íntima da pessoa (VIEIRA, 2007).

[12] Artigo 5º da Constituição Federal, inciso XI.

Cada tipo de dado deve ser tratado de forma distinta, conforme aponta Antônio Jeová Santos (2001). Os dados não sensíveis:

- Coleta: podem ser coletados e armazenados sem prévio e expresso consentimento de seu titular ou representante.
- Exemplo: nome, sobrenome, sexo, estado civil e outros.

Já os dados sensíveis:

- Coleta: necessitam da prévia e expressa permissão do titular ou de seu representante para serem tratados; exceto se houver autorização legal, quando será dispensável essa manifestação.
- Exemplo: dados íntimos como a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, *saúde* e vida sexual do indivíduo.
- Risco: a recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento e eliminação de dados sensíveis é considerada atividade de risco pela responsabilização objetiva pela divulgacão ou acesso indevidos.

Dados de tratamento proibido:

- Coleta: deve existir vedação legal de seu tratamento, para sua total e absoluta proteção.
- Exemplo: aspectos relacionados à dignidade humana de seu titular.

Doneda (2006) concorda com Santos (2001) ao considerar que os dados de saúde são considerados dados sensíveis.

3.4 Marco civil da internet no Brasil

As redes WBAN comunicam-se via internet sem fio (*wi-fi*), por isso é relevante abordar a a Lei 12.965, de 23 de abril de 2014, conhecida como Marco civil da internet, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. Também chamada de "Constituição da internet", preencheu uma lacuna na legislação brasileira definindo de forma clara direitos e responsabilidades relativas à utilização dos meios digitais,

ao invés de apenas criminalizar condutas nesses espaços. [13] Construído de forma colaborativa, tem como um de seus eixos a Privacidade na rede.

Já nas disposições preliminares, no artigo 3º que aborda os princípios da disciplina do uso da internet no Brasil, a "proteção da *privacidade*" aparece no II inciso e a "proteção dos dados pessoais, na forma da lei" no III inciso.

Nos três primeiros incisos do artigo 7º do Marco Civil, são aventados os direitos dos usuários, inviolabilidade da intimidade e da vida privada; inviolabilidade e sigilo do fluxo de suas comunicações pela internet; inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

O artigo 8º, no capítulo sobre os Direitos e Garantias do usuário, condiciona à privacidade o exercício do direito de acesso à internet: "Art. 8º A garantia do direito à *privacidade* e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.".

O Marco civil da internet dispõe de forma geral sobre os direitos de *privacidade* dos usuários da internet, estabelecendo normas para a proteção da *privacidade*, tanto sobre a guarda e o tratamentos de registros, quanto sobre a forma como essas informações devem ser disponibilizadas ao cidadão (art. 11, §3º). O artigo 11, da seção II, do capítulo III, Da provisão de conexão e de aplicações de internet, incide: "Art. 11º Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à *privacidade*, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.", sendo o parágrafo terceiro: "§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à *privacidade* e ao sigilo de comunicações."

3.5 Proteção de dados pessoais – Anteprojeto de Lei

O direito a proteção de dados atualmente no Brasil não está identificado especificamente no artigo 5º da Constituição Federal, está sim posto como decorrência dos direitos à intimidade e privacidade (BOSSOI, 2014).

[13] <http://participacao.mj.gov.br/marcocivil/a-importancia-do-marco-civil-e-seu-historico/ >Acesso em 9 de março de 2015.

Para resolver tal questão, há um debate público do Anteprojeto de Lei de Proteção de Dados Pessoais no sítio http://participacao.mj.gov.br/dadospessoais/ [14], que ocorre por meio de comentários em discussão aberta a qualquer cidadão sobre o texto de lei sugerido.

Organizado de forma colaborativa, o Anteprojeto de Lei de Proteção de Dados Pessoais é resultado de um amplo debate público promovido pelo Ministério da Justiça, em parceria com o Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil, com duração de cinco meses, recebendo mais de 14 mil visitas e mais de 800 contribuições, entre 2010 e 2011.

No site do Projeto Pensando o Direito [15] - <http://participacao.mj.gov.br/pensandoodireito/ >, que é uma iniciativa da Secretaria de Assuntos Legislativos do Ministério da Justiça, dedicada desde 2007 a promover a democratização do processo de elaboração legislativa no Brasil, o Ministério da Justiça declara considerar fundamental ter um marco legal de proteção de dados no Brasil, e afirma que atualmente mais de 100 países já possuem leis de proteção de dados pessoais.

Uma lei sobre proteção de dados permite que o cidadão tenha controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Tem por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado para seu uso e outros, sempre garantindo ao cidadão protagonismo nas decisões fundamentais a este respeito. O impacto maior de uma lei sobre proteção de dados pessoais é o equilíbrio das assimetrias de poder sobre a informação pessoal existente entre o titular dos dados pessoais e aqueles que os usam e compartilham.[16]

4 Privacidade em e-saúde (*e-health*)

4.1 No Brasil

O ano de 2003 foi marcante no Brasil para o debate e a fundamentação de uma proposta de política nacional de informação e informática em saúde, quando o Ministério da Saúde definiu como um de seus objetivos setoriais prioritários a elaboração da política de informação e informática em saúde (MINISTÉRIO DA SAÚDE, 2004). Brender et al.(2000), Rigby (1999), e Morris et al (2002) enfatizam que o contexto internacional vem destacando a

[14] Acesso em 6 de março de 2015.
[15] Acesso em 9 de março de 2015.
[16] <http://participacao.mj.gov.br/dadospessoais/importancia-de-uma-lei-sobre-protecao-de-dados/ >Acess em 9 de março de 2015.

relevância de políticas e estratégias setoriais de comunicação e informação em saúde, diante de suas possibilidades de geração de novos processos e produtos, e de mudanças nos modelos institucionais de gestão.

Em 2011, o Ministério da Saúde (MS) redefiniu o Comitê de Informação e Informática em Saúde (CIINFO) (BRASIL, 2011), incluindo dentre suas competências a revisão, promoção e fortalecimento da Política Nacional de Informação e Informática em Saúde (PNIIS). "A efetivação da PNIIS visa ainda a uma melhor governança no uso da informação em saúde e dos recursos de informática, integrando-se ao conceito de Governo Eletrônico" (BRASIL, 2011).

Como alicerces da estrutura da PNIIS 2013, foram definidos nove princípios, destacando-se o sétimo e o oitavo, que abordam diretamente a privacidade:

> 7. Informação de saúde pessoal é toda aquela atinente à gestão, à vigilância e à atenção à saúde individualmente identificada ou identificável, garantida ao indivíduo a sua confidencialidade, sigilo e privacidade de dados; e 8. A informação de saúde que identifica a pessoa, gerada em qualquer evento de atenção à saúde, é de interesse do indivíduo, e seu uso somente pode ser autorizado pelo indivíduo ou por seu responsável legal, salvo disposição legal (BRASIL, 2011, pág. 11)

O entendimento do termo *e-saúde*, também conhecido por seu equivalente em inglês *e-health* neste artigo considera o glossário da PNIIS, 2013, que segundo a *Healthcare Information and Management Systems Society* (HIMSS), trata-se de

> qualquer aplicação de internet, utilizada em conjunto com outras tecnologias de informação, focada na melhoraria do acesso, da eficiência, da efetividade e da qualidade dos processos clínicos e assistenciais necessários a toda a Cadeia de Atendimento à Saúde. O objetivo único é prover melhores condições de tratamento aos pacientes e melhores condições de custeio ao Sistema de Saúde. O conceito de e-saúde engloba desde a entrega de informações clínicas aos parceiros da cadeia de atendimento, passando pelas facilidades de interação entre todos os seus membros, chegando a disponibilização dessa mesma informação nos mais difíceis e remotos lugares. (pág. 27)

Por meio da resolução WHA58.28 da Organização Mundial da Saúde (OMS), de 2005, foi introduzido o conceito de e-saúde: "e-saúde é o uso das tecnologias de informação e comunicação para a saúde. Exemplos incluem assistência a paciente, pesquisa, educação e capacitação da força de trabalho em saúde e monitoração e avaliação em saúde[17]".

A OMS (2011), em estudo que aborda as tecnologias móveis (*m-health*), que são englobadas pelo conceito de e-saúde, demonstra a preocupação quanto a segurança dos dados e a privacidade do cidadão como áreas que requerem atenção legal e política para garantir que os dados dos usuários de *m-health* sejam devidamente protegidos.

No Brasil, a privacidade e o sigilo de informações em saúde são abordadas por algumas normas setoriais e éticas.

Entre os seus princípios, o Código de Ética Médica (CEM)[18] trata do dever de sigilo profissional, salvo por motivo justo, dever legal ou consentimento do paciente; veda ao médico permitir o manuseio dos prontuários sob sua responsabilidade por pessoas não obrigadas ao sigilo profissional (art. 85); e proíbe também, durante o exercício da docência, a prática da medicina sem o consentimento do paciente e sem zelar por privacidade (art. 110).

A Agência Nacional de Saúde Suplementar (ANS) estabeleceu na Resolução Normativa 305 (RN 305), de outubro de 2012[19], um padrão obrigatório para a troca de informações em saúde entre operadoras de planos privados de assistência à saúde e prestadores de serviço, chamado de Padrão TISS (Troca de Informações na Saúde Suplementar). A segurança e privacidade dos dados são um dos componentes desse padrão, que prevê os requisitos para proteção dos dados de atenção à saúde, devendo seguir a legislação vigente.

Duas portarias do Ministério da Saúde manifestam preocupações com a segurança e a privacidade das informações de saúde no Brasil:

a) Portaria 2.073/2011[20], que discorre 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, que coloca entre seus objetivos a promoção da utilização de uma arquitetura da informação em saúde de modo a

[17] Disponível em <http://www.who.int/healthacademy/media/WHA58-28-en.pdf >Acesso em 6 de março de 2015.
[18] Disponível em http://www.portalmedico.org.br/novocodigo/integra_preambulo.asp Acesso em 6 de março de 2015.
[19] Disponível em < http://www.ans.gov.br/aans/noticias-ans/operadoras-e-servicos-de-saude/1764-padrao-tiss-versao-30-?highlight=WyJybiIsMzA1LCJybiAzMDUiXQ== > Acesso em 7 de março de 2015.
[20] Disponível em < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html > Acesso em 7 de março de 2015.

permitir o compartilhamento de informações em saúde num meio seguro e com respeito ao direito à privacidade (art 2º, II); e

b) Portaria 940/2011[21], que regulamenta o Sistema Cartão Nacional de Saúde, e especifica as regras para garantia do sigilo dos dados e das informações dos usuários SUS coletados pelo Sistema.

4.2 Nos Estados Unidos

O Comitê Nacional de Estatísticas Vitais e de Saúde (NCVHS), que é um comitê consultivo chave para o Departamento de Saúde e Serviços Humanos dos Estados Unidos, adota as seguintes definições para privacidade, confidencialidade e segurança:

> A *privacidade* das informações sobre saúde é um direito de um indivíduo para controlar a aquisição, utilização ou divulgação de seus dados de saúde identificáveis. *Confidencialidade*, questão estreitamente ligada, refere-se às obrigações das pessoas que recebem informações de respeitar os interesses de privacidade das pessoas a quem os dados se referem. Já a *segurança* trata de garantias ou ferramentas utilizadas para proteger os dados identificáveis de saúde de acesso indevido ou divulgação (Cohn, 2006, tradução livre[22]).

Nos Estados Unidos, em 1996 foi aprovada a *Health Insurance Portability and Accountability Act*, conhecida como HIPAA (HIPAA, 2010), que destina-se a garantir a portabilidade e prestação de contas de todos os profissionais de saúde e seguradoras, e identificar importantes direitos de privacidade e políticas de segurança.

O conjunto de regras sobre privacidade na área de saúde mais conhecido são as Regras de Privacidade e Segurança da HIPAA (HIPAA, 2010) que, entre outras coisas, procuram garantir que informações pessoais de saúde, mesmo que na posse de prestadores de cuidados de saúde e pagadores (Operadores de saúde, por exemplo), sejam protegidas de usos e divulgações que possam comprometer os interesses dos pacientes.

As Regras de Privacidade e Segurança da HIPAA fornecem uma linha de base de proteção de privacidade para as informações de saúde nos Estados Unidos, enquanto permite que as leis estaduais mais protetoras continuem em vigor, impondo restrições à utilização e

[21] Disponível em < http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html > Acesso em 7 de março de 2015.
[22] Relatório de Privacidade do Departamento de Saúde e Serviços Humanos dos Estados Unidos – 2006-2008. Definições de privacidade, confidencialidade e segurança publicados pelo Instituto de Medicina, no estudo "Disposição do Estudo de Saúde da Força Aérea" (2006). Disponível em <http://www.cdc.gov/nchs/data/ncvhs/ncvhs06-08.pdf >Acesso em 16 de março de 2015.

divulgação de informações de saúde individualmente identificáveis, prevendo penalidades civis e criminais para as violações. Ao mesmo tempo, a regra de privacidade é equilibrada de modo que permite a divulgação de informações de saúde necessários para o atendimento ao paciente e outros fins importantes. Aborda também o uso e divulgação de "informações de saúde protegidas" de um paciente por planos de saúde, prestadores de serviços médicos, e câmaras de compensação, também chamado de "entidades abrangidas". As "entidades abrangidas", que geralmente têm interação direta com o paciente, são os agentes primários que capturam informações de saúde do paciente para uma variedade de fins, incluindo tratamento, pagamento, gerenciamento de operações de saúde, ou de investigação clínica.[23]

A HIPAA abrange apenas as entidades que prestam cuidados de saúde (por exemplo, hospitais, clínicas e médicos) ou que lidam com o pagamento (por exemplo, companhias de seguros, operadoras de saúde), mas não outras entidades, como colegas de trabalho que executam uma variedade de serviços (por exemplo, gestão de sinistros ou de contabilidade) para hospitais e médicos, ou prestadores de serviços como Google Health ou Microsoft HealthVault.

Entidades abrangidas que detêm informações de saúde protegidas (*protected health information* – PHI) podem usá-las sem o consentimento de um indivíduo para fins de fornecimento de tratamento para o indivíduo. No entanto, a autorização assinada do paciente é necessária para usar a sua PHI para outras atividades, tais como marketing, pesquisa, ou captação de recursos (AVANCHA, BAXI e KOTZ, 2012, pág. 8).

As Regras de Privacidade HIPAA são regulamentos complexos expressos em inglês legal, e continua a ser um desafio interpretar estas regras e implementá-los em sistemas de *workflow* e de informação clínica. Vários pesquisadores têm desenvolvido métodos formais para extração de regras precisas a partir da linguagem de regulamentação, de forma que possam orientar os engenheiros de software que executam tais sistemas (BARTH et al. 2006; BREAUX e ANTON, 2008).

Já as tecnologias vestíveis, ubíquas, como às ligadas em redes do tipo WBAN, são utilizadas fora do contexto clínico, e por isso, as proteções legais da HIPAA podem não se aplicar. Ainda não está claro, por exemplo, se os registros de WBAN ou algum aplicativo *mobile health* armazenado em um telefone celular ou em um Registro do paciente (prontuário médico, por exemplo), podem ser sujeitas a inspecção por agentes de aplicação da lei que obtiverem um mandado de busca. Avancha, Baxi e Kotz (2012) alertam que as informações

[23] <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html >Acesso em 12/03/2015.

arquivadas no registro do paciente ou no celular, com dados de sua localização no último ano, por exemplo, com monitoramento de registros cardíacos, poderia interessar a um laboratório forense investigando um crime, que poderia verificar a localização do monitorado no momento do crime, além de averiguar o ritmo cardíaco no momento do crime. Seria também uma informação de interesse para os departamentos de marketing das empresas, que poderiam associar a oscilaçao cardíaca ao dia a dia, estudando comportamentos de consumo, por exemplo. No caso de registros de redes WBAN, os levantamentos realizados para produção deste artigo apontaram que não há legislação que proteja estas informação e a privacidade individual do monitorado nos Estados Unidos.

5 Considerações finais

Os desafios da preservação do direiro à privacidade nos dispositivos WBAN, tanto à luz da legislação brasileira como da americana estão evidentes, uma vez que os avanços tecnológicos tem evoluído tão mais rapidamente que o ordenamento jurídico.

O compartilhamento de informações geraradas a partir de dispositivos ligados à redes WBAN (*wireless body area network*) gera uma grande oportunidade assistencial e de manutenção da vida, ao mesmo passo que pode ser considerada uma barreira ao desenvolvimento de projetos desta natureza diante da fragilidade legislativa da proteção do direito à privacidade da informação do monitorado. Há que se pontuar a evolução alcançada no Brasil com a regulamentação do Marco civil da internet no ano de 2014, e a que está por vir com a aprovação da Lei de proteção de dados pessoais, importantes para proteção da privacidade dos brasileiros.

Contudo, considerando a legislação existente sobre privacidade no Brasil, 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.

Os Estados Unidos possuem uma legislação muito mais robusta e abrangente que a brasileira, porém sem abordar especificamente as questões de dispositivos móveis de saúde – no país, a maior parte das leis e regulamentos que se aplicam aos cuidados de saúde estão focadas no ambiente clínico, e uma vez que muitos aplicativos móveis, como os das redesWBAN são utilizados fora do ambiente clínico, tais dados ficam descobertos pelas normas vigentes.

Pelo fato de dispositivos de redes WBAN serem, por característica, móveis, eles “andam” com o monitorado, que pode deslocar-se de um país para o outro, fazendo com que o

monitorado viajante encontre uma variedade de quadros jurídicos (AVANCHA, BAXI e KOTZ, 2012). Tal questão aponta para a importância do desenvolvimento de normas jurídicas internacionais para proteger os monitorados por WBAN que viagem por países com padrões mais baixos de privacidade do que o seu país de origem lhes garante.

A Organização Mundial da Saúde (2011) ressalta que os países em processo de desenvolvimento de políticas e legislação de saúde como o Brasil devem preocupar-se em incluir e-saúde e *m-health* no âmbito das suas políticas, uma vez que um campo é uma extensão do outro e as ações, políticas, considerações legais e soluções técnicas são praticamente as mesmas.

É preciso avançar mais rapidamente na regulamentação de tais questões, especificamente as de saúde, incluindo regulamentações sobre informações trafegadas por redes de dispositivos móveis e vestíveis, como a WBAN, de forma que os brasileros que adquirirem e usarem tais produtos, além de beneficiarem-se com a possibilidade de acesso rápido ao socorro e monitoramento constante, resultando num cenário de sobrevida com maior qualidade para pacientes crônicos e familiares, tenham seu direito à privacidade garantido, impossibilitando que tornem-se reféns de suas próprias informações e dados pessoais.

6 Referências

AL AMEEN, Moshaddique; LIU, Jingwei; KWAK, Kyungsup. **Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications**. J Med Syst, 36:93–101, 2012.

ALMEIDA, Daniela Lima de. **Alimentação adequada como direito fundamental: desafios para garantir a efetivação**. Revista Internacional de Direito e Cidadania. n.º 8, p. 55-70, out/2010.

ARAÚJO, Alexandra Maria Rodrigues, OLIVEIRA, José Sebastião De. A **transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação no direito da união europeia**. Direito e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI/UFPB; coordenadores: Aires José Rover, José Renato Gaziero Cella, Fernando Galindo Ayuda. – Florianópolis: CONPEDI, 2014.

ARAÚJO, R. B. (2003). **Computação Ubíqua: Princípios, Tecnologias e Desafios. In: Simpósio Brasileiro de Redes de Computadores**. (Org.). Computação Ubíqua: Princípios, Tecnologias e Desafios. 1 ed. Natal - RN: SBRC2003, p. 45 - 115.

ARSHNEY, U. 2007. **Pervasive healthcare and wireless health monitoring**. Mobile Netw. Appl. 12, 2-3, 113–127. DOI 10.1007/s11036-007-0017-1.

AVANCHA, S., BAXI, A., and KOTZ, D. Privacy in mobile technology for personal healthcare. ACM Comput. Surv. 45, 1, Article 3 (November 2012), 54 pages, 2012.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo: Saraiva, 1989, vol. 2, p. 63.

BAKER, C. R., ARMIJO, K., BELKA, S., BENHABIB, M., BHARGAVA, V., BURKHART, N., DER MINASSIANS, A., DERVISOGLU, G., GUTNIK, L., HAICK, B. M., HO, C., KOPLOW, M., MANGOLD, J., ROBINSON, S., ROSA, M., SCHWARTZ, M., SIMS, C., STOFFREGEN, H., WATERBURY, A., LELAND, E. S., PERING, T., AND WRIGHT, P. K. 2007. **Wireless sensor networks for home health care**. In Proceedings of the International Conference on Advanced Information Networking and Applications Workshops. IEEE Computer Society, 832–837, 2007.

BARAKAH, D. M., AMMAD-UDDIN, M. **A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture**. Third International Conference on Intelligent Systems Modelling and Simulation, 2012.

BANCO MUNDIAL. **Envelhecendo em um Brasil mais velho**. Washington DC: Banco Mundial, 2011.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 5a ed. Rio de Janeiro: Forense Universitária, 2001, pp. 64-65.

BOBBIO, Norberto. **A Era dos Direitos**. Rio de Janeiro, Campus, 1992.

BOLSONI, E.P., CARDOSO, C., MEDEIROS DE SOUZA, C.H. **Computação Ubíqua, Cloud Computing e PLC para Continuidade Comunicacional diante de Desastres**. V Seminário Internacional de Defesa Civil – DEFENCIL, São Paulo, 2009.

BORIC-LUBECKE, O, LUBECKE, V. M. **Wireless house calls: using communications technology for health care and monitoring**. IEEE Microwave Magazine 3, Vol.3, pág. 43–48, 2002.

BOSSOI, Roseli Aparecida Casarini. **A proteção dos dados pessoais face às novas tecnologias**. Direito e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UFSC; coordenadores: Aires José Rover, José Renato Gaziero Cella, Fernando Galindo Ayuda. – Florianópolis: CONPEDI, 2014.

BRASIL, Ministério da Saúde. **Vigitel Brasil 2011: Vigilância de fatores de risco e proteção para doenças crônicas por inquérito telefônico**. Brasília – DF, 2012.

_____, Ministério da Saúde, Comitê de Informação e Informática em Saúde (CIINFO). **Política Nacional de Informação e Informática em Saúde,** 2013.

_____, Ministério da Saúde. Portaria nº 940, de 28 de abril de 2011. **Regulamenta o Sistema Cartão Nacional de Saúde (Sistema Cartão)**, 2011.

_____, Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. **Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar**, 2011.

_____. Lei n° 12.965, de 23 de abril de 2014. **Estabelece princípios, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União. Seção 1, de 24 de abril de 2014. p.1-3. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em 2 de março de 2015.

BRENDER, J., NOHR, C., MCNAIR, P. **Research needs and priorities in health**

informatics. International Journal of Medical Informatics; 58: 257-289, 2000.

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

CAVALCANTE FILHO, João Trindade. **Teoria geral dos direitos fundamentais**. 2015.

CHRISTENSEN, H., BARDRAM, J., **Pervasive Computing Support for Hospitals: "An overview of the Activity-Based Computing Project"** In: IEEE Pervasive Computing, vol. 6, issue 1, p. 44-51, 2007.

COHN, S. P. **Privacy and confidentiality in the nationwide health information network**. 2006.

COMPARATO, Fábio Konder. **A afirmação histórica dos Direitos Humanos**. 2 ed. São Paulo: Saraiva, 2001.

COSTA Jr., Paulo José da. **O direito de estar só: tutela penal da intimidade**. São Paulo: RT, 1995.

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

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

IBGE. **Síntese de indicadores sociais: Uma análise das condições de vida da população brasileira 2014**. Rio de Janeiro, 2014.

IBGE, Tábua Completa de Mortalidade 2013. Disponível em ftp://ftp.ibge.gov.br/Tabuas_Completas_de_Mortalidade/Tabuas_Completas_de_Mortalidade_2013/pdf/ambos_pdf.pdf Acesso em 2 de março de 2015.

LEITHARDT, V. R. Q. et al, **Uma Proposta de Classificação de Dados para Gerenciamento de Privacidade em Ambientes Ubíquos Utilizando o Modelo UbiPri**. Nuevas Ideas en Informática Educativa TISE, 2014.

MACHADO, A., LIBRELOTTO, G. R., AUGUSTIN, I. **Ferramenta para definição de contexto pelo usuário-final na programação de tarefas clínicas em um sistema de saúde pervasivo**. Anais do XXX Congresso da Sociedade Brasileira de Computação (SBC), Belo Horizonte, 2010.

MORAES, Alexandre de. **Direitos humanos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. 3. ed. São Paulo: Atlas, 2000. 320 p. (Temas jurídicos v. 3)

MORRIS, L., TAYLOR, MW., HUNTER, C., CAMPBELL, L.M. **Information management in primary care: delivering a strategy to improve patient care in Scotland**. Informatics in Primary Care, 10:85-8, 2002.

NASRI, F. **O envelhecimento populacional no Brasil**. Einstein, v. 6, 2008.

RINDFLEISCH, T. C. **Privacy, information technology, and health care**. Communications of the ACM, v. 40, n. 8, p. 92-100, 1997.

ROBL FILHO, Ilton Norberto. **Direito, intimidade e vida privada: uma perspectiva histórico-política para uma delimitação contemporânea**. Revista Eletrônica do CEJUR, v. 1, n. 1, ago./dez. 2006

ROSARIO, Mauricio de Souza. **A segurança das informações em saúde sob responsabilidade do DATASUS: uma análise com enfoque na privacidade e na confidencialidade**. Dissertação (Mestrado) – Escola Nacional de Saúde Pública Sergio Arouca. Rio de Janeiro, 2010.

ROSSONI, Carolina, BOLESINA, Iuri, **A teoria dos círculos concêntricos e a proteção à vida privada: análise ao caso von hannover vs. alemanha, julgado pela corte europeia de**

direitos humanos. XI Seminário Internacional de demandas sociais e políticas públicas na sociedade contemporânea. VII Mostra de trabalhos jurídicos científicos, 2014.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte**, p. 254. 1998.

UNITED NATIONS. **World population prospects: The 2010 revision and world urbanization prospects: The 2011 revision**. 2014.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Dissertação curso de pós-graduação *stricto sensu* em Direito, Estado e Sociedade: Políticas Públicas e Democracia da Universidade de Brasília, 2007.

QUEIROZ, Ana Carolina S., BARBOSA, Antonio Pires. **Racionalidade e Incorporação de Tecnologia em Saúde: A Experiência de um Hospital de alta complexidade em São Paulo**. RAE-eletrônica, Volume 2, Número 1, jan-jun/2003.

RIGBY, M. **The management and policy challenges of the globalization effect of informatics and telemedicine**. Health Policy, 46(2):97-103, 1999.

SANTOS, Antonio Jeová. **Dano moral na internet**. São Paulo: Método, 2001.
United Nations. **World Urbanization Prospects The 2014 Revision**. New York, 2014.

VARSHNEY, U. **Pervasive healthcare and wireless health monitoring**. Mobile Netw. Appl. 12, 2-3, 113–127, 2007.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Dissertação curso de pós-graduação stricto sensu em Direito, Estado e Sociedade: Políticas Públicas e Democracia da Universidade de Brasília, 2007.

Weiser, Mark. **The Computer for the 21st Century**. Scientific American Ubicomp, vol. 265, no. 3, pp. 66–75, 1991.

WINIKES, Ralph, CAMARGO, Rodrigo Eduardo. **A Concepção de vida privada e de intimidade no direito brasileiro**. Direito civil [Recurso eletrônico on-line] / organização CONPED/UFF; coordenadores: Celia Barbosa Abreu, Elcio Nacur Rezende, Roberto Senise Lisboa. Florianópolis: FUNJAB, 2012.

WOLKOWSKA, Wiktoria, ZIEFLE, Martina. **Perception of Privacy and Securuty for Acceptance of E-health Technologies**. International Conference on Pervasive Computing Technologies for Helthcare (Pervasive-Heath) and Workshops, German, 2011.

WORLD HEALTH ORGANIZATION. **mHealth New horizons for health through mobile technologies: Based on the findings of the second global survey on eHealth**. (Global Observatory for eHealth Series, 3). Geneva: World Health Organization, 2011. Disponível em: <http://www.who.int/goe/publications/goe_mhealth_web.pdf>Acesso em 10 de março de 2015.