REVISTA BRASILEIRA DE DESENVOLVIMENTO E INOVAÇÃO

ESTUDO EXPLORATÓRIO SOBRE OS ATAQUES CIBERNÉTICOS E A INEFICIÊNCIA PENAL

BRITO, Jaqueline Ursino de[1]. *BASTOS, Alder Thiago*[2].

RESUMO: O presente estudo aborda a crescente ameaça dos ataques cibernéticos e um novo contexto criminoso que explora o mundo digitalmente interligado, destacando a importância da compreensão das complexidades técnicas e implicações jurídicas desses incidentes. A análise se estende aos contornos legais que moldam as respostas governamentais, as responsabilidades das partes envolvidas e as lacunas na paisagem regulatória. Destaca-se a relevância do tema não apenas em termos de segurança cibernética, mas também nas esferas sociais, econômicas e políticas. A legislação brasileira, como o Código Penal, é mencionada como uma ferramenta para abordar invasões de dispositivos informáticos, mas ainda incipiente quanto às formas de penalização desse imbróglio. Isso porque, a evolução dos ataques cibernéticos ao longo das décadas, desde os primeiros vírus de computador até os sofisticados ataques de *ransomware* e *phishing* dos dias de hoje contemplam a própria evolução criminosa alinhavada com os dispositivos eletrônicos do século XXI. A discussão inclui a variedade de ataques, as motivações dos atacantes e o impacto nos negócios e na sociedade. Estratégias de prevenção e mitigação são discutidas, incluindo a necessidade de investimentos em tecnologias de segurança cibernética, educação dos usuários e colaboração internacional. No entanto, reconhece-se que a segurança cibernética nunca será absoluta, exigindo uma mentalidade de resiliência e planos de resposta a incidentes. Em última análise, a conclusão enfatiza a importância da abordagem multifacetada na prevenção e mitigação dos ataques cibernéticos, bem como a necessidade de colaboração entre organizações públicas e privadas para enfrentar eficazmente essa ameaça em constante evolução, utilizando-se, para tanto, a metodologia de revisão bibliográfica, amparadas em referenciais teóricos publicados em meios físicos e digitais.

PALAVRAS-CHAVE: Ataques cibernéticos; evoluções no crime; insuficiência da lei penal.

EXPLORATORY STUDY ON CYBER ATTACKS AND CRIMINAL INEFFECTIVENESS

ABSTRACT: This study addresses the growing threat of cyberattacks and a new context of crime that exploits the digitally interconnected world, highlighting the importance of understanding the technical complexities and legal implications of these incidents. The analysis extends to the legal contours that shape government responses, the responsibilities of the parties

[1] Graduanda 10ª semestre das Faculdades Integradas Campos Salles.

[2] Pós-doutorando em Direito pela *Mediterranea International Centre for Human Rights Research* - Università "Mediterranea" di Reggio Calabria. Doutor em Direito Ambiental Internacional pela Universidade Católica de Santos – UNISANTOS. Tese selecionada para o programa de Bolsa CAPES (2023). Mestre em Direito pela Universidade Santa Cecília (UNISANTA) – Santos/SP (2018). Membro da *International Association of Artificial Intelligence* – I2AI. Membro da Associação Nacional das Advogadas e Advogados de Direito Digital – ANADD. Pesquisador junto ao Grupo de Pesquisa - Direito Ambiental, Estado e Sociedade da Universidade Católica de Santos (UNISANTOS). Compõe os Núcleos de Desenvolvimento Estruturantes da FABE e Faculdades Integradas Campos Salles. Advogado (Orientador).

involved, and the gaps in the regulatory landscape. The relevance of the topic is highlighted not only in terms of cybersecurity, but also in the social, economic, and political spheres. Brazilian legislation, such as the Penal Code, is mentioned as a tool to address invasions of computer devices, but it is still incipient in terms of the forms of penalization for this imbroglio. This is because the evolution of cyberattacks over the decades, from the first computer viruses to today's sophisticated ransomware and phishing attacks, contemplates the very evolution of crime aligned with the electronic devices of the 21st century. The discussion includes the variety of attacks, the motivations of the adventurers, and the impact on business and society. Prevention and mitigation strategies are discussed, including the need for investments in cybersecurity technologies, user education, and international collaboration. However, it is confirmed that cybersecurity will never be absolute, requiring an obligation of resilience and incident response plans. In the final analysis, we conclude the importance of a multifaceted approach in the prevention and mitigation of cyberattacks, as well as the need for collaboration between public and private organizations to effectively address this constantly evolving threat, using a literature review methodology, expanded on theoretical references published in physical and digital media.

KEYWORDS: Cyber-attacks; developments in crime; insufficiency of criminal law.

INTRODUÇÃO

Dentro das evoluções tecnológicas vivenciadas no Século XXI, sem dúvidas, a possibilidade de conexão ininterrupta traduz no direcionamento que se compreende na contemporaneidade do denominado “mundo” globalizado, impactando às relações pessoais e interpessoais que, atualmente, em grande parte, é desempenhada por intermédio de dispositivos eletrônicos (Freire e Almeida, 2015; Bastos, 2023).

De um lado, se a evolução da *internet*, com a ampliação das comunicações mundiais, foi decisiva para o desenvolvimento tecnológico identificado no final do século passado; de outro, a mesma evolução trouxe impactos no desenvolvimento dos crimes cibernéticos, reverberando em uma forma mais aprofundada de crimes que são desenvolvidos e utilizados a partir, única e exclusivamente, de dispositivos eletrônicos.

Isso porque, se de um lado os dispositivos ficam, em regra, conectados 24 (vinte e quatro) horas por dia; por outro lado, essa conexão ininterrupta, mesmo sem utilizações dos respectivos usuários, geram a exposição para os fins de ataques cibernéticos, que, em regra, são efetuados por mecanismos tecnológicos desconhecidos e eficientes que ocultam os reais criminosos e, por

vezes, implicam na utilização de dispositivos de pessoas comuns que estejam conectados à *internet*[3].

Deste modo, através da metodologia de revisão bibliográfica, ancoradas em publicados em meios físicos e digitais, busca-se, a partir da ciência de ataques cibernéticos, demonstrar a ineficácia da legislação penal para buscar os criminosos e a exposição de pessoas comuns que acabam, direta ou indiretamente, se envolvendo nos crimes, sem ter qualquer participação, apenas por manter-se eletrônicos conectados à *internet* (a exemplo dos roteadores das empresas de *internet*).

Nesse contexto, o presente estudo dividir-se-á em aspectos técnicos e jurídicos a fim de revisitar a bibliografia existente sobre o tema, fazendo breves considerações finais a respeito.

1. ATAQUES CIBERNÉTICOS

Os ataques cibernéticos são uma realidade cada vez mais presente em um mundo digitalmente interligado e analisá-los criticamente é essencial para compreender as suas implicações, consequências e as estratégias de prevenção e, quando ocorridos, mitigação dos seus efeitos.

Isso porque, os ataques cibernéticos são realidades que dialogam diretamente com os meios tecnológicos que subsistem no Século XXI, sendo certo que, segundo aponta Luiz Sérgio Dutra Nagli, a escala foi exponencialmente aumentada na pandemia decorrente do COVID-19 e o próprio isolamento social impostos em diversas nações, justificando que tais ataques não precisam, necessariamente, de pessoas operando o dispositivo, podendo ser alinhavados por dispositivos remotos (2022).

Desse modo, os principais mecanismos conhecidos para ataques cibernéticos são os *malware*, *phishing*, ataques de negação de serviço (DDoS), e, em últimas identificações, invasões de rede e roubo de dados, trazendo à tona a fragilidade que, além de expor os usuários, mostrando que o sistema de proteção das operadoras é frágeis, reverberam em consequências

[3] Grande parte dos crimes cibernéticos são feitos através de dispositivos remotos ou por meio de ocultação de IPs, em complexos arranjos que expõe a vulnerabilidade da rede, e, principalmente de seus usuários, refletindo aspectos penais, como o discutido no presente artigo, como aspectos de ineficiência da proteção da relação de consumo, implicando, pois, um arcabouço legislativo (brasileiro e mundial), ineficaz para a proteção contra os criminosos e exposição de dados de usuários comuns.

devastadoras que podem ser identificadas através de prejuízos financeiros ou imputação de pessoas comuns a fatos não cometidos[4].

Dentre os ataques cibernéticos conhecidos, é possível destacar o *phishing*: Este é um tipo de ataque de engenharia social que visa induzir os usuários a revelarem informações pessoais ou financeiras. Tais ataques geralmente são enviados por *e-mail* ou mensagens de texto, podendo se parecer com uma comunicação legítima de uma empresa ou organização confiável (Ramzan, 2010).

Por sua vez, também há os denominados ataques de injeção de SQL (5) em que busca explorar as vulnerabilidades em *sites* ou aplicativos que usam bancos de dados SQL. Os invasores podem injetar código SQL maliciosos em um campo de entrada e, em seguida, executar esse código no banco de dados. Isso pode permitir que eles roubem dados, excluam dados ou alterem dados no banco de dados (Zemke, 2012).

Também se verifica a existência de Ataques de sites cruzados (XSS) reverberado em uma eficaz forma de ludibriar os usuários a fim de que insiram seus dados, sendo uma forma de coleta, através JavaScripts maliciosos em um site e, em seguida, executar esse código quando um usuário visita o site. Isso pode permitir que eles roubem *cookies* de navegadores, redirecionem usuários para sites maliciosos ou disfarcem o site original (Bolivar, 2021).

Por sua vez, também se tem conhecimento dos ataques de negação de serviço (DoS), cujos mesmos visam sobrecarregar um *site* ou serviço com ataques volumétrico (alto tráfego), onde ele se torna indisponível para usuários legítimos. Os ataques DoS podem ser lançados de um único computador ou de um *botnet*, que é uma rede de computadores infectados com *malware* todos ao mesmo tempo (Laufer, Velloso, Duarte, 2005).

Estes são alguns dos ataques que se tem conhecimento dentro da literatura informática, não se tratando, decerto, apenas esses existentes, porquanto, a cada avanço tecnológico que é identificado, os mecanismos criminosos também são aprimorados, trazendo aspectos como a *dark net*, invasões de dispositivos que bastam estar conectados à rede para concretização,

[4] Comumente se verifica que atualmente se clonam dispositivos de celular, com fotos e aparente pessoas que, em verdade, são criminosos que simulam certo aspecto de veracidade e buscam, em verdade, proveitos econômicos. Outros fatos mais graves são as fragilidades sistêmicas, inclusive expostas por Edward Snowden quando declarou uma engenhosa rede de espionagem que atacou diversos governantes, inclusive, à época, a presidente brasileira em exercício (Scheirman, 2014).

utilização de IPs falsos ou de outrem, que dialogam com as preocupações das inúmeras formas de ataques cibernéticos conhecidas (Bastos, 2023).

O que se percebe, contudo, é o fato de que, da mesma foram em que a tecnologia é exponencialmente alterada em prol dos diversos avanços que, atualmente, refletem na própria forma de diálogo da sociedade, referido crescimento tecnológico não é um amplo espectro para novas formas contemporâneas de crimes cibernéticos, lesionando pessoas e empresas, sem que tais fatos possam ter a mesma eficácia no seu combate.

2. A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS

A evolução dos ataques cibernéticos é uma realidade preocupante para empresas em todo o mundo. Desde os primeiros vírus de computador até as sofisticadas campanhas de *phishing* e *ransomware* de hoje, porquanto se tornaram mais frequentes e sofisticados.

Na década de 80, surgiram os primeiros indícios dos ataques cibernéticos, marcando o início de uma era de desafios digitais para as empresas. Em 1983, o vírus "Elk Cloner" foi identificado como o primeiro vírus de computador a se espalhar de forma selvagem, afetando sistemas Apple II (Araújo, 2020).

Em 1988, o infame "worm Morris" se tornou o primeiro grande ataque de larga escala à internet, paralisando milhares de computadores conectados e demonstrando o potencial devastador das ameaças cibernéticas (Eisnberg, 1989). Na década de 90, testemunhou-se o surgimento dos primeiros grandes ataques cibernéticos, marcando o início de uma era de ameaças digitais (Oppermann).

Em 1998, o vírus "CIH" ou "Chernobyl" ganhou notoriedade ao destruir dados em milhares de computadores em todo o mundo, coincidindo com o aniversário do desastre nuclear de Chernobyl, demonstrando que, enquanto a tecnologia avançava, os mecanismos de vírus e ataques cibernéticos igualmente se modernizavam (Lima, 2017).

Ano após ano, se passa e os vírus exsurgem de forma mais exponencial do que a própria melhoria das tecnologias. Isso porque, no de 1999 marcou o surgimento do vírus "Melissa", que se espalhou rapidamente por e-mail e causou grandes problemas para empresas ao redor do mundo (Astani, Reichling, Schnitzler, 2012);

Na década de 2000, vimos também uma rápida evolução dos ataques cibernéticos, com ameaças cada vez mais sofisticadas afetando empresas em todo o mundo, em que um ataque de negação de serviço (DDoS) contra o provedor de serviços *online* Yahoo destacou a vulnerabilidade das grandes empresas à interrupção digital além de, no mesmo período, reportar os documentos que o vírus "ILOVEYOU" se espalhou rapidamente por *e-mail*, causando danos significativos a sistemas empresariais ao redor do globo (Pinto Ferreira, 2001).

Em 2007, o ataque à estatal estoniana por meio de um ataque DDoS foi um dos primeiros exemplos de um ataque cibernético usado como arma em conflitos entre nações, sendo anos mais tarde vivenciado tais ataques pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça, trazendo uma demasiada fragilidade do sistema de *internet* das instituições públicas, especialmente o Poder Judiciário que concentrou sua atuação no meio digital.

Ainda, o surgimento do *malware* Conficker em 2008 demonstrou a capacidade de infiltração e controle remoto avançados de sistemas (Zhang; Zhou; Chain, 2015), demonstrando que, a cada ano que se verificava a evolução dos sistemas de informação, sejam quais forem, os ataques cibernéticos também ficavam mais aprimorados.

Na década de 2010, os ataques cibernéticos se tornaram mais frequentes e sofisticados, representando uma ameaça significativa para as empresas em todo o mundo. Isso porque, em 2013, o ataque ao varejista Target por meio de malware de ponto de venda comprometeu milhões de informações de cartões de crédito, destacando os riscos associados à segurança de dados do cliente (Araujo, 2020).

Por sua vez, em 2014, tivemos o surgimento do *ransomware* CryptoLocker, que marcou uma nova era de extorsão digital, onde empresas eram alvo de sequestro de dados com exigências de resgate. (Adamov; Carlsson, 2017. p. 1-8) e em 2017, tivemos o ataque global do *ransomware* WannaCry, que afetou empresas e organizações em mais de 150 países, causando interrupções significativas nas operações e elevando o alerta para a gravidade das ameaças cibernéticas em larga escala (Mohurle, Patil, 2017).

Desse modo, a evolução tecnológica nos traz que os *hackers* estão constantemente inovando e suas técnicas para explorar vulnerabilidades em sistemas e redes empresariais, visando roubar informações confidenciais, interromper operações e exigir resgates ao passo que a legislação brasileira e mundial não acompanha tais inovações que busquem, de alguma forma, circundar a perseguição desses infratores.

Atualmente, além dos ataques cibernéticos, se combate uma rede de espionagem efetuada por dispositivos eletrônicos, trazendo novos aspectos as concentrações e, principalmente, as fragilidades sistêmicas, bem como, através do caso Edward Snowden, conforme identificou a pesquisa de Silas Antunes de Carvalho Gavetti (2021).

Portanto, o crescimento exponencial da tecnologia levou a uma severa e incontrolável onda de crescimentos de crimes que se desenvolveram a partir da perspectiva da era digital, não havendo um mecanismo certo, seja pela legislação, sejam pelos próprios conteúdos tecnológicos, de enfrentamento de frente da questão.

3. DISPOSITIVOS LEGISLATIVOS NACIONAIS E INTERNACIONAIS QUE BUSCAM COMBATER OS CRIMES CIBERNÉTICOS

Dentro da ideia de *Hard Law*, a Convenção de Budapeste sobre o Crime Cibernético é o documento internacional que busca alinhavar a ideia de uma corrente uníssona de combate às inovações dos crimes cibernéticos. Isso porque, é necessário anotar que os meios digitais não permitem, sobretudo, a ideia de soberania (absoluta), territorialidade e fronteiras, porquanto segue uma lógica distinta quando todo o ambiente digital é encontrado a partir de uma interconectividade que não prestigia a lógica de territorialidade (Bastos, 2023; Brasil, 2023).

Alder Thiago Bastos aponta que:

> Na atualidade existem dois documentos importantes no cenário internacional que refletem diretamente sobre uma sociedade equilibrada, preservando os referenciais da Declaração Universal de Direito Humanos, que são a Convenção de Budapeste sobre os Crimes Cibernéticos, de 2001, criada com o objetivo de obstar, em uma coalizão internacional, os crimes cibernéticos praticados no meio ambiente digital (2023. 278).

Deste modo, os direitos humanos, alinhavados pela Declaração Universal, alinham-se a ideia de uma conduta uníssona e inquestionável de preservação de preceitos basilares para a defesa de pessoas, frente aos desenvolvimentos contidos no mundo, buscando, a partir do cenário pós-bélico vivenciado pela Segunda Grande Guerra anotar premissas intransponíveis em prol da dignidade e da própria continuidade humana (Comparato, 2017, Bastos, 2019).

Portanto, a lógica seguida nos documentos Hard Law, como a Convenção de Budapeste, é justamente compreender que a própria tecnologia é aplicada em prol da humanidade, salientando-se que tais premissas fidelizam-se nos valores buscados através de diversas normas internacionais que anotam a prevalência de direitos humanos em detrimento de outros direitos.

Em outras palavras, conforme preciso posicionamento de Flávia Piovesan (2013, p. 205), a propósito, esclarece que:

> A Declaração Universal de 1948 objetiva delinear uma ordem pública mundial fundada no respeito à dignidade humana, ao consagrar valores básicos universais. Desde seu preâmbulo, é afirmada a dignidade inerente a toda pessoa humana, titular de direitos iguais e inalienáveis. Vale dizer, para a Declaração Universal a condição de pessoa é o requisito único e exclusivo para a titularidade de direitos. A universalidade dos direitos humanos traduz a absoluta ruptura com o legado nazista, que condicionava a titularidade de direitos à pertinência à determinada raça (a raça pura ariana). A dignidade humana como fundamento dos direitos humanos e valor intrínseco à condição humana é concepção que, posterior- mente, viria a ser incorporada por todos os tratados e declarações de direitos humanos, que passaram a integrar o chamado Direito Inter- nacional dos Direitos Humanos (2013, p. 205).

Dentro desse modelo referencial, a legislações do mundo avançam em seus territórios, na hercúlea busca de responsabilização (civil ou criminal) de situações enfrentadas no enredo tecnológico ou a partir da conectividade ininterrupta, alinhavando-se uma invencível tarefa de enfrentar a mesma criatividade em que os crimes avançam ao passo que os mecanismos tecnológicos se desenvolvem para a melhorias às vidas humanas.

Desse prisma, vale destacar o quanto alinhavado por Alder Thiago Bastos,

> Reflexos da internalização da Convenção de Budapeste sobre os Crimes Cibernéticos pode ser sentido no Brasil, pela Lei de nº 12.737/2012, que incluiu o tipo penal de invasão de dispositivo informático, nos artigos 154-A e 154-B no Código Penal ou pela Lei de nº 14.155/2021 que agravou as penas estabelecidas na Lei nº 12.737/2012, além de trazer a nova modalidade de estelionato pela fraude eletrônica (2023, p. 192).

Estreitando-se para o território nacional, a Lei dos crimes Cibernéticos 12.737/2012 apelidada com o nome da atriz Carolina Dickmann, referendando a invasão de seus dispositivos frente ao ataque cibernético, foi a primeira a relacionar invasão de computadores e celulares, violação de dados de usuários e interrupção de sites (governamentais ou não). Tal lei não só protege os cidadãos, mas sim, instituições comerciais, instituições financeiras e governamentais que constantemente vem sofrendo com invasões frequentemente vítima de ataques, golpes e roubo de dados.

Contudo, a grande questão não é a resposta a conduta criminosa em si, mas sim, atentar-se à materialidade e, principalmente, identificar a autoria dos criminosos, buscando a persecução penal, aliado ao próprio fato de que a lei, a priori, estabelece singelas respostas ao problema social identificado.

De outro lado, ainda há que se frisar sobre a Lei nº 12.965/2014 – Marco Civil sancionado em 2014 onde nascera, ao menos em tese, os deveres e direito dos usuários da rede.

Contudo, ainda que haja uma expectativa de que a lei salvaguarde aspectos sensíveis, ela não se trata de uma perseguição penal daqueles que utilizam as redes, tratando-se, em verdade, de uma legislação civil comum que, mais tarde, trouxe os enredos da Lei Geral de Proteção de Dados, não influenciando os atos criminosos praticados em redes sociais.

Portanto, ainda que haja combate à pornografia infantil, espelhando-se no Estatuto da Criança e do Adolescente que, em seu artigo 241-A, prevê expressamente a conduta criminosa desse ato nevrálgico, certo que às pessoas que se utilizam da "oferta, transmissão ou distribuição" desses conteúdos, jamais os fazem por meio de seus próprios dispositivos, trazendo articuladas formas a fim de que salvaguardem a ocultação de suas identidades e da própria prática criminal contida nesse cenário.

Ademais, dentro dos marcos legislativos brasileiros, foi promulgada a Lei nº 14.155/2021 alterou o Decreto Lei º 2848/1940, agravando-se as penas de invasão de dispositivos, furto qualificado e estelionato ocorridos em meio digital, conectado ou não à *internet*.

Contudo, ainda parece que os documentos legislativos internos e os documentos internacionais de espectro *Hard Law* são incipientes, porquanto, não traz uma resolução propriamente dita ao anseio de combate buscado pelos documentos internacionais, alinhavando-se à ideia de que a "internet", em pleno ¼ do Século XXI, permanece uma "terra de ninguém", permitindo-se condutas reprováveis e sem as respectivas sanções penais a respeito.

4. A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA

Deste modo, apesar de os textos legislativos demonstrarem preocupações com o desenvolvimento de ataques cibernéticos, historicamente, pela revisão de textos, eles não foram suficientes para coibir as diversas formas de ataques cibernéticos. Isso porque, partir-se de uma lógica, os criminosos não são presencialmente identificados pelas vítimas, sempre se mascarando através de programas e articulações que obnubile qualquer forma de identificação.

Ainda que atos sejam, em primeiro momento, consentidos, a mera utilização ou exposição pública dessas informações, não havendo como controlar o alcance quando alguma coisa chega à internet, torna-se um ato pernicioso e impacta a vida das pessoas que é dele vitimado (Salgado, 2021).

Nesse contexto, é redundante falar que se deve manter *software* e o sistema operacional atualizados a fim de garantir benefícios das correções de segurança mais recentes para proteger seu computador.

Deste modo, usar um antivírus ou uma solução de segurança de *internet* abrangente, como o Kaspersky, Avast, Norton, McAfee, são algumas formas inteligentes de proteger seu sistema contra os ataques. Os softwares de antivírus permitem que você verifique, detecte e remova ameaças antes que elas se tornem um problema. O uso dessa proteção ajuda a garantir a segurança de seu computador e seus dados contra crimes cibernéticos, dando a você mais tranquilidade.

Nesse contexto, mantenha-se o antivírus atualizado para obter o melhor nível de proteção. Levando-se em consideração o contexto abordado sobre o como combater o crime cibernético, temos que nos atentar a cada dia em utilizarmos senhas fortes que sejam difíceis de adivinhar e não as registre em lugar algum. Ou seja, então, facilite o processo usando um gerenciador de senhas de confiança para gerar senhas fortes aleatoriamente. Nem toda a população terá domino intelectual para acessar e manusear esta ferramenta, mas um combinado de 6 letras com 6 números misturados e não em sequência já ajudaria nesse processo, melhorando ainda mais com letras maiúsculas e minúsculas e caracteres especiais.

Uma maneira muito comum pela qual os computadores acabam infectados por ataques de malware e outras formas de crime cibernético é por meio de anexos em e-mails de spam. Nunca abra um anexo de um remetente que você não conhece.

É importante ser prudente e perceber o quanto antes que você foi vítima de um crime cibernético. Fique de olho nos seus extratos bancários e questione o banco sobre qualquer transação que pareça estranha. O banco poderá investigar que se trata de uma ação fraudulenta.

Portanto, demonstra-se que os mecanismos de proteção são da própria pessoa, não havendo políticas públicas ou repreenda criminal que possibilite o combate efetivo pelos meios legislativos, a prevenção se torna medida de rigor a fim de circundar ataques cibernéticos de quaisquer naturezas.

]

CONSIDERAÇÕES FINAIS

Este artigo, tem como objetivo investigar o desenvolvimento dos crimes e vulnerabilidade dos usuários e os ataques cibernéticos será fundamentada no Método Indutivo. Esse método parte da arte de observações específicas ou exemplos para formular uma conclusão geral. Se utiliza a generalização para chegar a princípios universais.

Primeiramente para a construção deste artigo será realizada uma revisão bibliográfica e análise de obras especificas que abrange tecnologias e tratados como o tratado de Budapeste que poderá nos nortear. O Brasil é muito pobre em conhecimento e legislação, então nós aderimos ao Tratado de Budapeste em 2023, após um longo processo de negociação e adequação da legislação interna. A adesão ao tratado foi um marco importante para o desenvolvimento da biotecnologia no país, pois facilita o acesso a recursos genéticos e incentiva a pesquisa e a inovação nesse campo. E outras ocorrências e boas práticas coletadas em outros países, que nos fazem potencializar e fortificar nossa legislação.

Com base nas nossas intuições para ver a onde o criminoso ou quais as possíveis arestas devemos cortas e afunilar para que não haja mais problemas ou erros a fim de preservarmos a sociedade e as instituições (Governo e Empresas) como um todo de possíveis prejuízos em todas as esferas.

Desta forma, todos os dados coletados serão analisados para que esse processo de investigação aperfeiçoamento possa contribuir para o avanço de ações e medidas para coibir essas infrações cibernéticas.

REFERÊNCIAS

ADAMOV; CARLSSON,. The state of ransomware. Trends and mitigation techniques. In: **2017 IEEE East-West Design & Test Symposium (EWDTS)**. IEEE, 2017. p. 1-8.

ARAÚJO, Franciele Cassimiro de; ROSSI, Jackeline Magrin. A evolução dos ataques cibernéticos. 2020. **Repositório Institucional do Conhecimento - RIC-CPS**. Disponível em: http://ric-cps.eastus2.cloudapp.azure.com/handle/123456789/5272. Acesso em: 05 abr. 2024.

ASTANI, Akram; REICHLING, Jürgen; SCHNITZLER, Paul. Melissa officinalis extract inhibits attachment of herpes simplex virus in vitro. **Chemotherapy**, v. 58, n. 1, p. 70-77, 2012.

BASTOS, Alder Thiago. **O Reconhecimento da Dimensão Autônoma do Meio Ambiente Digital em um Contexto Global**. New York: Lawinter Editions, 2023.

BOLIVAR, Toshiro Nagata et al. Análisis y optimización del proceso de validación de ataques de secuencia de comandos en sitios cruzados (XSS) empleando Burp Suite para evadir medidas de seguridad. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E39, p. 414-432, 2021.

BRASIL. Ministério Público Federal. Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. **Ministério Público Federal. Procuradoria-Geral da República** Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 26 jan. 2022.

CHANG, J. E. Análisis de ataques cibernéticos hacia el Ecuador. **Revista Científica Aristas**, p. 18-27, 2020.

COMPARATO, Fabio Konder. **A afirmação histórica dos direitos humanos**. 11ª Ed. São Paulo: Saraiva, 2017.

EISENBERG, Ted et al. The Cornell commission: on Morris and the worm. **Communications of the ACM**, v. 32, n. 6, p. 706-709, 1989.

FREIRE E ALMEIDA. Daniel. **Um tribunal Internacional para a Internet**. São Paulo: Almedina, 2015.

GAVETTI, Silas Antunes de Carvalho. **A ORGANIZAÇÃO INTERNACIONAL PARA A PROTEÇÃO DE DADOS PESSOAIS COLETADOS NA INTERNET EM ESCALA GLOBAL.** Dissertação apresentada à banca de defesa da Universidade Católica de Santos, como requisito para conclusão do curso de mestrado em Direito Internacional. Área de concentração: Direito Internacional. Orientador: Prof. Dr. Daniel Freire e Almeida, 2021.

LAUFER, Rafael P.; VELLOSO, Pedro B.; DUARTE, O. C. M. B. Um novo sistema de rastreamento de pacotes ip contra ataques de negação de serviço. In: **XXIII Simpósio Brasileiro de Redes de Computadores-SBRC'2005**. 2005.

LIMA, José Jeneci de. A segurança na navegação da internet: um estudo sobre o comportamento dos internautas na grande rede. 2017.

MOHURLE, Savita; PATIL, Manisha. A brief study of wannacry threat: Ransomware attack 2017. **International journal of advanced research in computer science**, v. 8, n. 5, p. 1938-1940, 2017.

NAGLI, Luiz Sergio Dutra. Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19 Pandemic in pandemic: the climbing of post COVID-19 cyber attacks. **Brazilian Journal of Development**, v. 8, n. 4, p. 28482-28493, 2022.

OPPERMANN, Daniel. **Governança multisetorial e o processo de governança da internet: um estudo de caso sobre crime cibernético e filtragem na internet entre 1990 e 2010. 2002. 264 f**. 2002. Tese de Doutorado. Tese de doutorado (Doutorado em Relações Internacionais). Instituto de Relações Internacionais, Universidade de Brasilia, Brasília.

PINTO FERREIRA. A Era da Informática e a Juscibernética. **Jornal o Judiciário**, p. 6-7, 2001.

PIOVESAN, Flávia. **Direitos Humanos e direito constitucional**, 14ª ed., rev. e atual. São Paulo: Saraiva, 2013.

RAMZAN, Zulfikar. Phishing attacks and countermeasures. **Handbook of information and communication security**, p. 433-448, 2010.

SALGADO, Rebeca Carneiro Costa Moura. Breve comentário sobre ciberespaço, pornografia de vingança e Convenção de Budapeste. *In*: **O Direito Digital em Temas Complexos e Internacionais.** p. 87-100. Organizado e Editado por FREIRE E ALMEIDA. Daniel. New York: Lawinter Editions, 2021.

SANTOS, Denise Tanaka dos. Delitos informáticos: Convenção de Budapeste. **Revista da Defensoria Pública da União**, v. 1, n. 04, 10 dez. 2018. Disponivel em: https://revistadadpu.dpu.def.br/article/view/159. Acesso em: 15 maio 2022.

SCHEUERMAN, William E. Whistleblowing as civil disobedience: The case of Edward Snowden. **Philosophy & Social Criticism**, v. 40, n. 7, p. 609-628, 2014.

SOUZA, Gills Lopes Macêdo. PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. ***Seminário Cibercrime e Cooperação Penal Internacional*** **1** (2009). Disponível em: https://www.mpam.mp.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf. Acesso em: 30 de março de 2022.

ZEMKE, Fred. What. s new in SQL: 2011. **ACM SIGMOD Record**, v. 41, n. 1, p. 67-73, 2012.

ZHANG, Changwang; ZHOU, Shi; CHAIN, Benjamin M. Hybrid epidemics—A case study on computer worm conficker. **PloS one**, v. 10, n. 5, p. e0127478, 2015.