ISSN: 2594-6153

Da Cybersegurança para Proteção de Dados de Pacientes

Roberto Bortman, Roberto Luiz Pardini Ferreira de Almeida, Karen Patella

Universidade Santa Cecília (UNISANTA), Santos-SP, Brasil
Email: bortman.rb@gmail.com

Resumo

Os dados de pacientes, constantes de prontuários médicos eletrônicos, contém dados, que se violados, podem acarretar danos irreparáveis tanto aos hospitais quanto aos pacientes em seus direitos de personalidade. A Legislação Brasileira possui instrumentos para efetivar a proteção dos dados, com o objetivo de tornar mais seguro a proteção desses dados. Concluiu-se que a legislação é suficiente pata tutelar e proteger direitos quanto a violação de dados , mas a fiscalização e controle ainda precisam de melhorias.

Palavras Chave: Saúde, Direito, Cybersegurança, Proteção.

Cybersecurity Technologies for Protection of Patient Data

Abstract

Patient data, contained in electronic medical records, contain data that, if violated, can cause irreparable damage to both hospitals and patients in their personality rights. The Brazilian Law has instruments to effect the protection of data, with the purpose of making the protection of such data safer. It was concluded that the legislation is sufficient to safeguard and protect rights regarding data breach, but enforcement and control still need improvement.

Key-Words: Health, Law, Cybersecurity, Protection.

Introdução

A vida moderna permitiu o avanço técnologico, que, por sua vez, gerou novas ferramentas para facilitar a vida das pessoas, especialmente na área da saúde. A tecnologia trouxe inúmeras possibilidades para o registro de dados e tratamentos dos pacientes.

Hoje utiliza-se até mesmo a robótica para a realização de cirurgias de alta complexidade.Contudo, como nem tudo está incolume de riscos, os dados digitais das pessoas no âmbito da rede mundial de computadores, também, estão sujeitos á violações de terceiros, os quais podem interceptar ou mesmo furtar esses dados pessoais, para fins de realização de fraudes ou outros escusos, assim como falsificar protocolos eletrônicos, gerando consequências danosas tanto ao prestador de serviços quanto ao consumidor de produtos e serviços.

O avanço tecnológico trouxe novas ferramentas para a prestação de serviços por

hospitais, clínicas e laboratórios, na rede mundial de computadores, tornando mais prática e agil a vida moderna, sendo que sem mecanismos eficientes de proteção digital, esses dados ficam vulneráveis, podendo tornar-se alvos de ataques dos denominados *hackers,* os quais se pode dar através da utilização de ramsonwares e trojans.

Objetivos

A pesquisa objetivou estudar a necessidade de estudar se a legislação brasileira é suficiente e eficiente para garantir a cybersegurança da base de dados existentes nas plataformas existentes na rede mundial de computadores.

Nesse contexto, procurou-se responder as seguintes questões: a Legislação Brasileira garante a cybersegurança dos pacientes? Ela obriga hospitais, clínicas e médicos, a ter algum tipo de cuidado especial para proteger os dados?

Metodos

A metodologia escolhida foi uma revisão bibliográfica e pesquisa de base de dados de normas, regulamentos, livros, teses, monografias, existentes na rede mundial de computadores, afim de se produzir texto dialético.

Resultados

A globalização trouxe a possibilidade dos povos fazerem negócios simultaneamente por meio do comércio eletrônico, que reduziu barreiras e tornou mais prático tal ato. Além disso, tinha por escopo estabelecer uma legislação padrão para o compartilhamento eletrônico de dados e seus meios conexos de transmissão de dados.

Acompanhando a evolução da rede mundial de computadores, a medicina tem também gradativamente tem se apropriado das novas tencologias, obtendo grandes conquistas na utilização de suas várias ferramentas . Com o passar do tempo, as inovações nessa área vem aumentando, citando-se por exemplo, desde de tecnologias para imagens e novos fármacos, formas terapeuticas e de gerenciamento de dados médicos.

A Intenet tem sido o elemento catalizador dessa evolução, seja para divulgar as novas tecnologias e novidades, seja para buscar inovações e aumentar as ferramentas disponíveis para a área da saúde.

A área da saúde, como qualquer segmento produtivo e de serviços, como se disse acima, seguiu no mesmo rumo e passou a operar na área digital, dentre elas: com a crição

de prontuários médicos eletrônicos, controles de saúde remoto, a telemedicina e entre outros.

A tele medicina, por exemplo, possibilita que médicos de diferentes localidades possam realizar uma conferência virtual para analisar em conjunto um caso específico. Atualmente, o Sistema Único de Saúde (SUS) vem se utilizando desse mecanismo para determinados casos, como forma de atender ao Princípio de Atendimento Integral e a prevenção da saúde.

A pesquisa concluiu que a legislação brasileira, apesar de vasta, é totalmente ineficaz na proteção, em razão da falta de uma fiscalização mais eficiente e efetiva para inibir os ataques de cybercriminosos.

Nesse sentido, foi analisada a legislação sobre a segurança cibenética na internet, visando a proteção do governo, pessoas jurídicas e pessoas físicas, contratando-se que até o ano de 2000, não houve a produção de leis específicas a respeito.

Veja-se o quadro abaixo:

Decreto-lei no 2.848, de 7 de dezembro de 1940-Código Penal	Estabelece punições definidas para a violação de correspondência e crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial.
Constituição Federal de 1988	Artigos 5º, 23º, 37º e 216, aborda pontos relacionados à segurança da informação,
Lei nº 8.078, de 11 de setembro de 1990-Código de Defesa do Consumidor	Artigos 43 e 44, protege a integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados
Decreto 3.505, de 13 de Junho de 2000	Política de Segurança da Informação nos órgão da Administração Pública Federal
Medida Provisória nº 2.216-37, de 31 de agosto de 2001	Criou o Gabinete de Segurança Institucional-GSI, ligado à Presidência, alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998, com o objetivo de coordenar as atividades de segurança, integrando o Conselho de Defesa Nacional-CDN
Lei no 10.406, de 10 de janeiro de 2002-Código Civil	Os Artigos 927 e 932, responsabilidade do estado por danos -Má gestão de informações por órgãos e entidades da administração pública
Decreto nº 5.772, de 8 de maio de 2006	Criou o Departamento de Segurança da informação e Comunicações-DSIC
Decreto nº 6.703 de dezembro de 2008	aprovou a Estratégia Nacional de Defesa.
Decreto nº 7.411, de 29 de dezembro de 2010	Dispõe sobre a competência do Gabinete de Segurança Institucional da Presidência da República-GSI, para planejar e coordenar a execução das atividades de Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal
Decreto Presidencial nº 7.809 de 20 de setembro de 2012	Inclui, na Estrutura do Exército brasileiro, o Centro de Defesa Cibernética
Lei nº 12.737, de 30 de Novembro de 2012.	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Portaria Normativa nº 3.389, do Ministério da Defesa de 21 de dezembro de 2012	Aprova a Política Cibernética de Defesa
Lei nº 12.965, de 23 de Abril de 2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Lei nº 13.709, de 14 de Agosto de 2018.	Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Em 06 de julho de 2016, a imprensa noticiou que uma grave falha nos sistemas de segurança da Prefeitura de São Paulo, resultou na exposição de dados pessoais de centenas de milhares de pacientes da rede pública de saúde. Conforme noticiado a falha:

> {tornou público desde informações pessoais sobre os cidadãos cadastrados e servidores da Secretaria Municipal de Saúde até detalhes de prontuários médicos. Estima-se que as planilhas divulgadas erroneamente expuseram cerca de 650 mil pessoas da maior cidade brasileira}[6]

Como se sabe, os dados dos pacientes, estão protegidos por sigilo médico, resultando que o vazamento destes dados, torna os hospitais, clínicas e médicos responsáveis pelos danos causados pelo vazamento, do qual não se isentam se não se desincumbirem do ônus de provar que adotaram todas as medidas de segurnça para a proteção destes dados.

Um grande passo foi dado com a edição da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)[3] e da Lei nº 13.709, de 14 de Agosto de 2018[4], que Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) [3] , por outorgar competencia a autoridade nacional para quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, enviar informe com medidas cabíveis para fazer cessar a violação.(art. 31 e 32) e ainda tratando da responsabilidade civil pelos danos causados (Arts. 42 a 45), sujeitando ainda os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas da Lei, à pesadas sanções administrativas aplicáveis pela autoridade nacional.

A cibersegurança no Brasil deve ser objeto de investimento e de constante incentivo vistas ao aumento de efetiva fiscalização para o combate eficaz de ataques cibernéticos, que colocam os às hospitais, clinicas, pacientes/clientes, sob risco. Ou seja, a cibersegurança deve ser priorizada.

A tecnologia trazidas pelas empresas que se dedicam a exploração de comércio e de serviços na rede mundial de computadores, na área da saúde deve ser acompanhada de uma tecnologia de ponta na proteção e segurança de todos os seus bancos de dados, como forma de garantir os direitos personalíssimos do paciente, de extrema confidencialidade.

Portanto, a cibersegurança da rede mundial de computadores deve ser melhorada e constantemente atualizada para garantir a proteção dos dados pessoais dos pacientes. Para isso, deve haver uma fiscalização constante e eficaz para haver o cumprimento da Lei, que é vasta e suficiente para determinar a proteção dos dados pessoais.

Referencias Bibliográficas

1.Alves V F; Souza C G; Chrispino A e Ogasawara E. (2014), Segurança Cibernética e Políticas Públicas no Brasil, trabalho apresentado no XI Simpósio de Excelência em Gestão e Tecnológia, realizado em 22,23,24 de outubro de 2014 Disponível em: https://www.aedb.br/seget/arquivos/artigos14/38620415.pdf, Acesso em: 21/09/2018.

2.Agostinho D A, Leis de Segurança da Informação, Universidade Federal de Santa Catarina, http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/Trabalhos%202004-2/artigo LeisDeSeguranca.pdf, Disponível em:. Acesso em: 21/09/2018.

3.Brasil, Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), publicado no DOU de 24.4.2014, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.Acesso em: 21.09.2018

4.Brasil, Lei nº 13.709, de 14 de Agosto de 2018, disponível em: http://www.planalto.gov.br/CCIVil_03/_Ato2015-2018/2018/Lei/L13709.htm, publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra acesso em: 21.09.2018

5.Cutait, R. (2018), Privacidade na saúde, publicado em 23.02.2018, disponivel em: https://veja.abril.com.br/blog/letra-de-medico/privacidade-na-saude/, Acesso em 29.09.2018

6.Falha de Segurança Expõe dados de Milhares de pacientes do Sus, https://canaltech.com.br/seguranca/falha-de-seguranca-expoe-dados-de-milhares-de-pacientes-do-sus-em-sao-paulo-72271. Acesso em 21/09/2018