

A INTELIGÊNCIA ARTIFICIAL COMO INSTRUMENTO NO COMBATE AOS CRIMES DIGITAIS NA ÁREA MÉDICA

ARTIFICIAL INTELLIGENCE AS A TOOL TO COMBAT DIGITAL CRIME IN THE MEDICAL FIELD

Rodrigo de Carvalho Gonçalves Júnior

Resumo: O artigo procura expor as mudanças na área médica em decorrência das novas tecnologias e os principais meios usados pelos criminosos para obter dados confidenciais dos pacientes. O texto apresenta, inicialmente, o contexto atual da medicina e novas tecnologias, bem como as modalidades de ataques hackers utilizados pelos criminosos na obtenção de dados e como estes conseguem obter vantagem financeira. Posteriormente, aponta alguns casos recentes acerca dos crimes digitais na área médica, a legislação brasileira a respeito da relação médico-paciente e sua aplicação. Ao final traz algumas ideias de como evitar falhas na proteção de dados.

Palavras-Chave: Área médica; novas tecnologias; *hackers*; proteção de dados.

Abstract: This article aims to explain the changes in the medical field due to new Technologies and the main means used by criminals to obtain confidential patient data. The next initially presents the current context of medicine and the Technologies, as well as the types of hacker attacks used by criminals to obtain data and how they can obtain financial advantages. It then points out some recent cases of digital crimes in the medical field, brazilian legislation regarding the doctor-patient relationship and its application. Finally, it provides some ideas on how to avoid data protection failures.

Keywords: Medical field; new Technologies; hackers; data protection.

INTRODUÇÃO

As novas tecnologias têm alterado profundamente as relações interpessoais. Através das inovações técnicas, é possível comunicar-se com pessoas de todo o mundo. Realizar reuniões virtuais, ler um livro digital, interagir com pessoas através de redes sociais são apenas alguns exemplos de como o mundo contemporâneo é altamente tecnológico.

Tal influência é presente na medicina, e com o passar dos anos vêm mudando a relação entre médico e paciente. Com o avanço da tecnologia e da Inteligência Artificial, os serviços médicos tornaram-se mais acessíveis. Atualmente é possível agendar consultas e receber exames através do autoatendimento na web, realizar consultas remotas -facilitando o acesso

dos médicos aos pacientes, realizar o monitoramento contínuo de pacientes com condições médicas fatais informando o médico quando ocorre uma mudança crítica, elaborar prontuários médicos precisos e atualizados e armazenar dados dos pacientes de forma digital.

Os serviços apresentados simplificam a rotina dos pacientes, melhorando o atendimento e influenciando de forma significativa os resultados de pacientes críticos e índices de sobrevivência.

Apesar de muitos benefícios, esse nível de inovação tecnológica expõe hospitais, laboratórios, clínicas médicas e planos de saúde a uma ampla variedade de ameaças de segurança cibernética.

O grande volume de dados de alto valor dos pacientes que as organizações de saúde precisam para manter o padrão de atendimento é alvo de grandes organizações criminosas.

O sequestro de dados dos pacientes atrai os *hackers* devido aos danos imediatos causados. Os criminosos utilizam a mesma lógica dos crimes mais tradicionais: resgate milionário e pouco tempo para negociação.

Na maioria dos casos, o pagamento de resgate costuma ser exigido por criptomoedas, o que impede o rastreamento do criminoso.

1 CIBER ATAQUE

Os crimes digitais apresentam uma variável muito ampla, desde pequenos roubos a atos de guerra.

Os criminosos usam uma variedade de técnicas para alcançar o objetivo desejado. Na maioria das vezes essa motivação para o crime é totalmente visando um ganho financeiro.

Infelizmente, as instituições de saúde é um grande alvo dos criminosos. Hospitais, clínicas e laboratórios armazenam uma grande quantidade de dados pessoais de pacientes.

Os *hackers* acessam os sistemas com o objetivo de captar esses dados pessoais para cometer o sequestro de identidade, vende-los na *dark web* ou mantê-los como resgate.

Os agentes desta ação criminosa resumem-se a organizações criminosas, atores estaduais e pessoas privadas, sendo divididas em agentes externos e internos.

Os agentes externos são os não autorizados a usar uma rede ou dispositivo, mas entram de qualquer maneira. Correspondem aos grupos criminosos organizados, *hackers* profissionais e amadores.

Os agentes internos são usuários que têm acesso autorizado e legítimo aos ativos de uma empresa. Correspondem aos funcionários, parceiros de negócios, clientes, prestadores de serviços e fornecedores com acesso ao sistema e que usam indevidamente ou acidentalmente seus privilégios.

Os interesses do criminoso em um meio digital visam o dinheiro que é obtido através da coleta de dados do cliente - informações pessoais identificáveis ou outros dados confidenciais.

No âmbito de crimes cibernéticos na área da saúde destacam-se duas espécies: *ransomware* e engenharia social.

2 RANSOMWARE

De acordo com o *X-Force Threat Intelligence Index* da IBM, o *ransomware* é o segundo tipo mais comum de ataque cibernético, representando 17% dos ataques.

Neste caso, os criminosos utilizam um tipo de programa de computador para sequestrar informações pessoais de clientes.

Através deste sequestro, os criminosos exigem um pagamento elevado em troca de não utilizar os dados coletados.

Geralmente, o pagamento do resgate costuma ser exigido em criptomoedas por ser um meio que impede o seu rastreamento.

3 ENGENHARIA SOCIAL

Os crimes de engenharia social é um dos mais espalhados e conhecidos.

Chamado de *phishing*, os criminosos compartilham links de divulgação de sites falsos muitos semelhantes aos originais com a emissão de segunda via de boletos.

As mensagens são projetadas para parecer que vêm de uma fonte legítima, mas, ao entrarem nos links, os usuários têm seus dados pessoais e bancários capturados pelos criminosos.

Esse tipo de ação é comum entre os usuários de planos de saúde, pois recebem muitos e-mails e mensagens do plano sobre cobranças e informações.

4 CASOS RECENTES

Em decorrência das novas tecnologias, hospitais, centro de exames, empresas de convênios e órgãos do governo estão cada vez mais dependentes de sistemas digitais.

A tecnologia investida na medicina revolucionou a relação médico-paciente. A Inteligência Artificial transformou mundialmente a área da saúde.

Os aparelhos investidos pelas entidades de saúde vão muito além da assistência médica para elaborar diagnósticos e prevenir doenças. Atualmente, diversas entidades médicas utilizam robôs para armazenar dados de pacientes, agilizar tarefas administrativas e até mesmo serviços de enfermagem.

Esses serviços apresentam maior individualidade, garantindo ao paciente um tratamento mais específico, certo e agilizado.

No entanto, os sistemas que armazenam as informações dos pacientes atraem *hackers*, devido à alta quantidade de informações pessoais.

O setor da saúde pública e privada é um grande alvo de ataques cibernéticos.

Segundo pesquisas, 35% dos ataques cibernéticos acontecem contra entidades de saúde. Infelizmente, o Brasil lidera o *ranking* como o país que mais sofre esse tipo de ataque.

Nos últimos anos destacam-se dois ataques sofridos em solo nacional: apagão nas plataformas do Ministério da Saúde e ataque na Unidade de Pronto Atendimento (UPAs) de Presidente Prudente-SP.

O primeiro caso ocorreu em dezembro de 2021, quando um ataque hacker acessou o aplicativo e-SUS Notifica, o Sistema de Informação do Programa Nacional de Imunizações e o “CONECTE SUS”.

O serviço do SUS ficou fora do ar, o que manchou os levantamentos estatísticos e impossibilitou a emissão de documentos como o Certificado Nacional de Vacinação da COVID-19 e a Carteira Nacional de Vacinação Digital.

O segundo caso é mais recente. Em maio de 2023 uma Unidade de Pronto Atendimento (UPAs) em Presidente Prudente-SP sofreu ataques cibernéticos por três dias. Os ataques afetaram o acesso dos médicos aos prontuários e históricos dos pacientes, sendo necessário realizar todo o trabalho de forma manual, resultando na lentidão das consultas.

Esses ataques acarretam diversas consequências.

As interrupções no sistema de saúde acarretam o atraso de atendimentos,

impossibilitando a equipe médica de realizar exames e acessar os prontuários eletrônicos.

O não acesso ao prontuário eletrônico limitam as informações do paciente quanto ao seu quadro de saúde e histórico, dificultando a tomada de decisão dos médicos.

Além disso, hospitais e empresas de saúde ficam muito prejudicadas financeiramente, pois precisam arcar com multas e indenizações devido ao vazamento de dados dos pacientes, cujo dados pessoais foram vazados.

Em 2021, o hospital *Saint Margareth's Health* nos Estados Unidos foi fechado devido a uma série de ataques cibernéticos. De acordo com o relatório da *American Hospital Association*, mais de 130 hospitais rurais foram fechados desde 2010 nos Estados Unidos. Os ataques cibernéticos atingiram hospitais de diversos tamanhos, mas, especialistas dizem que alguns grupos criminosos se concentram em hospitais e sistemas menores por não possuírem um sistema de defesa adequado. Tal exemplo demonstra a gravidade do impacto financeiro e social causado por um ataque cibernético.

5 A LEI Nº 13.709/2018 (LGPD) NO DIREITO MÉDICO

O direito ao sigilo, à privacidade, à autonomia e à dignidade são garantias previstas na Constituição Federal de 1988, e, a Lei nº 13.709 de 14 de agosto de 2018 (LGPD) veio como um instrumento do Estado para reforçar a proteção desses direitos constitucionais.

Quando se trata de saúde, essa proteção torna-se ainda mais importante, pois os sistemas dos hospitais, clínicas, laboratórios e empresas de convênio médico são ricas em informações íntimas do paciente, que são imprescindíveis para o exercício da medicina.

A coleta de dados do paciente é imprescindível para o exercício da atividade. O histórico de saúde e as condutas do profissional são registradas por meio do prontuário, um documento que reúne informações do paciente, sinais e imagens registradas de exames, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, conforme definido pelo Conselho Federal de Medicina, Resolução CFM nº 1.638/2002.

6 A IMPORTÂNCIA DOS DADOS NA RELAÇÃO MÉDICO-PACIENTE

De acordo com os dados fornecidos, o médico elabora a anamnese, um procedimento essencial para que a equipe de saúde possa compreender o histórico e os sintomas do paciente para chegar a um diagnóstico.

Para a elaboração deste relatório é essencial que exista uma relação de confiança entre paciente e o profissional da saúde. Quanto maior a riqueza de detalhes coletados maior será a eficácia do tratamento médico.

7 PROTEÇÃO NORMATIVA DOS PACIENTES

Com a LGPD em vigor, o cuidado médico referente às informações dos pacientes teve que ser redobrado devido às sanções administrativas descritas na lei.

Como mencionado anteriormente, a LGPD veio para reforçar a proteção de direitos previstos na Carta Magna e outras leis.

Podemos encontrar a garantia da proteção de dados nas seguintes normas e resoluções:

Constituição Federal de 1988: é constitucional o direito a dignidade da pessoa humana, intimidade, vida privada, honra e imagens. É assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação.

Código Civil: de acordo com a legislação civil, os direitos da personalidade são irrenunciáveis. É possível ao titular exigir que cesse a ameaça, ou a lesão, e reclamar perdas e danos.

Código Penal: a legislação penal tipifica o crime de violação de segredo profissional. Artigo 154, Código Penal: “revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena-detenção, de três meses a um ano, ou multa”.

Código de Ética Médica: elenca os deveres de sigilo e respeito à autonomia do paciente.

Resolução CFM nº1605/00: garante ao paciente que o conteúdo do seu prontuário ou ficha médica não será revelado sem seu consentimento.

Resoluções CFM nº1.821/07 e 2.218/18: aprova as normas técnicas concernentes à digitalização e uso dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

As resoluções são hierarquicamente inferiores às leis. Havendo incompatibilidade entre uma resolução do Conselho Federal de Medicina e a Lei Geral de Proteção de Dados (LGPD), prevalecerá a regra da lei.

8 RESPONSABILIDADE DOS MÉDICOS, CLÍNICAS E HOSPITAIS

Quando ocorre uma invasão bem-sucedida ao sistema de saúde ou membros da equipe médica compartilham dados pessoais de pacientes, a LGPD elenca sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

As sanções administrativas (multas) não excluem as responsabilidades cíveis e penais resultantes da falha de segurança de dados.

9 COMO EVITAR FALHAS NA PROTEÇÃO DE DADOS?

A Lei Geral de Proteção de Dados determina que sejam utilizadas medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais, ilícitas e de situações de destruição, perda, alteração, comunicação e difusão de dados.

Com a crescente evolução das tecnologias e suas inovações, a medicina passa por um processo de modernização constante, trazendo muitos benefícios para os profissionais da saúde e pacientes. No entanto, o mundo do crime evoluiu e trouxe várias vulnerabilidades aos sistemas operacionais das instituições de saúde.

Ao mesmo tempo que houve melhorias significativas na área da saúde houve vulnerabilidades nos sistemas que permitiram o acesso de hackers nos sistemas, causando prejuízos milionários.

Segundo cálculos da International Business Machines (IBM), a violação de dados na área da saúde trouxe um prejuízo de 10 milhões de dólares, somente em território americano, e os custos decorrentes desses ataques cresceram 42% desde 2020.

Para evitar esses prejuízos milionários, é preciso adotar medidas rápidas na área de saúde. Instituições públicas e privadas precisam investir em cibersegurança para garantir maior proteção dos dados. Investir na segurança dos dados para bloquear acessos indevidos é necessário, mas, só isso não basta.

A adoção de medidas tecnológicas não é suficiente para a proteção jurídica dos agentes de tratamento de dados, pois a maioria das falhas na segurança resulta de ação humana.

Por isso, é necessário realizar um treinamento e conscientização de todos aqueles que trabalham na unidade e que possam ter acesso aos dados dos pacientes.

A LGPD destaca a importância da adoção de práticas de governança e políticas

internas que demonstrem o compromisso com a segurança dos dados.

CONCLUSÃO

Devido às novas tecnologias usadas na medicina, a relação médico-paciente foi profundamente alterada.

A Inteligência Artificial tornou-se uma grande aliada da área da saúde, sendo responsável por armazenar dados dos pacientes, apresentar diagnósticos, monitorar pacientes e realizar atuação preventiva. No entanto, as instituições públicas e privadas de saúde são um grande alvo para os criminosos devido ao grande armazenamento de dados confidenciais de pacientes.

A motivação financeira é o principal objetivo para a realização de sequestro de dados. As informações obtidas podem ser muito lucrativas para os criminosos, e este tipo de crime está cada vez mais frequente.

Hospitais, laboratórios, clínicas e empresas de convênio estão cada vez mais dependentes dos sistemas digitais, devido aos benefícios gerados, como celeridade e assertividade. Mas, infelizmente tais sistemas estão cada vez mais expostos a sofrerem ataques cibernéticos devido a falhas técnicas e falhas humanas.

Um ataque cibernético bem-sucedido pode gerar graves prejuízos aos pacientes, aos profissionais da saúde e instituições.

Para assegurar os direitos destes pacientes e profissionais, a Lei nº 13.709/2018 (LGPD) tem um papel muito importante.

A Lei Geral de Proteção de Dados (LGPD) tem por objetivo reforçar direitos constitucionais relacionados à privacidade e intimidade, assim como regulamentar as condutas médicas no meio digital, garantindo maior segurança aos médicos, pacientes e sistemas operacionais.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil**. 5 de outubro de 1988.

BRASIL. **Lei nº 10.406,10 de janeiro de 2002**. Código Civil.

BRASIL. **Decreto-Lei nº 2.848, 7 de dezembro de 1940**. Código Penal.

BRASIL. **Lei nº13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados.

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução nº1.605, 15 de setembro de 2000.**

CONSELHO FEDERAL DE MEDICINA (CFM - BRASIL). **Resolução nº1.821, 11 de julho de 2007.**

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução nº2.218, 21 de setembro de 2018.**

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução nº1.638, 10 de julho de 2002.**

BONFIM, BRUNA. **Ataques cibernéticos prejudicam atendimentos nas UPAs de Presidente Prudente.** Veja, 2023. Disponível em: <https://g1.globo.com/sp/presidente-prudente-regiao/noticia/2023/05/27/ataques-ciberneticos-prejudicam-atendimentos-em-upas-de-presidente-prudente.ghtml> Acesso em 22 de outubro de 2024.

FELIX, PAULA. **Setor de saúde tem epidemia de hackers** – e Brasil é um dos mais expostos. Veja, 2024. Disponível em: <https://veja.abril.com.br/saude/setor-de-saude-tem-epidemia-de-hackers-e-brasil-e-um-dos-mais-expostos#googlevignette> Acesso em 22 de outubro de 2024.

NETO, Miguel; NOGAROLI, Rafaella. **Debates Contemporâneos em Direito Médico e da Saúde**-Ed. 2023. São Paulo (SP): Editora Revista dos Tribunais.

SOUTHWICK, RON. **After cyberattack and other financial woes, an Illinois hospital closes its doors.** Chief healthcare executive, 2023. Disponível em: <https://www.chiefhealthcareexecutive.com/view/after-cyberattack-and-other-financial-woes-an-illinois-hospital-closes-its-doors> Acesso em 22 de outubro de 2024.

QUINTINO DE OLIVEIRA JÚNIOR, Eudes. FRANCIELE NEVES DE OLIVEIRA, JÚLIA. **Lei geral de proteção de dados e o tratamento de dados na saúde.** Migalhas, 2023. Disponível em: <https://www.migalhas.com.br/coluna/leitura-legal/385614/lei-geral-de-protecao-de-dados-e-o-tratamento-de-dados-na-saude> Acesso em 22 de outubro de 2024.

TECNOLOGIA DA INFORMAÇÃO. **Informativo SPDM. Ciberataques na área da saúde.** Disponível em: https://spdm.org.br/wp-content/uploads/2022/06/2a-Ed.-CIBERATAQUES-NA-AREA-DE-SAUDE_Rev.pdf Acesso em 22 de outubro de 2024.

O QUE É UM ATAQUE CIBERNÉTICO. IBM. Disponível em: <https://www.ibm.com/br-pt/topics/cyber-attack> Acesso em 22 de outubro de 2024.