doi.org/10.51891/rease.v9i11.12291

CRIMES CIBERNÉTICOS: DA INEFICÁCIA DA LEI CAROLINA DIECKMANN NA PRÁTICA DE CRIMES VIRTUAIS[1]

Adrielle da Silva Bispo[2]
Emanuel Vieira Binto[3]

RESUMO: Este presente artigo almeja abordar a ineficácia da Lei Carolina Dieckmann no enfrentamento dos crimes cibernéticos. Busca-se compreender os desafios enfrentados na aplicação da lei e propor medidas para aprimorar o combate aos crimes virtuais. Nesse contexto, o problema a ser enfrentado é: Com o avanço da tecnologia será que a legislação está sendo eficaz para identificar e reprimir os crimes virtuais? Para tanto, o objetivo geral deste estudo é analisar a eficácia da lei no combate dos crimes cibernéticos além disso, são objetivos específicos: Investigar a lacuna existente na legislação, analisar a realidade das ameaças virtuais e compreender os desafios na recolha de provas para processar os infratores. Esse estudo consiste em uma pesquisa bibliográfica e documental de cunho descritivo e explicativo tendo na sua metodologia a abordagem qualitativa, baseada em uma análise extensiva da literatura acadêmica, ordenamento jurídico, sites, artigos científicos, livros, relatórios de organizações internacionais e documentos legais relacionados ao tema. Diante de tudo, esta pesquisa aponta para a necessidade premente de atualização e aprimoramento da legislação existente, bem como para a implementação de abordagens multidisciplinares e colaborativas no combate aos crimes cibernéticos. A Lei Carolina Dieckmann, por si só, não é suficiente para enfrentar as ameaças virtuais em constante evolução. É essencial fortalecer a cooperação entre órgãos de aplicação da lei, promover a educação cibernética, sensibilizar o público sobre os riscos digitais e investir em tecnologias de segurança.

Palavras-chave: Crimes Cibernéticos. Lei Carolina Dieckmann. Segurança Digital.

[1]Artigo apresentado a Faculdade de Ciências Sociais Aplicadas, como parte dos requisitos para obtenção do Título de Bacharel em Direito, em 2023.

[2]Graduanda em Direito pela Faculdade de Ciências Sociais Aplicadas – FACISA, Itamaraju-BA – Email: m

[3] Professor-Orientador. Mestre em Gestão. Social, Educação e Desenvolvimento Regional, no Programa de Pós-Graduação STRICTO SENSU da Faculdade Vale do Cricaré - UNIVC (2012 -2015). Especialista em Docência do Ensino Superior Faculdade Vale do Cricaré. Possui graduação em Biblioteconomia E Documentação pela Universidade Federal da Bahia (2009). Possui graduação em Sociologia pela Universidade Paulista (2017-2020). Atualmente é coordenador da Biblioteca da Faculdade de Ciências Sociais Aplicadas da Bahia. Coordenador do NTCC FACISA,Pesquisador Institucional do sistema E-MEC FACISA, Recenseador do Sistema CENSO MEC FACISA. Coordenador do NTCC FACISA. Avaliador da Educação Superior no BASis MEC/INEP. ORCID: 0000-0003-1652-8152.

ABSTRACT: This article aims to address the ineffectiveness of the Carolina Dieckmann Law in combating cybercrimes. The aim is to understand the challenges faced in law enforcement and propose measures to improve the fight against virtual crimes. In this context, the problem to be faced is: With the advancement of technology, is legislation being effective in identifying and repressing virtual crimes? To this end, the general objective of this study is to analyze the effectiveness of the law in combating cyber crimes, in addition, the following are specific objectives: Investigate the existing gap in legislation, analyze the reality of virtual threats and understand the challenges in collecting evidence to prosecute criminals. offenders. This study consists of bibliographical and documentary research of a descriptive and explanatory nature, using a qualitative approach in its methodology, based on an extensive analysis of academic literature, legal system, websites, scientific articles, books, reports from international organizations and legal documents related to the theme. Overall, this research points to the pressing need to update and improve existing legislation, as well as to implement multidisciplinary and collaborative approaches to combating cybercrime. The Carolina Dieckmann Law alone is not enough to face constantly evolving cyber threats. It is essential to strengthen cooperation between law enforcement agencies, promote cyber education, raise public awareness about digital risks and invest in security technologies.

Keywords: Cybercrimes. Carolina Dieckmann Law. Digital Security.

INTRODUÇÃO

O Brasil passou por atualizações legislativas significativas no âmbito das leis de proteção de dados virtuais. Um exemplo disso é a Lei Carolina Dieckmann, também conhecida como lei 12.737/12. O tema falará exatamente sobre essa lei, embora tenha representado um avanço importante na regulamentação dos crimes cibernéticos no Brasil, iremos analisar os desafios significativos em sua aplicação prática. Pois a velocidade das mudanças tecnológicas, a complexidade das ameaças virtuais e a dificuldade de rastrear e identificar criminosos cibernéticos são alguns dos obstáculos que limitam a eficácia da legislação.

É importante ter em mente que os esforços para combater os crimes virtuais no Brasil nem sempre têm sido bem-sucedidos, como exemplificam as deficiências da lei 12.737/12 (também conhecida como Lei Carolina Dieckmann). A problemática está relacionada com os crimes virtuais que continuam a ocorrer diariamente e com o avanço tecnológico as agências responsáveis pela aplicação da lei não estão sendo eficiente para reprimir os infratores. Dado isso, o problema evidenciado será: Com o avanço da tecnologia será que a legislação está sendo eficaz para identificar e reprimir os crimes virtuais?

O objetivo geral deste estudo é analisar a eficácia da lei no combate dos crimes cibernéticos, visando uma compreensão mais elaborada. Além disso, os objetivos

específicos pautados foram investigar a lacuna existente na legislação, analisar a realidade das ameaças virtuais e compreender os desafios na recolha de provas para processar os infratores.

Diante exposto, fica evidente a importância do tema abordado. A capacidade da Lei Carolina Dieckmann de combater crimes virtuais tem sido questionada devido a diversos desafios e limitações. Estas preocupações levantam dúvidas sobre a capacidade das autoridades para fazer cumprir a lei, salvaguardar as vítimas e responsabilizar os cibercriminosos pelas suas ações. O que torna esse estudo de grande relevância. Pois iremos avaliar e medir a eficácia da Lei Carolina Dieckmann na dissuasão e na repressão de crimes cibernéticos. Identificar eventuais inadequações nas disposições da lei e apresentar sugestões para aumentar a resposta jurídica a estes tipos de crimes e torna-los mais eficaz.

A metodologia adotada consiste em uma pesquisa bibliográfica e documental de cunho descritivo e explicativo tendo na sua abordagem qualitativa, baseada em uma análise extensiva da literatura acadêmica, ordenamento jurídico, sites, artigos científicos, livros, relatórios de organizações internacionais e documentos legais relacionados ao tema.

O referencial teórico se divide em seis etapas, primeiramente iremos abordar sobre a historicidade dos crimes cibernéticos, a evolução da legislação conforme o grande avanço tecnológico mundial e o principal crime virtual cometido no Brasil, no segundo tem a caracterização e conceito do crime cibernéticos, no terceiro tópico, retrata sobre a lei Carolina Dieckmann trazendo surgimentos e conceitos, logo em seguida na quarta a ineficácia da lei 12.737/12, que não conseguiu suprir de forma eficaz deixando várias lacunas. Na quinta A lei da proteção de dados que regula as atividades de tratamento de dados pessoais, e por fim o direito à privacidade que é um direito fundamental para a humanidade, correspondente a um conjunto de dados contidos na vida pessoal, profissional e social do ser humano que não podem fugir ao seu domínio, com as práticas dos crimes virtuais muitas pessoas tem esse direto lesionado como foi o caso da Carolina Dieckemann.

Os resultados alcançados foram a demonstração da Lei Carolina Dieckmann representa um marco significativo nos esforços do governo brasileiro para fazer cumprir as regulamentações do crime cibernético. No entanto, a sua falta de eficácia na prática real realça a necessidade urgente de medidas suplementares, bem como de uma abordagem colaborativa e multidisciplinar.

O combate ao cibercrime exige uma estratégia abrangente que envolva a participação de governos, instituições, empresas e cidadãos. Somente trabalhando em conjunto, de forma sincronizada e sustentada, poderemos enfrentar os desafios em constante mudança colocados pelo cibercrime e criar um domínio virtual que seja seguro e confiável para todos.

1.METODOLOGIA

A Metodologia tem um papel indispensável na elaboração de um trabalho cientifico, pois ela é a sistematização da pesquisa. É a partir dela que conseguimos percorrer o caminho para chegar na construção de um estudo e alcançar os resultados esperados, tem como objetivo, organizar o conhecimento adquirido e auxiliar na criação e estruturação do trabalho cientifico. Se tornando a ferramenta mais importante para a construção de um projeto.

> A metodologia vai organizar a pesquisa, estabelecendo os caminhos a serem seguidos a fim de que se alcancem os objetivos. Ao escolhermos a metodologia, definimos o tipo de pesquisa a ser desenvolvida e como esse trabalho seguirá até sua conclusão: os passos a serem dados, os instrumentos utilizados e a forma como os dados de estudo serão coletados. (BLOISE, 2020, p. 02).

A abordagem utilizada nesta pesquisa foi a qualitativa pois Segundo Triviños, "a abordagem de cunho qualitativo trabalha os dados buscando seu significado, tendo como base a percepção do fenômeno dentro do seu contexto". (TRIVIÑOS, 1987, *apud*. OLIVEIRA, 2011, p. 25). Envolve um exame completo e organizado de uma ampla gama de fontes bibliográficas e documentais para determinar a eficácia da Lei Carolina Dieckmann no que diz respeito à prevenção e punição de crimes cibernéticos. Também tem o caráter descritivo e explicativo, trazendo fundamentos lógicos para melhorar a resposta legal a estes crimes.

> Quando se diz que uma pesquisa é descritiva, se está querendo dizer que se limita a uma descrição pura e simples de cada uma das variáveis, isoladamente, sem que sua associação ou interação com as demais sejam examinadas. (CASTRO, 1976, p. 66. *Apud*. OLIVEIRA, 2011, p. 22)

O local de estudo será o próprio contexto Nacional com as legislações pertinentes ao assunto, delineando uma pesquisa voltada à aplicabilidade da Lei Carolina Dieckmann no contexto dos crimes cibernéticos bem como as lacunas pertinentes na legislação. Ao realizar uma revisão abrangente da literatura, é possível aprofundar a complexa relação entre os estatutos jurídicos brasileiros e a questão cada vez mais difundida da atividade

criminosa virtual. Esta análise crítica fornece informações valiosas sobre os desafios enfrentados na prática.

O surgimento para realização dessa pesquisa começou a partir da curiosidade de saber como a legislação faz para identificar e punir criminosos que agem por meio virtual e se as vítimas são resguardadas de forma eficiente. A partir daí, foram utilizados diversos recursos, incluindo bases de dados acadêmicas e mecanismos de busca online como Google Scholar, PubMed, Lilacs e Scielo. A seleção criteriosa de palavras-chave específicas, como "crime cibernético", "Lei Carolina Dieckmann", "segurança digital" e outros termos relacionados, foi de extrema importância para identificar o tema em questão.

1.BREVE HISTÓRICO DOS CRIMES CIBERNETICOS

O presente capitulo ira retratar a historicidade dos crimes virtuais para isso iremos voltar na década de 1960 Segundo Jesus: "Para a doutrina internacional, os crimes virtuais tiveram início na década de 1960, quando foram identificadas as primeiras referências sobre o tema, cuja maior parte foi de delitos de alteração, cópia e sabotagem de sistemas computacionais. " (JESUS, 2016, p. 17. *Apud.* VIEIRA, 2021, p. 2). Tendo as condições técnicas ruins na época era até difícil detectar o autor.

No ano de 1980, foi quando aconteceu o maior alastramento dos mais diferentes delitos pertinentes aos crimes cibernéticos. Foi nessa época que identificaram várias ações criminosa com a utilização de meios virtuais, a pirataria de programas foi uma das ações cometida na época.

> Na década de 70 a figura do Hacker já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso à necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo. (CARNEIRO, Adeneele Garcia, 2017. *Apud.* VIEIRA, 2021, p. 2).

Foi a partir daí que começaram a surgir as primeiras legislações para regulamentar a pratica dos crimes ilícitos. "Por mais uma vez, os Estados Unidos da América foram pioneiros no assunto, quando em 1984 editaram a legislação "Crime Control Act" e logo em seguida o "Computer Fraud and Abuse Act, em 1986". (ASSIS 2016, p. 16).

A Alemanha, em 1986, editou a Lei "Computer Kriminalitat", seguida da Franca que em 1988 editou a Lei Godfrain. Posteriormente, em 1995 a Espanha incluiu crimes de informática na reforma do seu Código Penal. (ASSIS 2016, p. 16).

Em 2001, o Conselho da Europa, elaborou a Convenção Europeia sobre Crimes Cibernéticos, objetivando uniformizar a legislação europeia quanto à política criminal dos crimes cibernéticos.

No Brasil, inicialmente o tema foi tratado como uma questão de direito penal, e editada em 1987 sendo a Lei n.º 7.646/87, cuja finalidade é a proteção à propriedade intelectual sobre programas de computador e sua comercialização no país.

> O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, leis relativas à competência do Estado sobre questões de informática. (CARNEIRO, Adeneele Garcia, 2017. *Apud.* VIEIRA, 2021, p. 3).

A Lei n.º 8.137/1990, foi editada, o qual define crimes praticados contra a ordem tributária. E na edição da Lei n.º 9.883/2000, passou a abranger a regulamentação de outros delitos relacionados à internet que não sejam de ordem econômica. A respectiva legislação tem a finalidade de proteger os dados e os sistemas de informação, punindo principalmente os crimes próprios de funcionários públicos que violem o sistema de informação da Administração Pública.

Recentemente houve a edição da Lei n.º 12.695/2014 foi sancionada pela presidente Dilma Rousseff o qual estabelece princípios, garantias, deveres e direitos aos usuários da internet assegurando uma maior proteção aos usuários da internet.

No Brasil ocorrem todos os tipos de ataques cibernéticos, incluindo ataques de phishing, que tornaram o país o mais afetado globalmente.

A palavra phishing é derivada da palavra pesca, que se refere ao ato de pescar. No contexto da segurança informática, phishing refere-se a uma mensagem enganosa enviada a vários indivíduos.

> O termo é originado do verbo inglês to fish que significa pescar e caracteriza a conduta de pesca de informações de usuários. Inicialmente, a palavra phishing era usada para definir a fraude de envio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Uma de suas características é que as mensagens estimulam ser de pessoas ou instituições legítimas como bancos, órgãos governamentais ou empresas. Hoje, a palavra também é utilizada para definir a conduta de pessoas que encaminham mensagens com a finalidade de induzir vítimas a enviar informações para os criminosos. (OTSU, Denise Pereira,2023, p. 22.)

De acordo com a análise de Pereira e Martins (2014), o phishing em sites de encontros tornou-se uma forma cada vez mais prevalente de crime cibernético, muitas vezes considerado como o método preferido de ataque. Nesse esquema, os invasores enviam uma mensagem projetada para ser compartilhada, infectando assim todos aqueles

que a acessam. Este método não apenas aumenta a probabilidade de contaminação, mas também explora a confiança estabelecida entre conhecidos que podem compartilhar involuntariamente um arquivo de phishing.

A prevalência deste tipo de ataque aumentou, resultando num aumento significativo no número de vítimas em todo o mundo. Essa tática ameaçadora abrange diversas formas de ameaças, como fraude, chantagem, roubo de identidade, perseguição e clonagem de cartões. Acredita-se que esta abordagem tenha se tornado a técnica preferida para a extração de informações, com uma taxa de utilização que aumentou mais de 60% entre aqueles que a praticam (CORTELA, 2013).

De acordo com uma pesquisa realizada pela Kaspersky, (2018), o Brasil é classificado como o principal país do mundo em ataques de phishing. Esse ranking foi consolidado no ano anterior, quando se descobriu que quase 30% dos usuários de internet no Brasil haviam sido alvo de pelo menos uma tentativa de phishing. Embora o número deste ano tenha diminuído para 23%, o Brasil manteve sua posição de liderança, sendo o phishing via WhatsApp o método mais utilizado.

1.CONCEITO E CARACTERIZAÇÃO DOS CRIMES CIBERNETICOS

O presente capitulo ira retratar o conceito e caracterização dos crimes cibernéticos. Os crimes cibernéticos têm várias nomenclaturas, podendo ser chamados também de crimes de internet. Segundo Antônio Chaves, cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação" (CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático, p. 19). Com tudo, podemos chegar na conclusão de que o crime cibernético está relacionado a condutas ou atividades criminosas que envolvem um computador ou dispositivo móvel com acesso à rede. Fabrizio Rosa conceitua o crime cibernético, como sendo:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O Crime de Informática é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos 10 crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua

> transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53).

Existe uma classificação que divide os crimes cibernéticos em dois tipos: os Crimes Cibernéticos Próprios e os Crimes Cibernéticos Impróprios. Nos crimes próprios a execução do crime e a consumação só podem ser praticados na informática "São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados) ". (VIANA, 2003). São exemplos os famosos "hackers".

Já os Crimes Cibernéticos Impróprios são aqueles que estão tipificados no Código Penal, pois violam bens jurídicos comuns, ferem à dignidade da pessoa humana, entre outros crimes que são praticados através do meio informativo.

1. LEI CAROLINA DIECKMANN

Depois de compreender as ideias-chaves por trás do crime cibernético, bem como a historicidade, conceito, classificação e a evolução da lei no Brasil e no mundo, podemos agora discutir quais ações os indivíduos podem tomar para se protegerem.

A Lei do Crime Cibernético, também conhecida como Lei Carolina Dieckmann, foi a legislação inicial para categorizar crimes digitais, como acesso não autorizado a computadores e dispositivos móveis, violação de informações do usuário e interrupção de plataformas online. Esta lei é identificada como Lei nº 12.737/2012.

É imprescritível falar de crimes cibernéticos e não relatar o caso da atriz Carolina Dieckmann. A lei ganhou esse nome devido a um caso de grande repercussão envolvendo a atriz, no qual suas fotos privadas vazaram online por meio de um e-mail infectado por vírus. Isto levou à classificação de tais invasões como crime, especificamente aquelas cometidas sem o consentimento ou autorização da vítima.

Depois do ocorrido em momentos mais de calma relata em uma entrevista para o Jornal Nacional diante da apresentadora Patrícia Poeta Carolina Dickemann discorre que foi momentos de desespero e euforia "acho que agora vou poder voltar a viver, porque minha vida estava em suspenso"G1.com (2012).

A lei proíbe o acesso não autorizado a informações ou dados pessoais de pessoas físicas ou jurídicas por meio de dispositivos eletrônicos como celulares, tablets e computadores, estejam ou não conectados à internet. Também proíbe a eliminação ou alteração dos referidos dados sem a devida autorização (NASCIMENTO, 2016).

A lei, apesar dos seus efeitos positivos, também teve consequências negativas, como salientaram alguns especialistas. Eles criticam a lei por suas punições brandas e por só criminalizar o ato de acessar dados caso uma barreira seja violada. Isso significa que se alguém acessar dados que estão disponíveis gratuitamente, como um celular desbloqueado, não é considerado crime. (NASCIMENTO, 2016).

O advogado e ex promotor de justiça Eudes Quitino de são Paulo publicou em um artigo a seguinte prerrogativa:

> Extrai-se do texto legal a finalidade de incriminar a conduta do agente que invade, driblando os mecanismos de segurança, e obtém, adultera ou destrói a privacidade digital alheia, bem como a instalação de vulnerabilidades para obtenção de vantagem ilícita. Observa-se, contudo, a necessidade da existência de um mecanismo de segurança no sistema do aparelho, uma vez que a lei condiciona a ocorrência do crime com a violação indevida deste. Assim, a invasão do dispositivo informático que se der sem a violação do mecanismo de segurança pela inexistência deste será conduta atípica. Por tal razão torna-se cada vez mais importante proteger os aparelhos com antivírus, firewall, senhas e outras defesas digitais. (JUNIOR, 2012)

Ou seja, mesmo com a lei tipificada é importante os usuários se proteger com antivírus, senhas e outros meios de segurança virtuais para poder evitar esses tipos de ataques.

INEFICACIA DA LEI CAROLINA DIECKMANN

Verificando a lei, e possível identificar uma grande lacuna existente nela seja na punição ou na produção de provas, apesar da lei acrescentar e modificar artigos do Código Penal. O advogado criminalista Luiz Augusto Sartori de Castro diz: "ausência de definição de diversos termos técnicos inseridos na lei, o que também inviabiliza a aplicação do tipo penal comentado". Como exemplo cita o artigo 154-A do Código Penal, no qual se faz a abordagem da invasão de sistemas informáticos, "vê-se que faltou suporte técnico-jurídico aos legisladores na redação dos dispositivos", "Quando a discussão chegar ao Poder Judiciário, deixará de ser punida a grande parcela daqueles que acessam indevidamente sistemas de informática. Isso porque não o fazem à força, como exige o tipo penal ao se valer do verbo invadir"(CASTRO *apud,* SÁ, 2021, p. 11).

Com tudo, para fazer valer o crime precisa ser violado o mecanismo de segurança primeiro. Vale salientar que até hoje não há uma definição de quais mecanismo de segurança são esses. E caso o dispositivo não tiver esses mecanismos a vítima vai ser violada e não haverá punição? Vários doutrinadores se questionam sobre essa questão.

> Diante de tantas lacunas, a lei apesar da sua importância, não consegue amparar boa parte da sociedade, pois umas parcelas de indivíduos são leigas em relação a

> dispositivos de segurança ou até mesmo não possuem recursos suficientes para arcar com a instalação de programas, como antivírus ou quaisquer outros que sirvam como forma de proteção pessoal dos seus dados. (SÁ, 2021, p. 11).

Mesmo que a lei foi um marco para o sistema jurídico brasileiro a lei é muito criticada por alguns doutrinadores, principalmente no tempo mínimo para a aplicação da pena, sendo abaixo de 1 ano. Sendo de menor potencial ofensivo amparado pela lei 9.099/95.

> Esta pena autoriza a suspensão condicional do processo, desde que, o autor tenha condenação ou processo por outro crime. Desta forma, retira o caráter de gravidade dos danos que causam a ação. E assim, não consegue atingir o objetivo principal que é de inibir os criminosos a realizar conduta, e havendo a ocorrência de crime, possibilitar uma punição de acordo com a agressão sofrida. (SÁ, 2021, p. 11).

A principal crítica ao sistema jurídico é a sua incapacidade de impor sanções mais severas àqueles que cometem crimes cibernéticos. As penalidades estabelecidas pela lei para acesso não autorizado a informações e hackers são relativamente brandas, com penas que variam de três meses a um ano de prisão. Isto é amplamente considerado inadequado para desencorajar futuros infratores, especialmente em situações em que os prejuízos do crime podem ser consideráveis, esses crimes devem ser julgados com agilidade pois possuem uma pena mínima, caso isso não aconteça, não haverá punição, por motivo de prescrição.

Em resposta a estas inadequações, numerosos especialistas e defensores dos direitos cibernéticos afirmam que é necessária uma abordagem unida dos legisladores, das agências responsáveis pela aplicação da lei e do campo tecnológico. Isto exige o estabelecimento de legislação mais robusta, a sensibilização, a garantia de recursos suficientes para investigações, a defesa da colaboração internacional e, o mais importante, a educação dos indivíduos sobre a segurança digital e o reconhecimento da atividade criminosa. A eficácia da Lei Carolina Dieckmann na prática de crimes cibernéticos persiste como um ponto significativo de discussão no domínio em constante mudança do crime cibernético (NASCIMENTO, 2016).

1. LEI DE PROTEÇÃO DE DADOS PESSOAIS

A lei geral de proteção de dados pessoais (LGPD), é uma legislação que trata sobre a proteção dos dados pessoais, nesse mundo cada vez mais virtuais que vivemos muitas empresas e organizações governamentais precisam de nossos dados para nos prestar algum tipo de serviço. Com isso será que nossos dados fornecidos estão protegidos? Será que essas

informações serão passadas para outras instituições? Então, são essas e outras questões que a lgpd visa regular no âmbito das informações que tramitam no território brasileiro, incluindo as empresas que mesmo não estando localizada fisicamente, oferecem serviços em nosso território brasileiro.

> Os avanços tecnológicos trazidos pela era digital, fizeram com que as informações coletadas pelas empresas e instituições (pública e privada), se tornassem valorosos ativos para o aspecto econômico. Esse movimento demandou uma nova visão, ao celebrar a informação como um bem valioso, e sua proteção, uma prioridade. Nesse espaço compreendido como era digital, diversos países se viram diante da necessidade de elaborar leis como forma de regulamentar o tratamento, disponibilidades, acessibilidade e uso desses bens, os dados pessoais e informações. (SOARES, 2022.)

O objetivo da LGPD é disciplinar e regulamentar o uso dos dados pessoais mantidos por empresas e órgãos governamentais, afim que se evitem abuso contra aqueles que confiarem a suas informações pessoais sobre a sua guarda. Todas as organizações públicas ou privadas que detém dados pessoais de pessoas naturais, com o objetivo de oferecer ou ter que prestar serviços, estão sujeitos ao regramento da LGPD. Caso não cumpra o dever de resguardar, proteger, e utilizar os dados apenas para as atividades autorizada ou necessária para a prestação de serviço poderão se sujeitar a penalidade da lei, incluindo multas ou suspenção de atividade.

Nos tempos modernos, há uma tendência crescente de utilização de uma rede de dispositivos interconectados que funcionam em conjunto com outros dispositivos e pessoas. Estas ferramentas podem ser monitorizadas e reguladas, mesmo à distância, para otimizar a eficácia dos sistemas e procedimentos. Isto leva a um melhor padrão de vida para a população (TEFFÉ, 2018).

Embora a Internet proporcione certamente oportunidades valiosas para a educação, simplifique as rotinas diárias, auxilie nos procedimentos médicos, melhore a segurança doméstica e eleve a qualidade e a acessibilidade de produtos e serviços, também é vulnerável a questões relacionadas com a privacidade e a segurança da informação. É crucial ter em conta o tipo de tratamento que os dados pessoais e a privacidade dos utilizadores recebem (TEFFÉ, 2018).

Os dados e informações que nos dizem respeito estão espalhados por diversas fontes, incluindo, mas não se limitando a: registros de registro nas entradas dos edifícios, informações de cartão de crédito em sites de varejo on-line, resultados de diagnósticos e exames coletados por laboratórios, pegadas digitais deixadas na internet, e informações de voz e texto armazenadas por operadoras de telefonia. Inúmeras pessoas e organizações têm

acesso a fragmentos das nossas informações pessoais, criando uma rede complexa de dados fragmentados (FREITAS, 2020).

> O conceito de proteção de dados centra-se na salvaguarda da personalidade do indivíduo, e não nos seus bens. É um direito pessoal e de segurança que é parte integrante da experiência humana, pois é uma expressão tangível da liberdade e da dignidade de um indivíduo (FREITAS, 2020).

Sem dúvida, a internet ampliou a disponibilidade de informações e facilitou o compartilhamento de dados. No entanto, a estrutura das redes dentro das organizações, bem como das instituições públicas, tem levado a uma invasão da privacidade tanto de clientes como de cidadãos em busca de informações pessoais.

Como tal, a Internet representa uma ameaça significativa à privacidade dos indivíduos, pois permite aos prestadores de serviços trocar informações e monitorizar o comportamento virtual dos utilizadores na rede.

Os termos "dados" e "informações" são vastos e suas definições variam nas diferentes legislações dependendo do ponto de vista de cada país, conforme afirma (FREITAS, 2020).

1.DIREITO A PRIVACIDADE

Nesse tópico iremos discorrer sobre o direito à privacidade. É um direito fundamental para a sociedade, pois existem um conjunto de dados contido na vida pessoal ou profissional do ser humano que de certa forma não podem fugir do seu controle. Sabemos que com a evolução do mundo digital, muitas pessoas acabam fornecendo dados sem ao menos pensar no dando que aquilo pode lhe trazer.

O mundo digital proporciona aos indivíduos acesso a uma infinidade de informações, desde básicas até altamente confidenciais. Muitas vezes, os usuários não têm consciência de que estão fornecendo essas informações e não consideram até que ponto estão se expondo à comunidade em geral (MARINELI, 2019).

O ordenamento jurídico defende o valor da privacidade, conforme delineado no item 5 de seus fundamentos: o respeito à privacidade das pessoas. Isso é estabelecido pela proteção da privacidade do indivíduo pelo sistema jurídico nacional, conforme estabelecido na Lei 13.709 de agosto de 2018 no Brasil.

> A capacidade de manter a privacidade é um aspecto essencial do desenvolvimento pessoal, pois permite que os indivíduos afirmem a sua identidade única na sociedade sem serem condenados ao ostracismo. Este direito à privacidade também implica o direito de regular as informações que lhe dizem respeito (FERNANDES, 2017)

A salvaguarda de informações e declarações pessoais é crucial para proteger o direito à privacidade. O acesso não autorizado a tais informações não só revela dados pessoais como também viola os direitos do titular.

É evidente que a utilização de uma vulnerabilidade, independentemente de ser ditada por uma autoridade ou entidade válida para fins razoáveis, cria oportunidades para intervenientes malévolos intercederem na comunicação ou serviço em funcionamento. Suas intenções podem ser causar danos ou apreender valor de dados pertencentes a terceiros (DONEDA, 2020).

> Notavelmente a internet apresenta inúmeras vantagens e benefícios para as pessoas, vez que reduziu as distâncias entre as mesmas, possibilitando a realização de relações sociais e comerciais entre as pessoas e nações que estão conectadas a rede, o que, de fato, possibilitou um imenso crescimento econômico dos países que estão conectados à internet. (NASCIMENTO, Natalia Lucas, 2016, p. 15)

Na contemporaneidade, a ameaça mais significativa à privacidade pessoal é o comércio. Devido à comercialização do mundo digital, os dados pessoais tornaram-se o bem mais valioso do mercado. As empresas aproveitam estes dados para acompanhar a vida dos indivíduos, criando bases de dados que contêm várias características pessoais, incluindo atributos físicos, situação económica, perfil psicológico e opiniões religiosas e políticas.

Embora algumas informações privadas sejam fornecidas voluntariamente em plataformas digitais por meio de cadastros em aplicativos, redes sociais e e-commerce, as empresas também utilizam outros métodos para coletar informações. Esses métodos incluem rastrear a localização GPS de celulares, analisar cookies e arquivos de internet armazenados temporariamente, além de monitorar hábitos de acesso. Consequentemente, as publicidades em sites e aplicações, pop-ups e outros meios digitais são personalizadas de acordo com as informações recolhidas (VALPORTO, 2017).

CONCLUSÃO

Ao concluir a investigação sobre a eficácia da Lei Carolina Dieckmann na prevenção e punição dos crimes cibernéticos, fica evidente que a legislação atual encontra obstáculos consideráveis na aplicação prática. Apesar da sua criação com a intenção de dissuadir condutas ilícitas no domínio digital, a natureza complexa e em constante mudança dos crimes cibernéticos expõe deficiências significativas.

É crucial reconhecer que a eficácia da Lei Carolina Dieckmann depende não apenas das suas disposições legais, mas também da boa execução de tais disposições, reforçando as competências investigativas e estabelecendo a cooperação internacional entre as agências de aplicação da lei. Além disso, é imperativo tomar medidas para aumentar a compreensão e a educação relativamente à segurança digital para reduzir a suscetibilidade da sociedade ao crime cibernético.

A presente pesquisa buscou mostrar a complexidade dos crimes cibernéticos, representa um obstáculo significativo para as agências responsáveis pela aplicação da lei em todo o mundo. Um dos maiores obstáculos é a natureza global e em constante mudança destes crimes, muitas vezes envolvendo múltiplos perpetradores localizados em diferentes jurisdições. Isto representa um desafio em termos de identificação, investigação e repressão de criminosos cibernéticos. Além disso, o ritmo acelerado dos avanços tecnológicos no ciberespaço torna difícil para os regulamentos acompanharem as novas ameaças e técnicas, complicando ainda mais a tarefa das agências responsáveis pela aplicação da lei.

Apelidada de "Lei Carolina Dieckmann", a Lei no 12.737, de 30 de novembro de 2012, A lei proíbe o acesso não autorizado a informações ou dados pessoais de pessoas físicas ou jurídicas por meio de dispositivos eletrônicos. A lei é fruto de projeto apresentado pelo Deputado Federal, cujo trâmite foi acelerado depois da invasão, subtração e exposição na internet de fotografias íntimas da atriz Carolina dieckemann, motivo pelo qual a lei ganhou essa nomenclatura.

A Lei Carolina Dieckmann foi um marco importante para esfera digital no país Entretanto a Lei tem algumas deficiências em seu texto legal, que são muito questionadas pelos juristas, apontando como o maior defeito á aplicação da pena branda, com isso concluímos que a legislação brasileira está bem longe de dar a devida proteção e alcançar a justiça para os usuários.

Com o desenvolvimento da tecnologia, as pessoas passaram a exercer mais funções on-line. Isso mostra como a privacidade na internet se tornou ainda mais importante para a sociedade. A Lei Geral de Proteção de Dados (13.709/2018) no Brasil tem papel importante estabelece uma estrutura legal de direitos dos (as) titulares de dados pessoais. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais realizado pelo órgão ou entidade.

Portanto, a ausência de educação sobre segurança cibernética e a negligência na salvaguarda de informações pessoais ainda deixam indivíduos e organizações vulneráveis a riscos consideráveis. A lei 13.737/12 Mesmo sendo uma grande conquista para o sistema jurídico brasileiro, no entanto deixou lacunas, nas quais existe uma necessidade grande de fazer alteração para concertar as lacunas trazendo assim uma melhor segurança e amparo jurídico na sua aplicabilidade e a vista disso tornando a Lei eficaz.

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Acesso em: 13 de agosto de 2023.

BRASIL. 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.** Acesso em: 13 de agosto de 2023.

BARROS, Bruno Mello Correa de; BARROS, Clarissa Teresinha Lovatto; OLIVEIRA, Rafael Santos de. **O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais**. 2017. Acesso em: 13 de agosto de 2023.

CORTELA, J. J. C. **Engenharia social no Facebook.** 2013. Acesso em: 01 de setembro de 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 2. Ed. São Paulo: Thomson Reuters Brasil, 2021. Acesso em: 01 de setembro de 2023.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional.** 2017. Acesso em: 01 de setembro de 2023.

FREITAS, Daniel Paulo Paiva**. Proteção e governança de dados Curitiba**, Contentus, 2020. Acesso em: 03 de setembro de 2023.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. Acesso em: 03 de setembro de 2023.

MORGENSTERN, G. G.; TISSOT, T. R. G. **Crimes cibernéticos: phishing – privacidade ameaçada**. In: SEMINÁRIO DE INICIAÇÃO CIENTÍFICA, 23., 2015. Acesso em: 03 de setembro de 2023.

MARINELI, Marcelo Romão. **Privacidade e redes sociais virtuais: sob a égide da Lei 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2018** – Lei Geral de Proteção de Dados Pessoais. 2019. Acesso em: 20 de setembro de 2023.

NASCIMENTO, Lucas Sousa do. **O POPULISMO PUNITIVO E A LEI CAROLINA DIECKMANN.** 2016. Acesso em: 20 de setembro de 2023.

PEREIRA, L. de D.; MARTINS, D. M. S. **Engenharia social: segurança da informação aplicada à gestão de pessoas – estudo de caso**. 2014. Acesso em: 12 de outubro de 2023.

TEFFÉ,Chiara Spadaccini de. **Proteção de dados pessoais na Rede: resenha à obra "A internet das coisas"**, de Eduardo Magrani. 2018. Acesso em: 12 de outubro de 2023.

VIANA, Igor Bonfim. **A proteção de dados pessoais na internet à luz do direito pátrio**. 2018. Acesso em: 12 de outubro de 2023.

VALPÔRTO, Ângela. **Privacidade na internet: o uso de dados na publicidade**. 2017. Acesso em: 07 de novembro de 2023.

BLOISE, Denise. **A importância da metodologia científica na construção da ciência.** Researchgate, 2020. Disponivel em: ‹https://www.researchgate.net/publication/342462072_A_importancia_da_metodologia_cientifica_na_construcao_da_ciencia›. Acesso em: 07 de novembro de 2023.

NASCIMENTO, Natalia Lucas. **Crimes cibernéticos**. Cepein, 2016. Disponivel em ‹https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf›. Acesso em 07 de novembro 2023.

Oliveira, Maxwell Ferreira. **METODOLOGIA CIENTÍFICA: um manual para a realização de pesquisas em administração**. Files, 2012. ‹https://files.cercomp.ufg.br/weby/up/567/o/Manual_de_metodologia_cientifica_-_Prof_Maxwell.pdf›. Acesso em 15 de novembro 2023.

OTSU, Denise Pereira. **CRIMES CIBERNÉTICOS E OS LIMITES DA LIBERDADE DE EXPRESSÃO NAS REDES.** Repositorio, 2023. ‹https://repositorio.animaeducacao.com.br/bitstream/ANIMA/35166/1/CRIMES%20CIBERNE%CC%81TICOS%20%281%29.pdf›. Acesso em 20 de novembro de 2023.