

Dimensões da privacidade das informações em saúde

Issues in healthcare data privacy

Dimensiones de la privacidad de la información en salud

Tania Margarete Mezzomo Keinert ¹
Carlos Tato Cortizo ¹

doi: 10.1590/0102-311X00039417

“...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” (Constituição Federal de 1988, art. 5º, inciso X).

A privacidade das informações em saúde é um tema contemporâneo, dado que são escassas as análises sobre privacidade nas práticas em saúde que se utilizam das novas tecnologias de informação e comunicação (TICs). Trata-se de um direito fundamental, baseado no princípio constitucional da dignidade da pessoa humana, ainda pouco disseminado ^{1,2}.

A reflexão parte da constatação de que vivemos hoje na chamada “Sociedade da Informação”, baseada nos grandes desenvolvimentos das TICs, na qual se multiplicaram, de forma exponencial, a velocidade e a quantidade de dados pessoais circulando em formato digital, nem sempre protegidos o suficiente para garantir privacidade ³.

Também, assume-se que existe uma “Sociedade do Risco”, em que o desenvolvimento das ciências e das técnicas não consegue dar conta de sua predição e controle. Isso gera consequências graves para a saúde humana ⁴.

O contexto em que se insere a discussão sobre a privacidade demonstra, paradoxalmente, que essas mesmas tecnologias propiciam a ampliação e o surgimento de novas experiências e práticas do exercício da cidadania. Por meio das TICs, há também a possibilidade de criação de inovações sociais, por meio das redes comunicacionais, da criação do ciberespaço e da cibercultura ^{5,6}.

A privacidade, porém, é seriamente ameaçada pela chamada “Sociedade da Vigilância”, baseada na mediação computacional constituída por mecanismos de extração, mercantilização e controle de dados que efetivamente retiram das pessoas o controle sobre suas próprias informações. O capitalismo de vigilância desafia as normas democráticas, pois cresce o interesse, tanto dos governos quanto da iniciativa privada, em relação ao acesso a informações pessoais, com reflexos evidentes na privacidade ^{7,8}.

A problemática da privacidade tem, nesse contexto, três grandes dimensões passíveis de análise: a normativa, a político-cultural e a tecnológica. Em relação ao enfoque normativo, verificou-se a necessidade de inovar e consolidar as normas em um corpo legislativo sistêmico. Quanto ao aspecto tecnológico, apontamos a necessidade de elevar a segurança, com a aquisição de sistemas operacionais, gerenciadores de bancos de dados, desenvolvimento de softwares seguros e anonimização de registros. A abordagem comportamental põe em foco a fundamental importância da formação técnico-tecnológica e político-ética de prestadores de serviços, gestores, profissionais e usuários ^{2,9,10,11}.

¹ Núcleo de Economia e Tecnologia em Saúde, Instituto de Saúde, São Paulo, Brasil.

Correspondência

T. M. M. Keinert
Rua Santo Antonio 590,
2º andar, São Paulo, SP
01314-000, Brasil.
taniak@isaude.sp.gov.br



Este é um artigo publicado em acesso aberto (Open Access) sob a licença Creative Commons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições, desde que o trabalho original seja corretamente citado.

Proteger juridicamente a privacidade significa garanti-la como direito fundamental baseado no princípio constitucional da dignidade da pessoa humana. Evitar o vazamento total ou parcial de informações sobre a saúde das pessoas é neutralizar seu potencial discriminatório ^{2,12}. Já em 2005, o relator especial sobre o direito à saúde da Organização das Nações Unidas (ONU), ao propor uma “estrutura analítica do direito à saúde”, alertava para a necessidade de não discriminação, igualdade e proteção à vulnerabilidade de certos grupos, como, por exemplo portadores de HIV ou de doenças mentais ¹³.

O uso de TICs para mediar a atenção à saúde é denominado de e-Saúde (*e-Health*). A terminologia, adotada pela Organização Mundial da Saúde (OMS), inclui assistência ao paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde. De modo mais específico, processos de e-Saúde incluem o Cartão Nacional de Saúde implantado no Sistema Único de Saúde (SUS), teleconsultorias, telediagnóstico, segunda opinião clínica, telecirurgia, telemonitoramento, televigilância, educação permanente, teleducação e prontuário eletrônico ¹¹.

Existe hoje uma extensão do corpo físico formada pelos dados pessoais que circulam virtualmente, constituindo uma espécie de “avatar” ou “corpo eletrônico” ao qual deveria ser estendida a tutela da personalidade “virtual” dos pacientes como derivação do próprio princípio da dignidade da pessoa humana ⁷.

A cidadania eletrônica envolve o direito à autodeterminação informativa, uma vez que os dados pertencem à pessoa e não às instituições que os coletam. Dados pessoais são aqueles em que o objeto da informação é a própria pessoa, sendo considerados dados sensíveis aqueles que, se revelados, podem discriminar ou lesar o indivíduo e até mesmo a sociedade. Os dados de saúde são considerados dados sensíveis ^{1,2,7,10,11}.

No setor privado, a Agência Nacional de Saúde Suplementar (ANS) estabeleceu um padrão obrigatório para a troca de informações entre operadoras de planos de assistência à saúde e prestadores de serviço, que foi denominado Padrão TISS (Troca de Informações na Saúde Suplementar). Um de seus componentes é o da segurança e privacidade, que prevê os requisitos para proteção dos dados.

No SUS, na 14ª Conferência Nacional de Saúde (CNS, 2012), as temáticas privacidade, sigilo e confidencialidade das informações em saúde ainda não foram contempladas na diretriz 12, destinada a construir uma Política de Informação e Comunicação.

O Plano Nacional de Saúde 2016-2019, aprovado pelo Conselho Nacional de Saúde, apoia a promoção de ações para assegurar a preservação dos aspectos éticos, de privacidade e de confidencialidade em todas as etapas do processamento das informações.

Na Política Nacional de Informação e Informática em Saúde (PNIIS, 2016), foram estabelecidos alguns princípios com vista a garantir a confidencialidade, o sigilo e a privacidade da informação de saúde pessoal como direito de todo indivíduo.

Pelo exposto, conclui-se que há, efetivamente, fragilidades na garantia à privacidade, ao sigilo e à confidencialidade das informações em saúde. No entanto, há iniciativas em andamento, para consolidar a legislação, desenvolver tecnologias mais seguras, implementar cursos de formação ético-profissional e ampliar a participação social.

Não há no Brasil, porém, legislação específica de proteção de dados pessoais. Há um anteprojeto de lei, em discussão, que prevê normas específicas sobre dados sensíveis. Ressaltamos a importância do chamado “Princípio da Precaução”, que prevê a inversão do ônus da prova, ou seja, quem pratica a ação que pode causar danos individuais ou coletivos deve apresentar as provas. Nos Estados Unidos, por exemplo, existe a HIPAA (*Health Insurance Portability and Accountability Act*), que visa a proteger toda informação pessoal utilizada na prestação de serviços de saúde.

Na dimensão tecnológica, há a adoção de criptografia forte, centrais comutadoras e roteadores fiscalizados, homologados e livres de programas espíões, com vista a aumentar a transparência e a segurança das informações em saúde. A utilização de softwares livres, ainda, contribui para aumentar a governabilidade sobre os códigos-fonte dos programas utilizados no processamento das informações em saúde ¹⁴.

Faz-se necessário, ainda, investir em formação ético-política, técnico-tecnológica, bem como em legislação profissional específica e relacionada aos Direitos Humanos e Fundamentais. A ampliação da participação social e a educação permanente podem auxiliar na produção de respostas urgentes às questões aqui expostas ¹⁵.

Para evitar o acesso indevido aos dados pessoais, faz-se necessária uma política de administração dessas informações, a fim de evitar sua manipulação descuidada, o que facilita sua difusão pública, quer acidental, quer intencional. Na Itália, por exemplo, há uma autoridade de proteção de dados pessoais denominada “Garante”. No Brasil, faz-se necessária a criação de um órgão regulador com características de agência independente, com participação da sociedade civil ^{7,10,11}.

Destaque-se, ainda, a importância da correta utilização do Termo de Consentimento Livre e Esclarecido (TCLE) nas pesquisas envolvendo seres humanos, bem como a elaboração de protocolos específicos para a proteção à privacidade dos usuários de serviços de saúde ¹².

Colaboradores

Ambos os autores participaram igualmente em todas as etapas da produção do texto.

1. Moraes IHS. Prefácio. In: Keinert TMM, Sarati FM, Cortizo CT, Paula SHB, organizadores. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde; 2015. p. 9-20.
2. Sarlet IW. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. 9ª Ed. Porto Alegre: Livraria do Advogado Editora; 2015.
3. Machlup F. The production and distribution of knowledge in the United States. Princeton: Princeton University Press; 1962.
4. Beck U. Sociedade de risco. Rumo a uma outra modernidade. 2ª Ed. São Paulo: Editora 34; 2011.
5. Castells M. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar Editora; 2003.
6. Lèvy P. Cibercultura. 3ª Ed. São Paulo: Editora 34; 2010.
7. Rodotà S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar; 2008.
8. Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology 2015; 30:75-89.

9. Moraes IHS, Gómez MNG. Informação e informática em saúde: caleidoscópio contemporâneo da saúde. *Ciênc Saúde Coletiva* 2007; 12:553-65.
10. Doneda D. Da privacidade à proteção dos dados pessoais. Rio de Janeiro: Renovar; 2006.
11. Kameda K. e-saúde e desafios à proteção da privacidade no Brasil. https://www.politics.org.br/sites/default/files/downloads/poliTI-Cs_16.pdf (acessado em 05/Abr/2017).
12. Sarlet IW, Keinert TMM. O direito fundamental à privacidade e as informações em saúde: alguns desafios. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB, organizadores. *Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética*. São Paulo: Instituto de Saúde; 2015. p. 113-45.
13. Naciones Unidas. Los derechos economicos, sociales y culturales. Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental, Sr. Paul Hunt. <http://daccess.ods.un.org/access.nsf/Get?Open&DS=E/CN.4/2005/51&Lang=S>.
14. 'Cortizo CT. Sistemas de informática e informação da atenção básica do Sistema Único de Saúde e o software livre: possibilidades e perspectivas [Dissertação de Mestrado]. São Paulo: Faculdade de Saúde Pública, Universidade de São Paulo; 2007.
15. Moraes IHS. *Política, tecnologia e informação em saúde: a utopia da emancipação*. Salvador: Casa da Qualidade Editora; 2002.

Recebido em 07/Abr/2017
Aprovado em 30/Nov/2017