ISSN: 2594-6153

Proteção de dados pessoais como direito fundamental na área da saúde e suas implicações para os profissionais médicos no Brasil cotejando aspectos do direito comparado na União Europeia e na China

José Carlos Massarelli Jr., Verônica Scriptore Freire e Almeida

Universidade Universidade Santa Cecília (UNISANTA), Santos-SP, Brasil
Mestrado em Direito da Saúde

E-mail: massarelli_direito@yahoo.com.br

Resumo: Neste trabalho apontamos alguns aspectos sobre a responsabilidade do médico na proteção dos dados do paciente e suas implicações em relação a responsabilidade civil deste profissional, fizemos uma comparação da legislação nacional com algumas legislações internacionais, apontando alguns aspectos relevantes relacionados à responsabilidade dos profissionais. Foi demonstrado que a responsabilidade do médico, neste aspecto, é objetiva, segundo a Lei de Proteção de Dados e como isto afeta a situação jurídica do profissional da saúde na gestão dos dados pessoais de seus pacientes.

Palavras-chave: proteção de dados; responsabilidade civil; responsabilidade objetiva; profissional da saúde; dados pessoais sensíveis.

Protection of personal data as a fundamental right in health and its implications for medical professionals in Brazil comparing aspects of comparative law in the European Union and China

Abstract: In this paper, we point out some aspects about the responsibility of the physician in the protection of patient data and its implications in relation to the civil liability of this professional. We made a comparison of national legislation with some international legislation, pointing out some relevant aspects related to the liability of professionals. It has been shown that physician responsibility in this regard is objective under the Data Protection Act and how this affects the legal status of the healthcare professional in the management of his patients' personal data.

Keywords: data protection; civil responsability; objective responsibility; Health professional; sensitive personal data.

Introdução

As alterações tecnológicas em nosso mundo têm causado inúmeras transformações sociais, desde o escândalo da *Cambridge Analytica* que foi denunciado por Carole Cadwalladr e Emma Graham-Harrison, no *The Guardian* [1], em que as eleições norte americanas foram, supostamente, manipuladas, resultando em uma multa de U$ 5 milhões de dólares ao Facebook [2] pela utilização de dados pessoais sem autorização e, em uma corrida para regular, delimitar, proteger e punir a utilização dos dados pessoais em países com maior consciência tecnológica.

ISSN: 2594-6153

No Brasil, foi aprovada em 2018, a Lei Geral de Proteção de Dados [3], bem como na Comunidade Europeia, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho [4] e, atualmente, existe um projeto de lei na China, a Lei Básica da Saúde e Promoção da Saúde [5], que já aponta para a proteção dos dados médicos, todos estes dispositivos implementam severas multas pecuniárias para as infrações cometidas.

Neste contexto, temos o profissional da saúde, que se utiliza dos meios tecnológicos para uso na telemedicina [4, 5] e transmite e/ou utiliza os dados, para aprimorar suas técnicas e aferir resultados diante das informações processadas pelos dados dos pacientes [6], bem como, para produzir e arquivar prontuários, que são obrigatórios e sigilosos nos termos do Código de Ética do Conselho Federal de Medicina [7].

Os dados dos pacientes são considerados, pela LGPD e pela Comunidade Europeia [3, 4], como dados pessoais sensíveis[1], e têm ampliada a proteção quando não anonimizados[2].

Por força destas mudanças, é necessário o estudo da proteção que a lei aufere para os dados pessoais sensíveis no Brasil, na Comunidade Europeia e na China e seu impacto.

Objetivos

O presente estudo tem por objetivo verificar a responsabilidade civil aplicada aos profissionais da saúde na Lei Geral de Proteção de Dados e suas implicações na verificação da culpa, além de apontar a responsabilidade auferida na legislação nacional, na Comunidade Europeia e na nova legislação da China sobre saúde, relacionando a proteção de dados pessoais como Direito Humano Fundamental.

Material e Métodos

Este trabalho se utiliza de pesquisa exploratória de análise dedutiva como metodologia, buscando informações nas legislações relacionadas no Brasil, Europa e China, bem como pesquisas e livros publicados em meio eletrônico e físico.

Resultados

Os dados pessoais são considerados como Direitos Fundamentais, na Carta de Direitos Fundamentais da Comunidade Europeia [8] em seu artigo 8, que declara esta condição.

No Brasil, caminhamos para o mesmo status, porquanto existe uma proposta de emenda à Constituição Federal, PEC 17/2019, iniciada pelo Senado e que se encontra na

[1] São dados referente à saúde ou à vida sexual, dado genético ou biométrico, vinculados a uma pessoa natural.
[2] Anonimização é um novo termo utilizado para identificar o dado pessoal que não pode ser individualizado, por meio de técnicas reconhecidas até o momento do tratamento.

Câmara dos Deputados, com vista a inserir este status constitucional a esta proteção de dados no artigo 5º da CF, onde estão inseridos a maioria dos direitos fundamentais [9].

Já na China, a Lei Básica da Saúde e Promoção da Saúde fala em proteção de dados de forma subsidiária, pois na eventualidade de vazamentos de informações médicas, em seus artigos 99 e 104, implicará em responsabilidade civil e penal para os infratores [5].

Na Comunidade Europeia a responsabilidade civil sobre o tratamento dos dados pessoais é objetiva, sendo que, os dados devem estar disponíveis, para o titular de dados[3], a qualquer momento, incluindo a forma de tratamento, e os resultados obtidos neste tratamento, sendo que o titular de dados pode cancelar a disponibilização, limitar o tratamento e alterar estes dados de forma unilateral, conforme disposto nos artigos 15 a 19 do Reg. (UE) 2016/679 do Parlamento Europeu e do Conselho [4].

No Brasil, a LGPD, impôs o mesmo tratamento aos dados pessoais, sendo objetiva a responsabilidade dos agentes de tratamentos em relação aos dados do titular de dados e a disponibilidade destes dados é, igualmente, ampla, nos termos dos artigos, 8, 9 e 15 da lei [3].

Na China, embora não seja explicita a menção de responsabilidade objetiva, o texto do projeto de lei, não deixa margem para outro entendimento, ao aplicar a responsabilidade civil e penal sem impor quaisquer explicações sobre as formas de infringência da lei, conforme artigo 99 [5], entretanto, ainda não fala nada sobre a autonomia da vontade do titular de dados sobre os dados.

Todos estes dispositivos estão ampliando o grau de proteção dos dados das pessoas físicas, em relação aos dados pessoais, forjando o conceito de autodeterminação informática[4], por força dos acontecimentos já descritos [1, 2], que está em consonância como a Declaração Universal dos Direitos Humanos da ONU, em seu artigo 12 que informa proteger a vida privada contra intromissões arbitrárias [10], o que é facilmente associado ao que fora asseverado por Bioni e Machado da Luz [8, 9].

Na telemedicina, os dados dos pacientes são considerados como pessoais, conforme Resolução CFM nº 1.643/2002, devendo haver a necessária confidencialidade e privacidade no trato destas informações [11], confirmado pelo Código de Ética Médica em seus artigos, 85 (privacidade), 88, 89 e 90 (acesso livre), todos relacionados ao prontuário médico [7].

Discussão

[3] Titular de dados é a pessoa física que tem seus dados captados por qualquer meio, seja físico ou digital.
[4] Autodeterminação informática é a possibilidade da aplicação da autonomia da vontade sobre os dados pessoais.

ISSN: 2594-6153

A construção da ideia de dados pessoais como direito fundamental é não linear, conforme aponta Bioni [12], e tem seu maior argumento no processo de "humanização do direito privado", o que é reforçado pela ideia de privacidade que, conforme Machado da Luz [13], está intimamente ligada à proteção dos dados pessoais.

A amplitude da proteção no tratamento de dados pessoais tem sido crescente e, tende a ser, cada vez mais ampliada por conta da privacidade do titular de dados [3, 4, 5, 6].

A ampliação dos direitos relativos a proteção de dados pessoais e a autonomia da vontade do titular de dados, traz implicações diretas sobre o tratamento dos dados para os agentes de tratamento de dados [3, 4, 5, 8], bem como para os profissionais da saúde, porquanto, também são considerados como agentes de tratamento [6, 7] e, os dados utilizados pela telemedicina devem, com maior rigor, ser protegidos [13].

Este agente de tratamento de dados[5], profissional da saúde, tem responsabilidade objetiva sobre os dados pessoais captados tratados ou não [3, 4, 5] o que implica na retirada da culpa em eventual discussão jurídica sobre danos ao titular de dados, como um eventual vazamento de dados, isto é reforçado pelos regulamentos da própria profissão médica [7, 13].

Para Bioni [12] esta proteção tem fundamento na projeção que os dados pessoais têm sobre a personalidade da pessoa humana, porquanto o novo contexto social permite a identificação do que ele chama "signos identificadores", que possibilitam a identificação por pontos dispersos de uma personalidade e, sua possível, manipulação, o que me parece razoável dados os eventos descritos neste trabalho [1, 2] e tantos outros já documentados.

Neste sentido, os dados pessoais sensíveis são mais importantes pois permitem "identificar individualidades mais sensíveis das pessoas [...], a partir de informações triviais" [12], o que enche de significado a responsabilidade objetiva sobre o tratamento e guarda de tais dados [3, 4, 5], sendo desta forma a própria privacidade pessoal do titular de dados que se está protegendo, em consonância com a Carta de Direitos Humanos da ONU e do Regulamento (UE) 2016/679 [8, 10].

Conclusões

Concluímos que, embora a responsabilidade dos médicos, em regra, pelos seus procedimentos técnicos, seja subjetiva, estamos diante de um nivelamento da responsabilidade dos profissionais da saúde, quanto ao tratamento dos dados pessoais de seus pacientes, para a responsabilidade objetiva, prescindindo da culpa. Isto demandará uma

[5] Agente de tratamento de dados é o responsável tanto pelo tratamento como pela coleta e armazenamento dos dados do agente de dados (paciente).

atenção especial por parte destes profissionais em contratar empresas de captação e tratamento de dados dos seus pacientes, porquanto, poderá ser responsabilizado pelo vazamento ou mau uso destes dados.

Referências

1. Cadwalladr C., Graham-Harrison E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. 17 mar 2018; The Guardian - The Cambridge Analytica Files. Acesso em 20 de setembro de 2019. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
2. Pozzi, S. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. Nova York - 13 JUL 2019. El País – Economia. Acesso em 20 de setembro de 2019. Disponível em: https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html.
3. Brasil. Presidência da República. Lei 1379 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra. Acesso em 20 de setembro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.
4. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Acesso em: 15 de setembro de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX: 32016R0679;
5. NPC Observer. Basic Healthcare and Health Promotion Law. NPCSC deliberation – 3rd round: August 2019 (Chinese only). Acesso em: 10 set. 2019. Disponível em: https://npcobserver.com/lawlist/basic-healthcare-and-health-promotion-law/.
6. Gusarova, A.. Data Protection in Telemedicine. SHS Web of Conferences. (2012). 2. 10.1051/shsconf/20120200013. Acesso em: 10 set. 2019. Disponível em: https://www.researchgate.net/publication/278116564_Data_Protection_in_Telemedicine/fulltext/57c786c908aefc4af34c83ce/Data-Protection-in-Telemedicine.pdf.
7. CFM. Resolução CFM nº 2.217/2018. Aprova o Código de Ética Médica. Acesso em: 01 set. 2019. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2217;
8. União Europeia. Carta dos Direitos Fundamentais da União Europeia. 2012/C 326/02. Acesso em: 20 de setembro de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT.
9. Brasil. PEC 17/2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Acesso em 25 de setembro de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594.
10. ONU. Declaração Universal de Direitos Humanos. Acesso em 28 de setembro de 2019. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por.
11. CFM. Resolução CFM nº 1.643/2002. Define e disciplina a prestação de serviços através da Telemedicina. (RESTABELECIDA pelo CFM nº 2.228/2018). Acesso em: 01 set. 2019. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643;

12. Bioni, B. R.. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. ISBN 978-85-309-8328-4.
13. Machado da Luz, P. H.; Battaglin Loureiro, M. F. Privacidade e Proteção de Dados Pessoais: Os novos desafios na sociedade em rede. Meritum: Revista de Direito da Universidade FUMEC, [s. l.], v. 13, n. 1, p. 69–86, 2018. Acesso em: 14 set. 2019. Disponível em: http://www.fumec.br/revistas/meritum/article/view/5811/pdf.