FACULDADE DE INHUMAS
CENTRO DE EDUCAÇÃO SUPERIOR DE INHUMAS

CURSO DE DIREITO

ANA LUIZA BRANDÃO CALIL POMPEU

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEI CAROLINA DIECKMANN

INHUMAS-GO
2022

ANA LUIZA BRANDÃO CALIL POMPEU

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEI CAROLINA DIECKMANN

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.
Professor (a) orientador (a): Fernando Emídio dos Santos.

INHUMAS – GO
2022

ANA LUIZA BRANDÃO CALIL POMPEU

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEI CAROLINA DIECKMANN

AVALIAÇÃO DE DESEMPENHO DO(S) ALUNO(S)

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.

Inhumas, 06 de maio de 2021.

BANCA EXAMINADORA

_____

Prof Fernando emídio dos Santos – FacMais
(orientador(a) e presidente)

_____

Profª Jullyana Macedo Rego – FacMais
(Membro)

Dedico esta monografia à minha mãe, por sempre estar ao meu lado dando-me sustento. Ao meu pai, Luiz Rogério (in memorian), e aos meus avós: Tereza, Edmundo e Luiza (in memoriam), que já não estão presentes aqui, os quais sempre me deram forças e, com certeza, continuam me proporcionando de onde estão. E, ainda, ao meu eterno namorado, Franciolly Filho, por estar sempre me amparando.

AGRADECIMENTOS

Primeiramente a Deus, por me dar forças e não me deixar perder a fé mediante a todos os obstáculos que enfrentei até aqui.

Aos meus pais, principalmente, à minha mãe, por estar presente em todos os momentos da minha vida e ser o meu ponto motivador e nunca me deixar desistir. Ao meu pai, que mesmo não presente em minha vida, me concedeu forças de onde estava.

Aos meus avós, que sempre foram essenciais na minha formação/ criação,,os quais gostaria que estivessem presentes nesse momento de uma das maiores conquistas de minha vida.

Ao meu namorado, que não me deixou desistir e sempre me motivou.

Aos meus amigos, que nunca me deixaram desamparada e estiveram aqui ,constantemente,arduamente ao meu lado.

Ao professor, Fernando Emídio, pela e orientação contínua, sempre dedicado e paciente. À professora Elizabeth, por ter se comportado como uma mãe na reta final da minha graduação e ter me proporcionado todo o suporte de que necessitava.

“A lei é inteligência, e sua função natural é impor o procedimento correto e proibir a má ação”. (CÍCERO).

LISTA DE ABREVIATURAS E SIGLAS

ABNT Associação Brasileira de Normas Técnicas

RESUMO

O avanço tecnológico que aconteceu ao longo dos anos, trouxe novidades para a sociedade em que vivemos, inclusive novos crimes que são cometidos virtualmente, que podem causar danos irreversíveis às vítimas. O Brasil ficou anos necessitando de uma legislação para criminalizar condutas cometidas na internet e através dela, bem como proteger o usuário desse meio, porém só aconteceu após um caso que repercutiu na mídia, onde uma atriz global Carolina Dieckmann teve inúmeras fotos íntimas vazadas. O Estado brasiliero se viu pressionado em criar uma legislação que regulamenta práticas como essa, a Le**i** n° 12.737/2012, mais conhecida como “Lei Carolina Dieckmann" responsável por tipificar criminalmente delitos cometidos em meio virtual.O principal objetivo da presente monografia foi analisar a ineficácia da Lei Carolina Dieckmann diante da solução e punição dos crimes cibernéticos, pela falha na legislação que é cheia de lacunas, penas ínfimas, dificuldade da investigação e identificação dos criminosos, bem como a falta de delegacias e pessoal especializado. A metodologia adotada no seguinte trabalho foi a pesquisa bibliográfica em base de dados disponíveis na internet, doutrinas e jurisprudências. Conclui que, mesmo o Brasil possuindo uma legislação que prevê a punição dos Cibercrimes, a lei ainda necessita de alguns ajustes, do mesmo modo em que há necessidade de o Estado intervir e investir em delegacias e pessoal especializado para reduzir a impunidade desses crimes.

Palavras-chave: Lei Carolina Dieckmann. Crimes Cibernéticos. Ineficácia.

ABSTRACT

The technological advance that has taken place over the years has brought news to the society we live in, including new crimes that are committed virtually, which can cause irreversible damage to victims. Brazil spent years needing legislation to criminalize conduct committed on the internet and through it, as well as protect the user of this medium, but it only happened after a case that had repercussions in the media, where a global actress Carolina Dieckmann had numerous intimate photos leaked. The Brazilian State was pressured to create legislation that regulates practices like this, Law No. the ineffectiveness of the Carolina Dieckmann Law in terms of solving and punishing cyber crimes, due to the flaw in the legislation, which is full of gaps, minimal penalties, difficulty in investigating and identifying criminals, as well as the lack of police stations and specialized personnel. The following work was the bibliographic research in databases available on the internet, doctrines and jurisprudence. It concludes that, even though Brazil has legislation that provides for the punishment of Cybercrimes, the law still needs some adjustments, in the same way that there is a need to the State to intervene and invest in police stations and specialized personnel to reduce impunity for these crimes.

Keywords: Carolina Dieckmann Law. Cyber Crimes. Ineffectiveness.

SUMÁRIO

INTRODUÇÃO

No Brasil, o alto índice de crimes cibernéticos tem contribuído para a criação de leis de proteção de dados em ambientes virtuais. A Lei nº 12.737/12 (Carolina Dieckmann), que trata da classificação dos crimes virtuais e da implementação de sanções e procedimentos regulatórios e a Lei nº 12.965/14 (Lei do Marco Civil da Internet) que dispõe sobre os princípios, garantias, direitos e obrigações relativos ao uso da internet, são exemplos dessas Leis criadas, em consequência de crimes virtuais.

Por exemplo, a lei 12.737/12 que omite o fato do caso da Carolina Dieckmann. Como resultado do crime em questão, onde quando a atriz Carolina Dieckmann teve uma invasão no seu computador, isso gerou gatilho para que os números dos crimes virtuais aumentassem no Brasil, por isso é difícil obter provas em delegacias especializadas, pois, não possuem uma estruturação adequada, não recebem verbas suficientes para suprir todas as necessidades.

As delegacias especializadas necessitam ser criadas o mais breve possível, e que possuam pessoas que sejam capacitadas para realizar um atendimento adequado à vítima, para que se sinta acolhida e não constrangida. É necessário, ainda, maiores investimentos no aparelhamento das delegacias já existentes e capacitação dos agentes. Algo que poderá impactar positivamente nas investigações desses crimes tanto no que se refere à investigação quanto, por consequência, no processamento e julgamento posterior em futura ação penal.

Ponto importante a ser notado, refere-se ao avanço nos combates aos crimes cibernéticos. Embora o poder legislativo tenha apresentado esforços nesse sentido, como, por exemplo, a edição da Leinº 13.709/18 alterada pela Lei nº 13.853/19, recentemente em vigor, o crescimento do acesso da população à internet, nos dias atuais, pode trazer um aspecto negativo para o combate aos delitos virtuais. Por uma consequência lógica, quanto maior o número de pessoas conectadas, maior o número de potenciais vítimas. Isto reforça ainda mais o que foi dito no sentido de que é necessário maiores investimentos em segurança pública para combater este tipo de crime.

A velocidade de crescimento, tanto da tecnologia quanto de usuários, vem crescendo com muita celeridade, esta revolução na tecnologia, e suas as grandes mudanças, às quais dominam a vida social das pessoas pode contribuir positivamente ou negativamente para o problema. A comunicação entre as pessoas tornou-se de abrangência mundial que faz com que em questão de segundos, milhares de pessoas pelo mundo se comuniquem.

Com toda essa evolução, houve o favorecimento para com que surgissem diversos crimes virtuais, os quais, na maioria das vezes, deixam as vítimas em estado de vulnerabilidade. Os inúmeros infratores retêm um conhecimento extraordinário nesta área, e eles acabam usando isso para se beneficiarem com as inúmeras práticas criminosas. Com todo esse surgimento, foram necessárias legislações específicas no qual tratassem de casos assim, que até então não existiam.

Com o grande avanço da internet, o qual trouxe uma enorme transformação mundial, e que tem sido a ferramenta essencial para que ocorram todos esses crimes. A internet hoje é reconhecida como uma excelente biblioteca virtual, ferramenta de compra, divulgação de obras pessoais e importante fonte de informações, as possibilidades de sua aplicação são infinitas.

Devido ao seu alcance e amplitude, o emprego, necessariamente, regulamentado por lei, em nosso sistema jurídico faz parte da nossa sociedade. No Brasil, essa lei é chamada de Marco Civil. A Internet é crucial para a correta interpretação e aplicação de seus termos pelas autoridades judiciárias.

Segundo Piberam (2008), Cibercrime é um crime cometido através da comunicação entre redes de computadores, notadamente através da internet.

Conforme Peixoto (1953, p. 11), a criminologia “é a ciência que estuda os crimes e os criminosos, e, portanto, a criminalidade”. Se referindo aos inúmeros atos de infrações cibernéticas que estão sendo cometidos na atualidade.

Sobre o tipo de metodologia adotada, utiliza-se através de pesquisas bibliográficas, base de dados de materiais publicados pelos vários meios de informação e através de livros.

A estruturação do TCC, terá como o primeiro capítulo a introdução com a explicação do que é a Lei Carolina Dieckmann, após, terá uma explicação da criação

da lei Carolina Dieckmann; a razão pelo qual existe a ineficácia; de onde surge a ineficácia; por fim a lei Carolina Dieckmann durante a pandemia COVID-19. Terão os problemas apresentados; a justificativa; os objetivos gerais e específicos; a revisão preliminar; as hipóteses e por fim a metodologia.

1. A PRIVACIDADE E O MEIO DIGITAL

O objetivo deste capítulo é conceituar os crimes virtuais e suas peculiaridades, bem como analisar os tipos de crimes virtuais e os mecanismos utilizados pelos criminosos para conseguir praticar os crimes. Para tal, ele está dividido em três partes.

Na primeira parte, será abordado o conceito dos crimes cibernéticos, algumas de suas características e peculiaridades. Na segunda parte, discorreremos sobre os tipos de crimes cibernéticos e sobre os vários meios que os criminosos utilizam para praticar tais delitos.

Na terceira parte, será feita uma análise sobre o direito à privacidade e à intimidade, direitos previstos constitucionalmente fundamentais no ordenamento jurídico brasileiro cuja análise será relevante para o presente trabalho.

1.1 CONCEITO DE CRIMES CIBERNÉTICOS

Com o avanço da internet, houve também, vários problemas como por exemplo os chamados crimes virtuais, de modo que atualmente há muito mais pessoas conectadas virtualmente do que cara a cara, de modo que tais crimes vêm ocorrendo de forma cada vez mais frequente.

São óbvios os benefícios que o crescimento da tecnologia trouxe tanto para os Governos como para a população, mas, em contrapartida, não se pode olvidar que esse meio de acesso volátil propiciou o aumento do surgimento de vários tipos de crimes.

É o que se segue, nas palavras de Mendes e Vieira:

> [...] apesar das facilidades e benefícios oferecidos pela internet, esse cenário também é propício para a prática de crimes. Cada vez mais, os criminosos se valem desse meio para praticar os mais variados tipos de crime. Pois, com o advento da internet, os crimes já tipificados pelo Código Penal passaram a ser praticados também no meio virtual, assim como, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio.

Os crimes cibernéticos ou cibercrimes referem-se àtoda e qualquer atividade ilegal conduzida na Internet por meio de dispositivos eletrônicos, como computadores e telefones celulares,materializados pela prática de vários crimes como fraude, estelionato, bullying na internet, falsificação de identidade, ameaças, entre outros.

O autor Pinheiro (2010, p. 46), define como:

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo entre outro.

Já Rosa (2018, pp. 53/54), verbera que crime de informática é:

> A conduta atenta 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 dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrados; 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 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, pertence à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Assim, pode-se dizer que os crimes cibernéticos são fatos típicos e antijurídicos cometidos por meio da internet ou contra um sistema, dispositivo informático ou redes de computadores, que podem ser cometidos por causa das inovações tecnológicas e digitais que vieram para facilitar a vida das pessoas,

permitindo postagens, divulgações de fotos contatos, documentos, vídeos e dados bancários em uma questão de segundos (WINCK et al., 2015).

Apesar de vários autores se arriscarem na conceituação do que é cibercrimes, Ferreira (2001, p.208), explica que não há um consenso entre os doutrinadores a respeito dessa conceituação, pois há várias possibilidades de ação criminosa na área da informática, abrangendo todas as tecnologias da informação , processamento e transmissão de dados, e que apesar dessa abrangência acabam por atingir um denominador comum.

Essa nova modalidade de crimes, possuem características específicas, como a facilidade de ocultação de rastros, uma vez que os dados informáticos são passíveis de serem apagados ou alterados, mascarando-se, assim, a conduta do agente e ainda a dificuldade de localização e identificação dos invasores.

Outra característica é a ausência de fronteiras geográficas, uma vez que os cibercrimes podem ocorrer à distância, e em qualquer lugar do mundo, permitindo que autor, vítima, objeto tutelado e resultado produzido estejam todos em localizações diferentes, dificultando a investigação e responsabilização pelos delitos.

Com a evolução das formas de comunicação e o aumento da propagação de dados e ideias por meio da rede mundial de computadores, surge a comunicação dinâmica com muito desenvolvimento tecnológico, através de aparelhos como smartphones ou tablets, conectados pela internet, o que facilita a comunicação em tempo real e permite que a troca de dados seja quase que instantaneamente (ALVES, 2014).

Apesar de ser um meio com muitas facilidades, se tornou uma ferramenta para os criminosos que utilizam o anonimato para cometer crimes, o que dificulta a identificação pessoal e a sua localização, de modo que qualquer pessoa pode ser vítima desses tipos de crimes e qualquer pessoa pode praticá-los. Sendo assim, os crimes cibernéticos se tornaram mais corriqueiros em face do pouco conhecimento e pouca legislação a respeito.

As práticas variam desde a disseminação de vírus por meio de links enviados por e-mail até a invasão de sistemas operacionais de empresas e até mesmo sistemas operacionais privados, com isso, os criminosos podem roubar informações

e dados confidenciais, por exemplo, aplicar declarações falsas fraudulentas e outros golpes.

Os indivíduos que praticam os crimes ganharam o nome de hackers, um designativo da era moderna para indivíduos que sempre existiram, o termo de origem inglesa é usado para qualificar programadores muito hábeis e talentosos, que conseguem ter informações de forma sigilosa sobre o sistema informático de outra pessoa para que possam olhar, usar ou trocá-lo[1], por e para vários pretextos.

Portanto, o crime cibernético pode envolver um ou mais criminosos, por um lado, e uma ou mais vítimas, por outro. desse modo, os sujeitos ativos do ato podem ser qualquer pessoa que invade, sem autorização, os equipamentos eletrônicos de outrem, e o sujeito passivo, qualquer pessoa que sofre com a consequência da invasão tendo seus dados roubados ou informações íntimas vazadas.

Segundo Tabosa et al. (2017), os crimes cibernéticos podem se dividir em duas categorias:

> Categoria I: Insere delitos com a finalidade de reunir informações pessoais de forma a prejudicar de alguma maneira a vítima, conceituado phishing. Por exemplo, se a vítima inocentemente instala em seu computador algum tipo de vírus, o autor do crime tem a possibilidade de acessar os seus dados, unicamente, com a intenção de lhe prejudicar.
> Categoria II: Abarca práticas de assédio e molestamento na internet, violência contra crianças, chantagem e intimidação. Por exemplo, o criminoso se insere em uma sala de bate-papo para interagir com a suposta vítima, estabelecendo uma relação de confiança, visto a facilidade de diálogo entre ambas e a “inocência” da mesma para concretizar relações afetivas. Após a consolidação da relação de confiança, os criminosos manipulam as vítimas de forma a praticarem atos que podem envolver a automutilação.

Essas condutas de violências e crimes sempre estiveram presentes, contudo, confome a tencologia foi avançando, houve o aumento da pratica que gerou consequências devastadoras á vida humana, pois um indivíduo ao sofrer calúnia, difamação, injúria, pedofilia e outras práticas consideradas ilícitas, tem como sequelas danos psicológicos irreversíveis (SOUZA; VOLPE, 2015).

A criminalidade da informática não trouxe apenas como resultados negativos o nascimento de novos comportamentos ilícitos, mas, também, inúmeros prejuízos

[1] Dicionário virtual Pearson-Longman. Disponível em: http://www.ldoceonline.com/dictionary/hacker.

ao bem jurídico tutelado da vítima, que na maioria dos casos é a honra, dificuldade que o Estado tem em elucidar esses crimes devido a dificuldade em encontrar os criminosos frente ao anonimato.

Embora haja dificuldade em descobrir os culpados por esses tipos de crime, há meios de se conseguir informações,afinal, tudo que é feito na internet produz rastros. Rastros como os dados que ficam registrados na rede de computadores,os quais podem ser acessados, como, por exemplo, o IP do computador ou aparelho de comunicação com acesso à rede usado no ato criminoso e os rastros deixados no acesso a sites virtuais, programas e aplicativos. Nesse sentido, a criação de delegacias especializadas com técnicos de informática que consigam fazer essa cobertura e descobrir os criminosos é imprescindível.

1.2 PRINCIPAIS TIPOS DE CRIMES CIBERNÉTICOS

Com o aumento das ferramentas de comunicação, incluindo os aparatos tecnológicos, houve também um aumento das vulnerabilidades que podem ser vasculhadas por cibercriminosos, de modo que para que o indivíduo possa ser atacado, ele deve, necessariamente permitir isso de alguma forma, seja de forma direta ou indireta (CASSANTI, 2014).

A invasão indireta é realizada através de vulnerabilidades de softwares, configurações incorretas ou falhas de segurança de firewalls de rede, sendo exploradas por invasores que ficam monitorando a rede à procura de brechas de segurança. Já na forma direta, o invasor utiliza meios para implantar um software malicioso no dispositivo, através de e-mails, mensageiro instantâneo, redes sociais, sistema de compartilhamento de arquivos, sites falsos, engenharia social e arquivos com códigos maliciosos infiltrados (CASSANTI, 2014).

Os aplicativos de mensagens instantâneas como Skype, WhatsApp, Google Hangouts, assim como as redes sociais Facebook, Twitter Youtube e Google+ são grandes disseminadores de links falsos, bem como através de emails, utilizando spam, vírus e golpe de roubo de identidade, que vem com anexos acompanhados

de arquivos maliciosos e links de redirecionamento para sites falsos (CASSANTI, 2014).

Outro método de invasão é a engenharia social, que consiste em ludibriar a vítima de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais simulando fazerem parte de instituições como bancos, sites de grandes lojas e órgãos do governo, utilizando como pontos de ataque a fragilidade humana, através de e-mails, mensagens SMS ou ligações, solicitando informações pessoais como senhas, número de cartão de crédito. A engenharia social não possui um procedimento definido, tudo vai depender da criatividade do atacante e da sua capacidade de persuasão. (WENDT; JORGE, 2013).

Com essas ferramentas disponibilizadas, os criminosos podem praticar diversos crimes, que são divididos em próprios e impróprios. Crimes próprios são aquelas condutas antijurídicas e culpáveis, as quais visam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade, conforme explica Damásio de Jesus (2001, p.01):

> Crimes eletrônicos puros ou próprios são aqueles que são praticados por computador e se realizam ou se consomem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

E tem-se os crimes impróprios que são as condutas comuns, típicas, antijurídicas e culpáveis, cometidas utilizando como mecanismos a informática, devido a possibilidade de anonimato, mas que poderiam ter sido praticadas por outros meios e, consequentemente, estimula o descumprimento das leis e um aumento expressivo de sua prática, conforme explica Damásio de Jesus (2001, p.01):

> Os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço ‘real’, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Dentre esses, destacam-se os crimes mais comuns: crimes de ódio em geral como os crimes contra a honra, sentimento religioso e bullyng, crimes de invasão de privacidade e intimidade, crimes de estelionato, crimes de pedofilia, entre outros.

Nos crimes contra a honra encontramos, na legislação penal três tipos de crimes distintos: calúnia, difamação e injúria, que são diferenciados pela lei:

> Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. Difamação
> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Art. 140 Injuriar alguém, ofendendo lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940).

Caluniar é, exatamente, atribuir a alguém fato definido como crime, sem que este tenha o cometido. Já a difamação é a atribuição de culpa a alguém pelo cometimento de fato não criminoso, porém ofensivo a sua reputação e, por fim, a injúria, que é a atribuição de qualidades negativas ou defeitos ao indivíduo (NORONHA, apud CUNHA, 2014).

Outro crime que pode ser praticado de forma virtual é a ameaça, crime contra a liberdade individual previsto no artigo 147 do Código Penal Brasileiro, onde deve ser analisado conforme a individualidade da vítima, idade, sexo, raça, cor, opção sexual, para caracterizar se houve ou não a conduta, tipificada como a promessa de se causar a alguém um dano injusto (CUNHA, 2014).

O crime de estelionato, previsto no artigo 171 do Código Penal, também é muito praticado no mundo virtual, pelo fato que o isolamento social fez com que cada vez mais pessoas utilizassem a internet para a realização de operações financeiras virtuais, movimentando valores, colocando senhas, códigos e links, o que facilitou a prática do crime, que pode ocorrer de várias formas, com "[...] criação de páginas falsas de agências bancárias e lojas, anúncios de promoções, crédito fácil ou ofertas, que, num primeiro olhar, instigam a vítima ao click" (MARTINS, 2020 apud SANTOS, 2020).

Outra modalidade muito frequente é a extorsão, conforme explica Martins (2020 apud SANTOS, 2020, p. 02), Hackers: “[...] por intermédio de programas

maliciosos, que permitem o acesso aos computadores e celulares das vítimas, sequestram dados, criptografam os arquivos e, sob a ameaça de apagá-los ou divulgá-los na rede mundial de computadores, exigem o pagamento de um resgate".

Com o crescimento do acesso de crianças a dispositivos que muitas vezes nem são vigiados pelos pais, tem-se outro crime em grande ascensão, a ciberpedofilia, que são crimes sexuais feitos contra crianças e adolescentes através da internet, de modo que os criminosos criam formas para atrair através de linguagem apropriadas que chamam a atenção e acabam conquistando a criança e ou o adolescente, e também com a criação de perfis falsos se passando por crianças para ganhar a confiança das vítimas com o intuito de praticar o crime (RODRIGUES & SIMAS FILHO, 2004 apud MORAIS, 2018).

Podemos falar ainda do crime de chantagem sexual, que é praticado por meio de intimidação às vítimas, que sofrem ao ter a ameaça de ter fotos íntimas divulgadas em algum ambiente virtual, em troca de algum valor exigido pelos criminosos, em relação a esse crime, temos um caso conhecido que repercutiu muito na mídia, o caso da atriz Carolina Dieckmann, que deu origem a Lei 12.737/2012 que será melhor explicada no capítulo seguinte, onde a atriz teve suas fotos íntimas expostas na internet por um criminoso virtual, que exigia uma certa quantia em dinheiro para não divulgá-las (MELO; SILVEIRA; SOUSA, 2017).

1.3 BREVES CONSIDERAÇÕES SOBRE A CONSTITUIÇÃO E O DIREITO À PRIVACIDADE E A INTIMIDADE

Com a promulgação da Constituição de 1988 houve a regulamentação de uma série de garantias e direitos fundamentais que visam assegurar a dignidade da pessoa humana.

A Carta Magna de 1988, foi a primeira constituição brasileira a fazer referência a intimidade e a vida privada, como podemos observar na redação do art.5º, que trouxe uma série de garantias, dentre as quais o direito à intimidade e à privacidade no art.5º, inciso X:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Muitos autores consideram que a intimidade é uma espécie do gênero privacidade, de forma que as duas são conectadas ao direito de personalidade, que é um direito fundamental, de modo que o direito à privacidade se diz respeito aos aos relacionamentos pessoais, comerciais e profissionais, já o direito à intimidade seria mais ligado a vida íntima do indivíduo envolvendo familiares e amigos.

Para tanto, mesmo sendo a intimidade e à privacidade direitos garantidos na Constituição Federal de 1988, o legislador não previu que a tecnologia iria tão longe, com tantos meios e informações disponíveis em tempo real, dados compartilhados a todo momento do mundo inteiro, e consequentemente o surgimento de vários crimes, violando direitos, e reduzindo a eficácia das garantias e direitos fundamentais.

Na doutrina e na jurisprudência há uma divergência sobre os conceitos desses dois direitos fundamentais, de forma que o conceito de privacidade englobaria o de intimidade, conforme explica Branco e Mendes (2012, p.3018):

> O direito à privacidade teria por objetivo os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, as relações comerciais e profissionais que o indivíduo não deseja que se espalhe ao conhecimento público. o objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos envolvendo relações familiares e amizades mais próximas.

Apesar de a proteção à intimidade e a privacidade ser de suma importância, na internet, ambas podem ser violadas com muita facilidade em decorrência da indiscriminada captação de dados, de modo que informações giram o mundo em questão de segundos, o que torna o ambiente propício para a prática de crimes TEIXEIRA, 2015).

Sendo assim, o direito à intimidade e à privacidade podem ser considerados direitos de personalidade, pois decorrem da autonomia de vontade e do livre arbítrio, de forma que o direito à privacidade confere ao ser humano, o direito de seguir suas escolhas de maneira que entender melhor, desde que respeitados o interesse coletivo e os direitos de terceiros, assim,, a privacidade e intimidade do indivíduo devem ser observados e respeitados, também no ambiente virtual, pois caso violados podem causar danos irreparáveis à imagem e dignidade do usuário, de modo que a violação a esses direitos fundamentais devem ser punidos.

2. O CASO “CAROLINA DIECKMANN”

Este capítulo versa sobre a Lei Carolina Dieckmann nº 12.737/2012, que surgiu depois que uma atriz global teve fotos íntimas vazadas, após se recusar a pagar uma quantia em pecúnia para os criminosos. Para tal ele está dividido em 03 partes.

Na primeira parte, será abordado a história da criação dessa lei e algumas considerações sobre ela, as modificações que ela introduziu no código penal. Na segunda parte será tratada sobre a ineficácia da Lei Carolina Dieckmann, que apesar de ter sido muito importante na regulação dos crimes cibernéticos ainda tem deixado muito a desejar.

E na terceira parte será tratado sobre a Lei Carolina Dieckmann nas delegacias especializadas, onde serão tratadas as formas que o Estado tem de localizar esses criminosos e as dificuldades encontradas, considerando o anonimato que impera nessa rede e a falta de especialização e pessoal qualificado na investigação desses crimes.

2.1 CRIAÇÃO DA LEI Nº 12.737/2012- “LEI CAROLINA DIECKMANN”

Com a globalização e com a expansão das tecnologias e do uso dos meios virtuais, surgiu uma nova categoria de crimes chamados de crimes virtuais informáticos, crimes eletrônicos ou crimes cibernéticos, sendo que a falta de legislação específica que regulamentasse o tema deixava os usuários desprotegidos.

Um marco que impulsionou a constituição de uma lei específica foi o caso da atriz global Carolina Dieckmann, que teve seu computador invadido e seus arquivos pessoais subtraídos, os criminosos começaram a chantageá-la para que fosse feito o pagamento da quantia de dez mil reais (R$ 10.000,00), para que suas fotos de teor

íntimo não fossem expostas na web, mas como a atriz não cedeu e denunciou a polícia, teve várias fotos íntimas vazadas e espalhadas através das redes sociais.

O acesso à intimidade da atriz ocorreu devido a uma situação corriqueira pela qual qualquer pessoa comum está sujeita, que ao levar seu computador pessoal para realizar um conserto o equipamento acabou sendo invadido através de seu email pessoal.

Antes do surgimento da lei, a invasão de um ambiente virtual e subtração de dados pessoais já era crime, no entanto, não haviam normas específicas do assunto. Para muitos especialistas, não ter Lei própria ou algum meio e inibir os crimes informáticos no ano de 2012, era um atraso muito grande para a legislação brasileira.

E quando a atriz se deparou com esse caso de repercussão nacional, e viu a necessidade de propor uma ação encontrou grandes obstáculos, como afirma o autor Crespo (2013, p. 59,):

> A ação judicial promovida por Carolina deparou-se, porém, com um obstáculo jurídico, o mesmo que vem atenuando a punição em casos semelhantes que ocorreram há mais de uma década no Brasil. “Se eu invadisse uma máquina e me valesse de informações confidenciais para ter um proveito financeiro, eu poderia responder por concorrência desleal, por extorsão, mas não pela invasão”. [...], por isso, os invasores responderão por crimes que a legislação brasileira já tipifica: furto, extorsão e difamação.

Contudo, por se tratar de uma figura pública e com forte influência, o Poder LEgislativo teve de dar a atenção necessária, para o tema dos crimes virtuais, de modo que foi sancionada a Lei 12.737/2012 que tratava especificamente dos crimes cibernéticos e fez mudanças em alguns crimes que já existiam.

A Lei 12.737/12, conhecida popularmente como “Lei Carolina Dieckmann", recebeu esse nome devido a repercussão, fazendo com que a atriz concedesse seu nome para esta causa que tem se tornado cada vez mais comum no mundo virtual. A Lei foi sancionada em 30 de novembro de 2012, publicada através do Diário Oficial da União em 03 de dezembro de 2012 e entrou em vigor no dia 02 de abril de 2013, estabelecendo a tipificação criminal de delitos informáticos.

A Lei, veio para tutelar o bem jurídico da liberdade individual e do direito ao sigilo profissional e pessoal, impactando no Direito Penal pois houve o acréscimo de

dois artigos que são 154-A e 154-B, intitulados “invasão de dispositivo informático” e também alterou os artigos 266 e 298 que são referentes à segurança no ambiente virtual, que preveem o uso indevido de informações e materiais que correspondem à privacidade da pessoa humana no meio da internet, como por exemplo, fotos e vídeos.

O artigo 154-A dispõe sobre a invasão de dispositivo:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (BRASIL,2012)

E por sua vez, o art. 154-B dispõe sobre o tipo de ação penal para tais crimes:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012).

O doutrinador Bittencourt (2019, p.662), tece considerações a respeito do tipo penal como sendo complexo:

> É um tipo penal complexo que conta com um elemento normativo especial da antijuridicidade — mediante violação indevida de mecanismo de segurança — e com dois elementos subjetivos especiais do injusto — (i) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou (ii) instalar vulnerabilidades para obter vantagem ilícita.

Apesar da mudança o bem jurídico protegido continua sendo a liberdade individual, com o núcleo sendo a palavra “invadir”, que tem o significado de entrar à força, ou de forma arbitrária ou hostil, sem o consentimento de quem de direito. Apesar de o núcleo ter esse significado, nesta figura típica, não significa o ingresso forçado ou arbitrário em espaço não autorizado, mas significa violar ou ingressar, clandestinamente, ou seja, sem autorização ou permissão do indivíduo dono daquele meio invadido, sem o consentimento (Bittencourt, 2019, p.664).

A ação penal desse crime é pública condicionada à representação, por se tratar de direito disponível, assim a ação penal depende de provocação do ofendido. Todavia, a ação penal será pública incondicionada se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (Bittencourt, 2019, p. 675).

A Lei Carolina Dieckmann deve ainda ser melhor estudada, para compreender melhor a sua aplicabilidade, levando em consideração a sua importância e efetividade na proteção dos direitos à intimidade da pessoa humana, pois tem como intuito reprimir condutas ilícitas e delituosas praticadas no meio virtual.

Apesar de já haver várias práticas ilícitas cometidas no meio virtual, tipificadas no Código Penal e em outras legislações, ainda há crimes que não possuem tipificação penal, o que colabora para a impunidade, assim a utilização da internet é necessária para toda a sociedade, mas por outro lado, casos de crimes cibernéticos são cada vez mais comuns, como peculato, roubo e violação de dados, extorsão, fraude, pedofilia por essa razão a grande necessidade de melhorar as normas de combate e prevenção aos crimes virtuais.

2.2 A INEFICÁCIA DA LEI CAROLINA DIECKMANN

O crime, constituído no ato ilegal de invadir dispositivos informáticos e obter para si informações de outrem, só há a punição do infrator quando houver a invasão e a violação dos mecanismos de defesa com a mesma finalidade. Mas também para adulterar ou destruir o que houver de informações nos dispositivos.

Vale lembrar que a lei foi e é um marco no sistema jurídico brasileiro. Pois apenas com ele, existe a possibilidade de aplicação de sanção quando houver violação de dados, apesar de e Lei Carolina Dieckmann ter sido muito importante na tipificação de crimes cometidos no mundo virtual, e considerando a rapidez com que foi elaborada, publicada e começou a vigorar, foi mal elaborada e possui algumas

lacunas na sua aplicação, como por exemplo penas muito brandas para crimes graves

Um exemplo é o crime de estelionato, inserido no Art. 171 do CP, em que os infratores fazem espionagem à vítima, com a finalidade de obter vantagens ilícitas, e posteriormente, adquirir dados pessoais através de solicitações que são realizadas através de links que são enviados por SMS, links dentre outros. Fazendo assim, que a vítima caia no golpe e forneça automaticamente dados pessoais e bancários.

Para o advogado criminalista Luiz Augusto Sartori de Castro, ele diz que ainda existem grandes lacunas legislativas sobre o tema. Pois mesmo impondo penas de prisão e multa aos criminosos. “Existe ainda uma ausência de definição de diversos termos técnicos que são inseridos em lei”.

Para que haja a configuração do crime, há a necessidade de que o infrator viole o mecanismo de segurança de dispositivos, ou seja, é um crime formal, exige para a consumação a invasão a um dispositivo informático de outra pessoa. Em contrapartida a simples invasão, não configura o crime, vez que se exige a finalidade específica de obter, adulterar ou destruir dados e informações.

Seguindo outra falha do tipo penal temos, a falta de conceituação de *“mecanismo de segurança”*, que é um ponto de suma importância para a configuração do crime, sendo que se o dispositivo invadido não possuir qualquer tipo de proteção (senha, antivírus, *firewall* etc.), não haverá crime, sendo a conduta atípica.

Apesar de haver inúmeras inovações ao sistema penal brasileiro, hoje em dias atuais, outra questão abordada é o favorecimento aos criminosos, sendo um dos fatos, a pena mínima aplicada que é abaixo de 01 (um) ano podendo ser suspensa. Retirando assim, a gravidade dos danos, se tratando então de crimes de menor potencial ofensivo, o que auxilia na impunidade conforme discorre França (2013, p. 5).

> A pena mínima, abaixo de 1 ano favorece a suspensão condicional do processo, se não houve condenação ou se não existe processo por outro crime. […] daí por que dizer que a reprimenda, associada ao comportamento delitivo, tem de ser idônea, isto é, deve fazer jus à gravidade da sua efetivação em face da liberdade do indivíduo, sob pena de, desnaturando as suas próprias funções, dá azo a inevitável autofagia.

> Noutras palavras, penas insignificantes não atendem aos princípios clássicos de Direito Penal, sobretudo o da lesividade.

Outra crítica que é realizada, é quando há apenas a invasão para realizar uma vasta visualização sem causar danos na vítima. Com isso, não é configurado crime, por não haver exposição da vida da vítima. Os indivíduos que possuem capacidade para criar programas para realizar a proteção de dados, são contratados por gigantes empresas e famosos para fazer proteção de dados.

Como por exemplo podemos citar duas situações: 1) se o indivíduo que teve suas informações roubadas não tiver senha no computador; 2) colegas que compartilham computadores e têm acessos aos dados um do outro e um deles acaba divulgando. Em ambas as situações não há fato típico, pois de acordo com a Lei 12.737/12 autor desta ação não poderá ser punido por meio da referida lei, pois não houve violação de mecanismos de segurança, para que o fato se torne típico.

Outro problema encontrado na aplicabilidade da Lei 12.737/2012 é o anonimato que impera nas redes virtuais, bem como a dificuldade de colher provas capazes de demonstrar a ocorrência dos crimes, conforme explica (GRECO, 2013, p. 598).

> Os delitos praticados através da informática podem ser de difícil apuração. Lucrecio Rebollo Delegado destaca três características muito importantes, que lhes são peculiares, dizendo que todas as atuações ilícitas cometidas no âmbito informático se realizarão: com celeridade e distância no tempo e no espaço, facilidade de encobrimento e dificuldade probatória.

Como visto, existem algumas formas de ocorrer a invasão e divulgação de informações sem que o invasor seja punido, o que acarreta a sensação de impunidade e o empobrecimento da lei, pois não há diminuição dos crimes pela carência da lei.

Perante tantas lacunas, a lei não consegue amparar grande parte da população que sofre por esse crime. Uma boa porcentagem de vítimas é bastante leiga e outros não possuem recursos suficientes para um realizar uma segurança boa, com a instalação de antivírus que na maioria das vezes são pagos e colocação

de senhas seguras, e consequentemente os criminosos seguem impunes, conforme ressalta Ferreira (2015, p.32):

> Por isso temos a sensação de impunidade, sendo um atrativo muito forte para o crescimento desse tipo de delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema como a (DEP WEB), como através de ataques mais sofisticados por hackers. A ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra esses delitos, por isso diante dessa dificuldade encontrada, ou até mesmo pela natureza taxativa do Código Penal, há uma grande impossibilidade da aplicação da analogia nos crimes virtuais.

Em vista disso, não há como omitir a deficiência desta lei, pois há uma grande necessidade de sanar as lacunas existentes, aumentando as penas e corrigindo de forma que a legislação se torne mais clara e mais eficaz na punição dos crimes cibernéticos que vem aumentando a cada ano que se passa.

2.3 A LEI CAROLINA DIECKMANN NAS DELEGACIAS ESPECIALIZADAS

Com o rápido e crescente desenvolvimento da internet, surgiram inúmeros crimes praticados por esse meio, que por intermédio desse os criminosos usam a vulnerabilidade dos sistemas e dos próprios usuários para cometer crimes, auxiliado ao anonimato, que criou um grande barreira para a investigação, punição e repressão dos crimes cibernéticos, considerando que as leis existentes não vem sendo suficientes para regular e acompanhar a velocidade com que esses crimes vem acontecendo, conforme visto nos capítulos anteriores.

No ordenamento jurídico brasileiro existem duas leis sancionadas, que modificaram alguns dispositivos do Código Penal e instituiram penas para estes crimes. A primeira delas é a Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, conforme capítulos anteriores. E a segunda, é a Lei 12.735/12 “Lei Azevedo”, que determina a instalação de delegacias especializadas para o combate de crimes digitais.

A Lei Azevedo, nº 12.735/12, conceitua para os órgãos da polícia judiciária que existe uma enorme necessidade da criação de setores específicos para combater estes crimes virtuais. Existem as delegacias, porém são muito poucas diante de toda a demanda existente atualmente.

Com finalidade de uma maior análise da ocorrência dos crimes, essas delegacias são essenciais. Como se sabe, todo procedimento que possui investigação. Porém, quando é desta natureza, a autoridade policial terá um olhar mais observador para a instauração da investigação que é mediante o T.C.O ou inquérito policial.

A responsabilidade da polícia judiciária, pois a polícia civil possui a ausência de pessoas qualificadas e de investimento material para tal crime. E isso mostra mais ainda a necessidade de termos as delegacias especializadas, possuindo uma estruturação humanizada e com os materiais necessários para que haja uma apuração e a punição dos crimes virtuais com uma maior efetividade.

Conforme Wendt (2013, p. 238), explica que existem poucos Estados brasileiros onde se encontram polícias especializadas em crimes virtuais. No país só há Delegacias de Polícia Especializadas no Rio de Janeiro, São Paulo, Minas Gerais, Pará, Rio Grande do Sul, Paraná, Espírito Santo, Sergipe, Piauí e Bahia, ou seja, a realidade brasileira está aquém do que a lei preconiza.

Outro ponto que podemos observar é o fato de o inquérito policial dos crimes cibernéticos, ainda estar em estágio embrionário e necessitar de muita melhora para que tenham elementos de investigação eficazes para alcançar o autor e a materialidade dos fatos, bem como ferramentas que possibilitem a identificação dos criminosos, que deixam poucos ou quase nenhum rastro, o que dificulta a solução e a punição dos crimes.

Apesar das deficiências e da falta de especialização das delegacias, a polícia vem utilizando o IP (Internet Protocol) para a identificação dos criminosos, e consequente redução do número de crimes, pois essa ferramenta consegue localizar o infrator, assim o combate ao crime cibernético está em constante evolução e especialização, pois necessitou se amoldar à nova realidade (SILVA, 2017).

Vale ressaltar que, mesmo que os criminosos consigam roubar os dados de forma anônima e deixar nenhum ou quase nenhum rastro, os cibercrimes deixam

alguns vestígios, de forma que a utilização dos métodos investigativos que a legislação dispõe, como a perícia se torna totalmente necessária, conforme explica Jesus e Milagre (2016, p. 193):

> Sabe-se que a prova pericial tem importância cada vez maior e sua realização deve se adequar a uma série de cuidados, sobretudo no que diz respeito à forma de realização. O exame de corpo de delito, em verdade, é perícia no escopo de se provar a materialidade de um crime. Em crimes informáticos, comumente o corpo de delito é direto, incidindo sobre os vestígios deixados pela infração. Excepcionalmente, pode ser indireto, quando os vestígios desapareceram.

Sendo assim, existem inúmeros mecanismos que possibilitam a localização dos infratores, apesar de a investigação virtual no Brasil se deparar com inúmeras barreiras construídas pela tecnologia, seja pela criptografia, o anonimato, a inexistência de delegacias e pessoal especializado ou pela expertise dos criminosos em eliminar as informações rapidamente da rede, se torna estritamente necessária a investigação e elucidação desses crimes.

3 A LEI CAROLINA DIECKMANN NA PANDEMIA DO COVID-19

O avanço tecnológico trouxe diversos benefícios ao homem. Ferramentas de informação, comunicação e de interação social, uniu a comunidade mundial frente a seus aparelhos, diante da acessibilidade que estes apresentam.

Com a chegada da pandemia do COVID 19, o isolamento social e a privação do direito de ir e vir, fizeram com que as pessoas ficassem, mas reféns das redes sociais, ainda mais com o surgimento do Home Office.

José Antônio Milagre, advogado e perito que é um especialista em Direito Digital e Crimes Cibernéticos explica:

> Tivemos um aumento de crimes cibernéticos contra o patrimônio a partir do momento em que profissionais tiveram que trabalhar em home office, sem que a empresa tivesse um programa de segurança em teletrabalho. Resultado, muitos golpes, fraudes e códigos maliciosos que infectam não só o computador do empregado, mas a rede da empresa. O aumento de reuniões e atividades on-line, diante do distanciamento social, também forneceu novas abordagens. Recebemos notificações de golpes do leilão, invasão de reuniões sigilosas e até transferências indevidas de valores a partir da invasão a contas bancárias... (Diário do Litoral, O Brasil sofreu mais de 3,4 bilhões de tentativas de ataques cibernéticos em 2020, 2020)

Em um mundo cada vez mais avançado tecnologicamente, o crime cibernético está se espalhando na Internet, com muitas vítimas todos os dias. Os mentirosos famosos estão sempre em guarda, especialmente neste momento delicado de nossas vidas.

A pandemia Covid-19 trouxe pânico, medo, incerteza e desinformação ao mundo. Devido ao isolamento social, as pessoas estão cada vez mais próximas e, em última análise, correm mais riscos. É preciso ter muito cuidado ao pagar contas, fazer compras pela Internet ou mesmo acessar links, pois é nesses momentos que os bandidos vão agir.

De fato, o isolamento social foi capaz de reduzir significativamente a prática de roubos e furtos nas cidades brasileiras, como consequência do zelar da população, ao preferir a segurança do ambiente domiciliar. No entanto, estas

mesmas circunstâncias serviram para a desenvoltura de crimes cibernéticos cometidos por Crackers (MARTINS, 2020).

Nas palavras de Martins (2020, p. 02):

> Criminosos percebendo o uso massivo da rede mundial de computadores por grande parte da população mundial procuraram, rapidamente, adaptar-se à nova realidade para cometer fraudes eletrônicas, aproveitando-se do estado de medo e ansiedade que a pandemia e a necessidade de isolamento causam às pessoas.

Usando uma matéria de Minas Gerais de exemplo, mostra que o número de crimes cibernéticos aumentou quase 50% em relação ao ano passado. De acordo com dados da polícia, de janeiro a maio deste ano, foram registrados 3.070 casos de crimes cibernéticos em todo o país, um aumento de quase 606% em relação ao mesmo período de 2019.

Como uma das redes mais utilizadas pelas pessoas, o WhatsApp sempre foi a maior "ferramenta" para os bandidos. Um de seus golpes mais comuns é o golpe de assistência de emergência. Primeiramente, o usuário precisa acessar o link e ser automaticamente incentivado a responder algumas perguntas, como: “Você é beneficiário do Bolsa Família?”.

Ao atender, a vítima se inscreve para receber o chamado de atendimento e deve compartilhar o link com seus contatos na rede social. Em seguida, a vítima foi direcionada para uma página onde eram necessários dados pessoais para o preenchimento do cadastro.

Ataques conhecidos como phishing foram responsáveis por 10% dos ataques da semana passada. Os invasores fingiram ser uma pessoa ou empresa confiável para obter informações confidenciais, como nomes de usuário, senhas e informações de cartão de crédito. A forma mais comum desse golpe é induzir as vítimas a abrir links ou anexos por e-mail, o que na verdade é um programa malicioso.

No caso de clonagem de cartão de crédito ou débito desta forma, o agente responderá pelos crimes de pirataria informática e falsificação de documentos privados em concorrência substantiva, nos termos do artigo 1.º. Artigo 298 da Lei Penal.

A rigor, a Internet pode ser usada para cometer uma variedade de crimes. No entanto, o próprio crime cibernético é regulamentado pela Lei n. 12.737 (Lei Carolina Dieckmann), crime comum cometido usando a Internet como ferramenta.

Nessas horas, você deve ter mais cuidado. Salvar seus arquivos mais importantes em dispositivos de armazenamento externos ou sites de armazenamento de dados em nuvem, não abrir links ou anexos em e-mails de fontes desconhecidas e alterar senhas regularmente são exemplos de medidas de saúde para proteger a segurança da informação.

Assim sendo, pode-se observar cada vez mais a adaptação das práticas criminosas no meio virtual neste período de pandemia. O isolamento social, de fato, nos fez crer que o lar seria um ambiente seguro, todavia estamos mais expostos ao mundo e aos riscos virtuais. Sabe-se que a internet é um meio de escape para muitos, como por exemplo a distração causada por jogos, àqueles que possuem ansiedade, depressão, e outros sentimentos que se desenvolvem em tempos de crise, no entanto, a necessidade de se conectar ao mundo cibernético expõem muito as pessoas, tornando-as vítimas de criminosos invisíveis.

CONSIDERAÇÕES FINAIS

A sociedade sempre necessitou de informações, e de acordo com que a internet foi evoluindo, e foram surgindo novos crimes nesse ambiente, o direito e as legislações tiveram que acompanhar de forma correspondente e na velocidade de evolução.

A maioria das pessoas hoje em dia dependem de aparelhos digitais, da internet, das redes sociais para registrar seus dados e informações, compartilhar informações, tanto na vida profissional como na pessoal.

Essas informações que ficam armazenadas nesses dispositivos acabam chamando a atenção dos criminosos, pois no meio desses dados e informações podem-se verificar contas bancárias, número de cartão de crédito, senhas de acesso à conta de *e-mails*, fotos íntimas e diversos outros dados que podem gerar vantagens econômicas.

Conforme visto no seguinte trabalho, apesar de existirem leis específicas no Brasil que visam combater os crimes, estas ainda são ineficientes e incompletas, e necessitam de modificações e melhorias, bem como a criação de delegacias especializadas com pessoal capacitado para solucionar esse tipo de crimes, tendo em vista que a grande maioria dos crimes virtuais seguem sem solução ou punição e seguem em aumento gradativo.

O principal objetivo da presente monografia foi analisar a ineficácia da Lei Carolina Dieckmann diante da solução e punição dos crimes cibernéticos, pela falha na legislação que é cheia de lacunas, dificuldade da investigação e identificação dos criminosos, bem como a falta de delegacias e pessoal especializado.

A Lei Carolina Dieckmann foi um símbolo importante na tipificação dos crimes cibernéticos, com a intenção de combater a atuação de criminosos que tinha a prática de invadir os dispositivos informáticos alheios sem permissão, e até mesmo o roubo de dados e falsificações cartões de crédito e débito, ou seja, a lei tinha a intenção de evitar a impunidade dos crimes cibernéticos e proteger os usuários.

Mas, por outro lado, a referida Lei possui algumas lacunas em seu texto legal, conforme visto nos capítulos do trabalho, e assim, é de suma importância o

aperfeiçoamento da lei 12.737, com a implementação de penas mais severas, mais claras e melhor fundamentadas, pois quanto mais Quanto mais impunidade existir, mais crimes serão cometidos.

Em suma, há necessidade de o Estado intervir com mais ênfase, melhorando os aparatos das delegacias especializadas, abrindo novas delegacias, treinando o pessoal, para que a partir de então a LEi CArolina Dieckmann seja realmente efetivada e os criminosos deixem de ficar impunes, diminuindo a incidência da prática desse tipo de crime.

REFERÊNCIAS

ABREU, Eduardo Franco. **Os entraves à repressão aos crimes cibernéticos, 2014**. Disponível em: https://edufranco91.jusbrasil.com.br/artigos/142294529/os-entravesa-repressao-aos-crimes-ciberneticos. Acesso em: maio de 2022.

ALVES, Fernando Antonio. **O Ativismo Popular nas Redes Sociais Pela Internet e o Marco Constitucional da Multidão, no Estado Democrático de Direito: uma discussão prévia sobre participação popular e liberdade de expressão no Brasil, pós manifestações de junho de 2013**. Revista Direitos Emergentes da Sociedade Global, Santa Maria, v. 3, n. 1, p. 16-49, jan.jun/2014.

BARRETO, Erick Teixeira. Crimes cibernéticos sob a égide da Lei n. 12.737/2012, março 2017. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/49678/crimes-ciberneticos-soba-egide-da-lei-12-737-2012. Acesso em: 14 jun 2021.

BRASIL. Lei 12.735 de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: abril de 2022.

_____. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em abril de 2022.

_____.Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br /ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: abril de 2022.

CAPEZ, Fernando. **Curso de Direito Penal, volume 2**. 13 ed. São Paulo: Saraiva, 2013.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** Rio de Janeiro: Brasport, 2014. Disponível em: https://pt.scribd.com/read/405825018/Crimes-Virtuais-Vitimas-Reais . Acesso em: abril de 2022.

CASTELLS, Manuel. **A sociedade em rede.** Trad. Roneide Vernâncio Majer. 6. Ed. São Paulo: Paz e Terra, 1999.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, Waldek Fachinelli. **Crimes Cibernéticos: noções básicas de investigação e ameaças na internet.** 2016. Disponível em: https://www.conteudojuridico.com.br/open-pdf/cj054548.pdf/consult/cj054548.pdf. Acesso em: abril de 2022.

COSTA, Taís Barros Trajano Ribeiro da. **O aumento do crime cibernético durante a pandemia do Covid-19.** Jus. 2020. Disponível em: https://jus.com.br/artigos/84536/o-aumento-do-crime-cibernetico-durante-apandemia-do-covid-19. Acesso em: abr. 2022

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo. Ed Saraiva. 2011.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito, ed.13ª, Jan. 2018. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t 5C_2019-2-28-16-36-0.pdf. Acesso em: abr. 2022

DERTROUZOS, Michael L. **O que será: como o novo mundo da informação transformará nossas vidas.** Trad. De Celso Nogueira. São Paulo: Cia. Das letras, 1998.

DESLANDES, Maria S. S.; ARANTES, Álisson R.. **Os perigos dos crimes virtuais nas redes sociais**, 2017. Disponível em: http://periodicos.pucminas.br/index.php/sinapsemultipla/article/view/16488/ 12745. Acesso em: 03 abr. 2021

DIOGO, Darcianne. C**om 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020.** Correio Braziliense, 13 fev. 2021. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2021/02/4906387-com-17-843-ocorrencias-crimes-cometidos-pela-internet-sobem-871--em-2020.html. Acesso em: abr. 2022.

FERREIRA, Ivette Senise. **A criminalidade informática.** In:LUCCA, Newton De; SIMÃO FILHO, Adalberto (Coord). Direito & Internet - Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001.

FRANÇA, Misael Neto Bispo da. **Crimes informáticos e lei "Carolina Dieckmann": mais do mesmo no direito penal contemporâneo**. Revista Jurídica Consulex. 2013.

FRANCESCO, W. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann"**. 2014. Disponível em: < http://wagnerfrancesco.jusbrasil.com.br/artigos/152372896/o-que-voce-precisa-saber

-sobre-a-lei-12737-2012-conhecidacomo-lei-carolinadieckmann?utm_campaign=new s letterdaily_20141120_336&utm_medium=email&utm_source= newsletter>. Acesso em: abril de 2022.

GOMES, Luis Flavio. Lei Carolina Dieckman e sua ineficácia. Disponível em: <http:atualidadesdodireito.com.br/lfg/2013/03/07/lei-carolina-dieckman-e-sua-ineficacia>. Acesso em fevereiro de 2022.

GRECO, Rogério, **Curso de direito penal, volume 2.** 10 ed. Rio de Janeiro: Impetus, 2013.

JESUS, Damásio De. ARAS, Vladimir. **Crimes de informática: Uma nova criminalidade.** Disponível em . Acesso em abril de 2022.

JESUS, Damásio de; MILAGRE, José Antonio. **Marco Civil da Internet: Comentário à Lei 12.965/14**. 1. ed. São Paulo: Saraiva, 2014.
JESUS, Damásio Evangelista de. **Direito penal, volume 2.** 33 ed. São Paulo: Saraiva, 2013.

MELO, Antonia Morgana de Alcântara Jorge; SILVEIRA, Neil; SOUSA, Mirian Lima de. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann.** Revista Jus. Disponível em: <https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-deprivacidade-a-luz -da-lei-carolina-dieckmann>. Acesso em: fevereiro de 2022.

NATARELLI, T. V. P. **Ocorrência de delitos no comércio eletrônico: quais os reais inimigos na era da informação?**. In: Âmbito Jurídico, Rio Grande, XIV, n. 92, set 2011. Disponível em: . Acesso em: abril de 2022.

OLIVEIRA JÚNIOR, E. Q. de. **A nova Lei Carolina Dieckmann. 2013**. Disponível em:<http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina--die ckmann. Acesso em março de 2022.

PEIXOTO, A. **Criminologia**. 4ª ed. – São Paulo: Saraiva, 1953.

PINHEIRO, Patrícia Peck. **Direito digital global e seus princípios fundamentais.** Revista Jurídica , São Paulo, p. 46-47, 2016.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

SIQUEIRA, Ethevaldo. **Para compreender o mundo digital**. 1 ed. São Paulo: Globo, 2008.

SOUZA, Henry Leones de. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais.** Disponível em: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em abril de 2022.

VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. jul./dez. 2010.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. C**rimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: https://pt.scribd.com/read/436286113/Crimes-ciberneticos-ameacas-e-procedimentos-de-investigacao-2%C2%AA-Edicao. Acesso em: abril de 2022.

WINCK, Daniela et al. **A legislação e os cybercrimes**. Seminário de Iniciação Científica e Seminário Integrado de Ensino, Pesquisa e Extensão, 2017.