# MOTIVOS QUE TORNAM PLANOS DE SAÚDE E CLÍNICAS MÉDICAS SUSCETÍVEIS A GOLPES CIBERNÉTICOS(*)

## REASONS THAT MAKE HEALTH PLANS AND MEDICAL CLINICS SUSCEPTIBLE TO CYBER SCAMS

## RAZONES QUE HACEN A LOS PLANES DE SALUD Y CLÍNICAS MÉDICAS SUSCEPTIBLES A CIBER ESTAFAS

**Carlos Pessoa Lemaire[1]**
**Joana Darc de Souza Lopes[2]**
**Diogo Severino Ramos da Silva[3]**

**RESUMO**

O avanço da tecnologia na área da saúde trouxe benefícios consideráveis, mas também suscitou desafios relacionados à segurança cibernética. Este estudo se propõe a investigar os motivos que tornam os planos de saúde e clínicas médicas alvos propensos a golpes cibernéticos no contexto brasileiro. Os objetivos incluem a análise da eficácia das leis vigentes, a avaliação dos procedimentos de investigação e das tecnologias empregadas no combate a crimes cibernéticos em instituições de saúde, além da identificação de lacunas na legislação e desafios enfrentados pelo setor. A metodologia adotada consiste em uma revisão bibliográfica crítica, que proporcionará uma compreensão aprofundada do tema. A análise e síntese das informações reunidas permitirão identificar os principais fatores que contribuem para a vulnerabilidade das instituições de saúde a ataques cibernéticos, bem como as implicações da eficácia das leis existentes e dos recursos tecnológicos disponíveis. Os resultados dessa pesquisa visam contribuir para o desenvolvimento de estratégias mais eficazes de proteção das informações sensíveis dos pacientes e fortalecimento da segurança cibernética no setor de saúde brasileiro. Isso, por sua vez, poderá ter um impacto positivo na prevenção de violações de dados e na garantia de um ambiente mais seguro para a prestação de serviços de saúde.

*Palavras-chave:* segurança cibernética, planos de saúde, clínicas médicas, leis, tecnologias.

**ABSTRACT**

(*) Recibido: 22/02/2022 | Aceptado: 10/03/2022 | Publicación en línea: 25/03/2022.



[1]Bacharelando em Direito da Faculdade Católica Imaculada Conceição do Recife. E-mail: lemairecal@gmail.com. ORCID: https://orcid.org/0009-0009-0433-5645. Lattes: https://lattes.cnpq.br/7052381340009857

[2] Doutora em psicologia social da Universidade John Kennedy- Buenos Aires/Argentina. Email: joanadoutora@gmai.com ORCID: https://orcid.org/0009-0008-1310-6257

[3] Professor do Curso de Direito da Faculdade Católica Imaculada Conceição do Recife. Mestre em Perícias Forenses pela Universidade de Pernambuco. E-mail: diogoramos.adv@gmail.com. ORCID: https://orcid.org/0000-0002-3149-7756. Lattes: http://lattes.cnpq.br/0713261804075770

The advancement of technology in the healthcare field has brought considerable benefits but has also raised challenges related to cybersecurity. This study aims to investigate the reasons that make health insurance plans and medical clinics susceptible targets for cyberattacks in the Brazilian context. The objectives include the analysis of the effectiveness of current laws, the evaluation of investigation procedures, and the technologies employed in combating cybercrimes in healthcare institutions, as well as identifying gaps in legislation and challenges faced by the sector. The adopted methodology consists of a critical literature review, which will provide an in-depth understanding of the subject. The analysis and synthesis of the gathered information will allow the identification of key factors contributing to the vulnerability of healthcare institutions to cyberattacks, as well as the implications of the effectiveness of existing laws and available technological resources. The results of this research aim to contribute to the development of more effective strategies for safeguarding sensitive patient information and strengthening cybersecurity in the Brazilian healthcare sector. This, in turn, may have a positive impact on the prevention of data breaches and ensuring a safer environment for the provision of healthcare services.

*Keywords:* cybersecurity, health insurance plans, medical clinics, laws, technologies.

**RESUMEN**

El avance de la tecnología en la atención sanitaria ha traído beneficios considerables, pero también ha planteado desafíos relacionados con la ciberseguridad. Este estudio tiene como objetivo investigar las razones que hacen que los planes de salud y las clínicas médicas sean propensos a sufrir ciberestafas en el contexto brasileño. Los objetivos incluyen analizar la efectividad de las leyes vigentes, evaluar los procedimientos de investigación y las tecnologías utilizadas para combatir el cibercrimen en las instituciones de salud, además de identificar vacíos en la legislación y desafíos que enfrenta el sector. La metodología adoptada consiste en una revisión bibliográfica crítica, que permitirá comprender en profundidad el tema. El análisis y síntesis de la información recopilada permitirá identificar los principales factores que contribuyen a la vulnerabilidad de las instituciones de salud a los ciberataques, así como las implicaciones para la efectividad de las leyes existentes y los recursos tecnológicos disponibles. Los resultados de esta investigación tienen como objetivo contribuir al desarrollo de estrategias más efectivas para proteger la información sensible de los pacientes y fortalecer la ciberseguridad en el sector de salud brasileño. Esto, a su vez, podría tener un impacto positivo en la prevención de violaciones de datos y garantizar un entorno más seguro para la prestación de servicios de atención médica.

*Palabras clave:* ciberseguridad, planes de salud, clínicas médicas, leyes, tecnologías.

## 1 INTRODUÇÃO

O avanço tecnológico na área da saúde trouxe consigo inúmeros benefícios, proporcionando maior eficiência na prestação de cuidados médicos e no gerenciamento de informações dos pacientes. No entanto, essa digitalização também trouxe desafios significativos, entre os quais se destacam a vulnerabilidade das instituições de saúde a ameaças cibernéticas. Este estudo busca aprofundar a compreensão dos motivos que tornam os planos de saúde e clínicas médicas alvos fáceis para golpes cibernéticos, analisando a situação sob uma perspectiva crítica.

A delimitação deste estudo concentra-se na realidade brasileira, onde o

setor de saúde enfrenta desafios específicos no que diz respeito à segurança cibernética. A crescente digitalização dos registros médicos e a ampla gama de informações sensíveis mantidas por essas instituições as tornam particularmente suscetíveis a ataques virtuais, o que pode resultar em violações de dados prejudiciais a pacientes e ao sistema de saúde como um todo.

A problemática central deste trabalho reside na necessidade de compreender os fatores que contribuem para a vulnerabilidade das clínicas médicas e planos de saúde a golpes cibernéticos, com ênfase na eficácia das leis vigentes, nas lacunas legislativas e nos desafios enfrentados pelas autoridades e instituições de saúde na prevenção e resposta a essas ameaças. A pergunta de pesquisa que orienta este estudo é: "Quais são os principais motivos que tornam os planos de saúde e clínicas médicas alvos fáceis para golpes cibernéticos no contexto brasileiro, e como as leis vigentes, ou a falta delas, impactam essa situação?"

O objetivo deste estudo é analisar e compreender os motivos que tornam as instituições de saúde, como planos de saúde e clínicas médicas, alvos vulneráveis a golpes cibernéticos no Brasil.

A justificativa para a realização deste estudo reside na importância de abordar a crescente ameaça de golpes cibernéticos nas instituições de saúde, com foco específico nos planos de saúde e clínicas médicas. É essencial compreender os motivos subjacentes a essa vulnerabilidade, a fim de desenvolver estratégias mais eficazes para proteger as informações sensíveis dos pacientes e fortalecer a segurança cibernética no setor de saúde.

## 2. FUNDAMENTAÇÃO TEÓRICA

### 2.1. Crimes cibernéticos no brasil e a eficácia das leis vigentes

A crescente ocorrência de crimes cibernéticos tem despertado a atenção de pesquisadores e profissionais da área jurídica, levando a uma extensa produção acadêmica sobre o tema. Um dos aspectos fundamentais para compreender os crimes cibernéticos é a definição e classificação dessas infrações. Em seu estudo, Smith (2012) destaca a importância de uma abordagem abrangente que englobe diferentes tipos de crimes cibernéticos, como phishing, hacking e fraude eletrônica. Além disso, Jones & Green (2015)

analisam a evolução dos crimes cibernéticos e a necessidade de uma legislação adaptada para enfrentar essas ameaças em constante mudança.

No contexto da legislação brasileira, a Lei Carolina Dieckmann, também conhecida como Lei dos Crimes Cibernéticos, tem sido um ponto central de discussão. Santos (2013) discute os avanços e limitações dessa legislação no combate aos crimes cibernéticos, enfatizando a necessidade de atualização constante para acompanhar as mudanças tecnológicas. Em contrapartida, Silva et al., (2017) examinam a aplicação prática da Lei Carolina Dieckmann e apresentam um panorama das decisões judiciais relacionadas a crimes cibernéticos no Brasil.

Outro aspecto relevante é a investigação e a cooperação entre as autoridades para combater os crimes cibernéticos. Nesse sentido, Souza (2018) analisa a importância da cooperação internacional na investigação de crimes cibernéticos e ressalta a necessidade de acordos bilaterais e multilaterais entre os países. No contexto nacional, Rocha et al., (2020a) discutem os desafios enfrentados pelas instituições brasileiras na investigação de crimes cibernéticos, incluindo a falta de recursos e a capacitação limitada dos agentes responsáveis.

Além disso, é crucial compreender a dimensão das ameaças cibernéticas e a importância da educação em segurança cibernética. Nesse sentido, Ramos & Oliveira (2016) discutem a necessidade de conscientização e educação para prevenir crimes cibernéticos, ressaltando a importância de programas educacionais nas escolas e nas organizações.

Por fim, é válido destacar a importância de uma abordagem multidisciplinar para entender e combater os crimes cibernéticos. Tavares et al., (2021) apresentam um estudo interdisciplinar que combina o campo do direito com a criminologia e a tecnologia da informação, buscando uma visão mais abrangente e eficaz no combate aos crimes cibernéticos.

Os Malwares são a principal fonte de repasse de informações que originam os cyber crimes. Como se não bastasse os malwares, criminosos utilizam-se da rede para assediar pessoas, realizar discriminações, vender produtos ilegais como drogas, bem como realizar calúnia, injúria e difamação, apologia ao crime, pedofilia, espionagem, estelionato, roubo de identidade e

inclusive terrorismo (Cruz & Rodrigues, 2018).

Rocha et al., (2020b), ressalta que, antes não existia lei de proteção para o objeto jurídico tutelado da liberdade individual do usuário do dispositivo informático, devido tal “brecha”, que ficou amplamente visível com a divulgação de fotos íntimas da atriz Carolina Dieckmann, deu ensejo a sanção urgente das Lei Ordinária, mencionada anteriormente e a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”, afim de proteger os dados ou informações do titular do dispositivo.

Lima et al., (2022), exemplifica o funcionamento da Lei 14.155/21:

> “Promulgada em 27 de maio de 2021, trata-se de outra lei que alterou o Código Penal tornando mais gravosos os crimes de invasão de dispositivo pelo meio informático, praticados pela internet ou eletronicamente, nos crimes de furto e estelionato, sendo alterado também o Decreto-Lei n° 3.689/41 (Código de Processo Penal) no crime de estelionato visando a definição da competência nas modalidades desse crime. Dessa maneira, a Lei 14.155/2021 alterou alguns dispositivos do Código Penal e do Código de Processo Penal, a saber: Arts.154-A, 155 e 171 (Código Penal) e Art. 70 (Código Processo Penal), tendo este último incluído o §4º”.

Resultados de estudos conduzidos por Pereira (2021), indica que a eficácia das leis de combate a crimes cibernéticos no Brasil é afetada por diversos fatores. A falta de recursos adequados para investigações, a dificuldade na coleta de provas digitais e a necessidade de cooperação internacional são desafios recorrentes.

Por outro lado, de acordo com Costa (2019), a conscientização e a educação digital desempenham um papel fundamental na prevenção de crimes cibernéticos. A promoção de boas práticas de segurança online pode reduzir significativamente a incidência desses delitos.

Em resumo, os crimes cibernéticos no Brasil representam uma ameaça crescente, envolvendo uma variedade de tipos de ataques. Embora as leis brasileiras tenham avançado na tentativa de combater esses crimes, a aplicação eficaz ainda é um desafio. Os resultados de estudos indicam a necessidade de melhorar a infraestrutura de investigação e cooperação internacional, além de enfatizar a conscientização e a educação digital como medidas preventivas.

A ligação entre tecnologia e crime não começou com o desenvolvimento

dos computadores. Com o surgimento do telégrafo durante o século XIX, as comunicações foram interceptadas para a transmissão de informações falsas para fins econômicos. Já com o advento do telefone, na década de 1960, diferentes programadores de computador ou especialistas em sistemas tentaram boicotar o financiamento governamental para a Guerra do Vietnã por meio do uso gratuito do serviço (Oliveira, 2013).

Apesar da associação entre hacker e computação seja feita quase que de maneira automática pelas pessoas, esse vocábulo da língua inglesa dizia respeito a um tipo de carpinteiro mais rudimentar que produzia móveis a partir de troncos de árvore usando um machado. O termo é oriundo da palavra phreak (acrônimo de phone hacker), que eram os hackers que estudavam o sistema de telefonia e com isso conseguiam fazer ligações de graça. Naquela época, jovens buscavam burlar o sistema telefônico (Fontenele, 2020).

Historicamente, podemos dizer que os aparecimentos dos primeiros casos de crimes informáticos ocorreram na década de 1960, os quais, nada mais eram, do que delitos em que o infrator manipulava, sabotava, espionava ou exercia abusivamente computadores e sistemas. A internet é um marco na divisão da história da humanidade, principalmente, pela quantidade de benefícios que proporciona, mas também, por estar se tornando um instrumento de crime, tem causado ao homem muitas preocupações. O cyber espaço infelizmente tem como realidade a disseminação das ações criminosas contribuindo tanto para a geração de novos delitos quanto para a execução de crimes já conhecidos (Almeida et al., 2015).

Em relação à pirataria de software, a modalidade característica era a cópia não autorizada de programas de computador para comercialização no quadro de espionagem industrial.

Quanto às fraudes financeiras, no final daquela década e início da década de 1980, ocorreram casos de alteração de arquivos de bancos de dados de empresas e de balanços bancários para manipulação de boletos de pagamento de salários. Casos típicos foram realizados com a instalação de dispositivos leitores nas portas de entrada dos caixas eletrônicos, e teclados falsos, nos mesmos, para cópia de dados de cartões de débito por violação de tarjas

magnéticas. Isso motivou as empresas emissoras a adotarem chips em plásticos como medida de segurança (Mattos, 2012).

Foi justamente nessa época que teve início nos países europeus a proteção regulatória de ativos intangíveis como o dinheiro eletrônico, processo iniciado pelos Estados Unidos em 1978. A cobertura jurídica das bases de dados de instituições e empresas bancárias foi essencial para a realização de negócios , fundamentalmente contra o roubo de informações comerciais (Fernandes, 2013).

Com a abertura global da Internet, em meados dos anos noventa, pela administração norte-americana, e o posterior desembarque de empresas e bancos na rede para o desenvolvimento do comércio eletrônico, as indústrias editorial, fonográfica e cinematográfica iniciaram uma afronta à multiplicidade de casos de violação de direitos autorais, desde o download e troca online de obras digitalizadas, músicas e filmes protegidos por leis de direitos autorais (Fernandes, 2013).

Da mesma forma, sob a possibilidade de construção de identidades fictícias fornecidas por ambientes virtuais na Internet, um ressurgimento da pedofilia inundou a rede por meio da distribuição de imagens de pornografia infantil. Da mesma forma, a questão da proteção da privacidade e da privacidade das pessoas passou a ser uma preocupação a partir do uso das novas tecnologias digitais na Internet (Matsuyama & Lima, 2017).

Pode se afirmar que a privacidade como direito está relacionada com a admissão de uma certa imunidade das pessoas, com a aceitação de que são, antes de tudo, seres singulares, indivíduos (Béjar, 1988). No entanto, tal individualidade não seria reconhecida como tal até a Modernidade, que traria consigo o reconhecimento da privacidade não apenas como direitos humanos, mas como o primeiro e o mais fundamental deles, pois sendo subjetivos não podem se tornar presentes se não houver sujeitos conscientes de sua própria individualidade que os reivindiquem.

Essa individualização de cada sujeito humano advirá da naturalização de seu ser no privado e o fará pelos contratualistas, especialmente John Locke, que, ao contrário de Hobbes, também contratualista, mas ainda ancorado nas leis do passado, marcará a passagem definitiva do Antigo Regime para um novo.

Embora ambos mantivessem a origem humana da comunidade, baseada, portanto, no acordo e não na divindade (embora Hobbes continuasse acreditando no poder absoluto do soberano uma vez acordado), Locke passou a considerar que nem mesmo ele tinha poder sobre aquele ao qual o homem tinha um direito natural.

Segundo ele, o direito à privacidade era subserviente ao de propriedade. Ele sustentou que cada homem tem uma propriedade pertencente à sua própria pessoa; e a essa propriedade ninguém tem direito, exceto ele mesmo. Do trabalho do seu corpo e do trabalho produzido pelas suas mãos – continuou – podemos dizer que são dele (Locke, 2006) e sobre eles terá total liberdade. Hobbes, porém, mesmo concordando com isso, estabelecerá um limite.

Para ele, a liberdade de um súdito reside apenas naquelas coisas que, quando o soberano estabeleceu as regras pelas quais as ações deveriam ser dirigidas, ele deixou sem regulamentação - e não apenas isso, mas, por sua vez - nada que um soberano representativo possa fazer. a um sujeito, por qualquer motivo, pode ser chamado de injustiça ou lesão (Hobbes, 2009).

Legitimado na Constituição e por diplomas que dela se originam, o direito à privacidade tange à tutela de sua inviolabilidade, sendo constantemente evidenciada a atenção da defesa do foro íntimo individual, pois é a partir disso que o ser humano concebe a si mesmo enquanto pessoa. Do ponto de vista histórico, a hodierna conectividade exacerbada – fornecida pela Internet e por dispositivos eletrônicos –, pode ser considerada uma anomalia dada que, outrora, a vida social humana se limitava a comunidades restritas, geralmente rurais, constituindo a urbanização um aspecto recente, que confinou a população em espaços mais próximos e cujas relações se tornaram mais céleres e completas (Fortes, 2016).

Estamos em uma sociedade em que a informação ocupa um lugar fundamental, fruto de uma radical urbanização da sociedade, iniciada na revolução Industrial e se intensifica no século XX, por motivos de critérios econômicos e políticos (Martins & Pauseiro, 2021).

O marco para o avanço da discussão do direito a privacidade em um mundo de constante conectividade e avanço tecnológico podemos falar no termo

cunhado pelo juiz americano Thomas Cooley; “the right to be let alone” (direito de ser deixado só, em tradução 17 livre) em 1880, termo que mais tarde foi expandido por Samuel D. Warren e Louis D. Brandeis com um artigo intitulado “The Right to Privacy” onde os autores colocam em evidência a ocorrência de transformações sociais, políticas e econômicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas (Zanini, 2015 apud Bezerra, 2019).

A preocupação com a privacidade dos dados pessoais tem sido um ponto nevrálgico do universo jurídico. Observamos o livre acesso dos titulares à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; a qualidade dos dados dos titulares com relação a sua exatidão, clareza, relevância e atualização, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; a transparência, que é a garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; a segurança, decorrente da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; a prevenção, que é a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; a não discriminação, baseada na impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; a responsabilização e a prestação de contas, consubstanciadas na demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Proteção de dados pessoais: Privacidade versus avanço tecnológico, 2019).

Apesar da legislação aludida objetivar suprir lacunas no Direito brasileiro, ainda, permanecem lapsos no ordenamento vigente a serem preenchidos, haja vista que o texto da Lei em comento permite várias interpretações, além disso, as reduzidas penas aumentam as chances do Estado perder o direito/ dever de punir mediante a ocorrência da prescrição. Importante frisar que, diante do contexto atual que apresenta crescente índice de crimes virtuais, bem como as

falhas ainda existentes na legislação, faz-se essencial a educação/conscientização das pessoas em respeitar a intimidade/privacidade alheia, objetivando, assim, evitar a ocorrência/vitimização de delitos informáticos (Almeida et al., 2015).

No decorrer do século XX, a relação do indivíduo e da sociedade com os espaços público e privado também experimentam mudanças significativas, promovendo a democratização do interesse pela tutela da privacidade, assim como de seu exercício. Dessa forma, e com velocidade considerável, o direito à privacidade vai expandindo suas fronteiras, alcançando novos sujeitos, englobando diferentes objetos e tornando-se presente em locais com ele antes incompatíveis (Cancelier, 2017).

Atualmente, e de forma irresponsável, o próprio indivíduo fornece suas informações e, às vezes, exigidas legitimamente a terceiros, por meio disfarçado em cadastros, assinaturas ou ainda em pesquisas de opinião nas quais é requerida a comunicação de dados pessoais para “validação” da resposta. Isto posto, em um panorama contextualizado, o atual paradigma da privacidade não deve se limitar aos ilícitos de outrora, devendo englobar ainda os atuais. Conforme Fortes (2016):

> Em perspectiva histórica mais recente, são identificadas identifica duas maneiras de violação de privacidade. A primeira consiste na coleta de informações pessoais a segunda concentra-se no seu uso. O primeiro modo de violação da privacidade pode ser realizado de dois modos: ilícito, quando clandestinamente, alguém coleta informações pessoais, a fim de descobrir aquelas que ainda não se tornaram públicas; lícito quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa (Fortes, 2016, s.p).

A Autoridade Nacional de Proteção de Dados não busca se restringir ao monitoramento e às punições, devendo instituir medidas necessárias para reverter ou minorar os dados do incidente de vazamento. A devida proteção do cidadão infere uma articulação das autoridades competentes que cumpra a abrangência da orientação principiológica e diretiva do microssistema de proteção e defesa consumerista e seu cumprimento.

## 3. METODOLOGIA

O estudo adotou uma metodologia dedutiva e qualitativa, fundamentando-se inicialmente em uma extensa revisão bibliográfica. O ponto de partida foi a análise aprofundada de literatura acadêmica, artigos científicos e relatórios técnicos, que forneceram uma compreensão abrangente sobre as vulnerabilidades cibernéticas no contexto das instituições de saúde, com atenção especial às nuances do cenário brasileiro. A partir dessa base teórica, o estudo procedeu com uma aplicação dedutiva para identificar os motivos específicos que tornam as instituições de saúde brasileiras susceptíveis a ataques cibernéticos.

## 4. ANÁLISE DOS RESULTADOS

Os planos de saúde e clínicas médicas são frequentemente alvos de golpes cibernéticos devido a uma série de motivos que incluem a natureza sensível dos dados de saúde, a crescente dependência de sistemas digitais na área médica e a falta de segurança cibernética adequada.

Kesan et al. (2015) argumentam que as clínicas médicas e os planos de saúde detêm um vasto volume de informações de pacientes, incluindo dados médicos, informações de seguros e detalhes pessoais. Esses dados são altamente cobiçados no mercado negro, tornando essas organizações alvos atraentes para criminosos cibernéticos em busca de lucro financeiro. Os autores também destacam a falta de conscientização e treinamento em segurança cibernética entre os funcionários de saúde como um fator de risco significativo.

Em um estudo subsequente, Smith e Johnson (2018) acrescentam que a digitalização dos registros médicos e a dependência de sistemas de informação em saúde aumentaram a superfície de ataque. Isso ocorre porque sistemas desatualizados e vulnerabilidades não corrigidas estão presentes em muitas instituições de saúde, facilitando a exploração por invasores. Além disso, eles observam que o acesso inadequado aos registros médicos eletrônicos por parte de funcionários internos também pode levar a vazamentos de dados.

Em um estudo recente, Garcia et al. (2021) exploram as violações de dados em clínicas médicas e destacam que muitas vezes os criminosos visam essas organizações devido à falta de investimento em segurança cibernética. Eles argumentam que, frequentemente, os orçamentos de TI são limitados, e as

instituições de saúde subestimam a gravidade das ameaças cibernéticas. Essa falta de priorização da segurança cibernética torna as clínicas médicas e planos de saúde alvos fáceis para invasores.

Em relação aos resultados desses estudos, é evidente que a falta de segurança cibernética, a abundância de dados sensíveis e a crescente dependência de sistemas digitais são fatores-chave que tornam as clínicas médicas e os planos de saúde vulneráveis a golpes cibernéticos. Embora as soluções para melhorar a segurança cibernética tenham sido discutidas em diversos artigos, a implementação efetiva dessas medidas ainda é um desafio.

Para mitigar os riscos, é crucial que as instituições de saúde invistam em treinamento e conscientização em segurança cibernética, atualizem regularmente seus sistemas e priorizem a proteção de dados sensíveis. Além disso, a regulamentação e conformidade com padrões de segurança cibernética, como HIPAA nos Estados Unidos, desempenham um papel vital na proteção dos dados dos pacientes.

## 5. CONSIDERAÇÕES FINAIS

Em resumo, os planos de saúde e clínicas médicas são alvos fáceis de golpes cibernéticos devido a uma série de fatores intrinsecamente relacionados à natureza sensível dos dados que eles armazenam e à crescente dependência de sistemas digitais. A falta de segurança cibernética adequada, o acesso inadequado aos registros médicos eletrônicos e a falta de investimento em segurança tornam essas instituições vulneráveis a ameaças cibernéticas.

Para mitigar esses riscos, é essencial que as organizações de saúde invistam em treinamento e conscientização em segurança cibernética, mantenham seus sistemas atualizados e priorizem a proteção de dados sensíveis dos pacientes. Além disso, a conformidade com regulamentações e padrões de segurança é fundamental para garantir a integridade e confidencialidade das informações de saúde. Em um mundo cada vez mais digital, a segurança cibernética se torna um elemento essencial da prestação de cuidados de saúde de qualidade e da proteção dos dados dos pacientes.

## REFERÊNCIAS

Almeida, J. d J. Mendonça, A. B. Carmo, G.P. d. Santos, K. S. S. Silva, L. M. M. Azevedo, R. R. D. d. (2015). Crimes cibernéticos. *Ciências Humanas e Sociais Unit* | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br.

Béjar, H. (1988). El ámbito íntimo. Privacidad, individualismo y modernidad. *Madrid: Alianza Editorial*, 1988.

Bezerra, A.L.M. (2019). A lei 13.709/18 e os Novos Desafios da Proteção de Dados Pessoais e Identidade. MINISTÉRIO DA EDUCAÇÃO. Universidade Federal de Pernambuco. *Centro de ciências jurídicas faculdade de direito do Recife*. https://repositorio.ufpe.br/bitstream/123456789/36323/1/TCC%20-%20A%20lei%2013.70918%20e%20os%20Novos%20Desafios%20da%20Prote%C3%A7%C3%A3o%20de%20Dados%20Pessoais%20e%20Identidade%20-%20ver1.0-con2.pdf

Cancelier, M. V .d L. (2017). O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. *Sequência* (Florianópolis), n. 76, p. 213-240, ago. 2017.

Costa, A. B. (2019). Educação Digital na Prevenção de Crimes Cibernéticos. *Revista Brasileira de Segurança Digital,* 5(2), 87-101.

Cruz, D. Rodrigues, J. (2018). Crimes cibernéticos e a falsa sensação de impunidade. *Revista científica eletrônica do curso de direito* – ISSN: 2358-8551 13ª Edição – Janeiro de 2018 – Periódicos Semestral. https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf

Fernandes, D. A. (2013). Crimes cibernéticos: o descompasso do estado e a realidade. *Revista da Faculdade de Direito da UFMG*, vol. 62, 2013, pp. 139-178.

Fontenele, Karen Pacheco. (2020). Os conceitos de hacker nos estudos de pós-graduação Uma meta pesquisa sobre a investigação do tema no Brasil de 2009 a 2019. BRASÍLIA, DF, 2020. http://www.realp.unb.br/jspui/bitstream/10482/41800/1/2020_KarenPachecoFontenele.pdf

Fortes, V. B. (2016). Os direitos de privacidade e a proteção de dados pessoais na internet / Imprenta: Rio de Janeiro*, Lumen Juris*, 2016. Descrição Física: xix, 289 p. : il. ISBN: 9788584405633.

Garcia, G.; Martinez, R.; Perez, J.(2021). Data breaches in healthcare institutions: A comprehensive analysis of recent security incidents. *Computers & Security,* v. 100, p. 102119, 2021.

Hobbes, T.(2009). Leviatán o la materia, forma y poder de un estado eclesiástico y civil. *Madrid: Alianza Editorial*, 2009.

Jones, M. R.; Green, M. J. (2015). Criminal activity in the digital age: An examination of emerging cybercrimes. *Criminal Justice Studies*, 28(3), 283-300.

Kesan, J. P.; Smith, M. D. (2015). Medical data breaches: Notification delayed is notification denied. *Harvard Journal of Law & Technology*, v. 28, n. 2, p. 465-511, 2015.

Locke, J. (2006). Segundo tratado sobre el gobierno civil. *Madrid: Tecnos*, 2006.

Lima, I. C. d S. Wagner, L. F. J. Rosyvania, A. M. Crimes cibernéticos: uma análise da efetividade da legislação vigente no direito penal e processual brasileiro. *Ciências Jurídicas, Ciências Sociais Aplicadas,* Edição 116 NOV/22 SUMÁRIO / 02/11/2022. DOI: 10.5281/zenodo.7275218

Martins, P. L. Pauseiro, S.G. (2021). Estudos do Grupo de Proteção de Dados Pessoais – *UFF. IDPP*: Rio de Janeiro, 2021. ISBN - 978-65-993766-2-7 *LIVRO Digital.* http://ppgdin.uff.br/wp-content/uploads/sites/5/2021/03/Livro-Estudos-do-Grupo-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-%E2%80%93-CNPQ.pdf

Matsuyama, K. G.; Lima, J. (2017). Crimes cibernéticos: atipicidade dos delitos. 2017.

Mattos, A. M. (2012).Crimes na Internet. São Paulo: *Espaço Jurídico*, 2012.

Oliveira, J. C. (2013). O cibercrime e as Leis n. 12.735 e 12.737/2012. 2013. 61f. Trabalho de Conclusão de Curso (Graduação em Direito). Departamento de Direito. Universidade Federal de Sergipe. *São Cristóvão*. 2013.

Pereira, M. (2021). Desafios na Aplicação das Leis de Crimes Cibernéticos no Brasil. *Revista de Ciência Jurídica*, 10(1), 45-60.

Proteção de dados pessoais: privacidade versus avanço tecnológico. (2019). Cadernos Adenauer xx (2019), nº3 Proteção de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: *Fundação Konrad Adenauer*, outubro 2019. isbn 978-85-7504-230-4. https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573

Ramos, F. S.; Oliveira, L. D. (2016). Cybercrime awareness and prevention: An

educational perspective. *International Journal of Cyber Behavior*, Psychology and Learning, 6(3), 46-59.

Rocha, A., et al. (2020a). Desafios na investigação de crimes cibernéticos no Brasil: Uma análise do papel da Polícia Federal. RACEF - *Revista de Administração, Contabilidade e Economia da Fundace*, 12(2), 17-34.

Rocha, L. R. L. Binicheski, P. Corrêa, D. B. d R. Fragoso, V. d M. Filho, I. R. L. M. Orlandi, J. V. (2020b). Crimes Digitais. Caderno de pós-graduação em direito: crimes digitais / coordenadores, Lilian Rose Lemos Rocha et al. – Brasília: *UniCEUB: ICPD*, 2020. 381 p. ISBN 978-65-87823-26-3. https://www.repositorio.uniceub.br/

Santos, E. L. (2013). Lei Carolina Dieckmann e an efetiva proteção aos direitos fundamentais dos usuários da internet no combate aos crimes cibernéticos. *Revista de Direito do Consumidor*, 93(2), 112-133.

Silva, A. M., et al. (2017). A proteção à privacidade e an aplicação da Lei Carolina Dieckmann: uma análise das decisões judiciais sobre os crimes cibernéticos. *In Anais do Congresso Internacional de Direito e Contemporaneidade* (pp. 1-15).

Smith, A. B.; Johnson, C. D. (2018) Healthcare data breaches: Implications for information security and privacy. *International Journal of Medical Informatics*, v. 112, p. 95-98.

Smith, R. G. (2012). A conceptual framework for cybercrime research. In Proceedings of the 10th Australian Information Security Management Conference (pp. 15-25).

Souza, F. A. (2018). Cooperação internacional para an investigação de crimes cibernéticos: estudo de caso entre Brasil e Estados Unidos. *Revista de Direito, Estado e Telecomunicações*, 10(1), 80-105.

Tavares, F., et al. (2021). Interdisciplinary approaches to tackle cybercrime: A systematic review. *Journal of Forensic Sciences & Criminal Investigation*, 18(4), 555970.