CENTRO UNIVERSITÁRIO BRASILEIRO

CURSO DE REDES DE COMPUTADORES

MIKAEL FILIPE DE LIMA NASCIMENTO

A IMPORTÂNCIA DA LEI KAROLINA DICKMANN NO COMBATE AOS CRIMES CIBERNÉTICOS

RECIFE/2024

MIKAEL FILIPE DE LIMA NASCIMENTO

A IMPORTÂNCIA DA LEI KAROLINA DICKMANN NO COMBATE AOS CRIMES CIBERNÉTICOS

Monografia apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de Tecnólogo em Redes de computadores Professor(a) Orientador(a): Mcs Wanuska Munique Portugal

RECIFE/2024

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

M528r Melo Júnior, Flávio Gonçalves de.
A importância da lei Karolina Dickmann no combate aos crimes cibernéticos / Mikael Filipe de Lima Nascimento. - Recife: O Autor, 2023.
18 p.

Orientador(a): Mcs. Wanuska Munique Portugal.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de computadores, 2023.

Inclui Referências.

1. Crimes virtuais. 2. Crimes. 3. Tecnologias. 4. Ambiente virtual. I. Centro Universitário Brasileiro. - UNIBRA. II. Título.

CDU: 004

Dedico este estudo aos meus pais e minha esposa por toda dedicação à mim durante toda a minha vida, e pelo incansável apoio ao longo de mais esta trajetória.

AGRADECIMENTO

Agradeço primeiramente ao Senhor Deus por seu amor imensurável comigo
A toda minha família pelo apoio constante;
Aos meus amados avós pela dedicação incansável;
Aos colegas, pelo companheirismo durante todo o processo deste curso e,
Aos mestre por terem compartilhado conosco seus conhecimento, contribuindo grandemente com o nosso crescimento pessoal e profissional.

“Os que acham que a MORTE é o maior de todos os males é porque não refletiram sobre os males que a INJUSTIÇA pode causar.”

(Sócrates – Filósofo grego)

RESUMO

O presente estudo tem como principal objetivo abordar os principais aspectos dos crimes cibernéticos, para isto busca-se compreender a evolução histórica das condutas e dos crimes que com o passar do tempo foram evoluindo de forma inversamente proporcional às leis. A globalização é fator fundamental ao que se refere as mudanças sofridas pela sociedade, assim como o uso crescente e continuo dos aparelhos tecnológicos. O referido estudo chama atenção para a falta de informação sobre as consequências dos crimes virtuais, onde se procurou discutir direitos, legislações e a busca de respostas para o controle dessa má conduta virtual. Ressalta-se que devido ao acesso habitual a internet os crimes virtuais vem acontecendo cada vez, mais rápidos e com maior agressividade tendo como objetivo final a perpetração do crime.

Palavras-chave: crimes virtuais, crimes, tecnologias e ambiente virtual.

ABSTRACT

This study aims to address the main aspects of cyber crimes, for it seeks to understand the historical evolution of conduct and crimes which over time have evolved inversely proportional to the laws manner. Globalisation is fundamental to respect the changes undergone by society and the growing and continuous use of technological devices. The study calls attention to the lack of information on the consequences of cyber crime, where it sought to discuss rights, legislation and the search for answers to control this virtual bad conduct. It is emphasized that due to regular access to the internet cybercrime is happening increasingly, faster and more aggressively with the ultimate objective of the commission of the crime.

Keywords: virtual crimes, crimes, technologies and virtual environment.

SUMÁRIO

1 INTRODUÇÃO

As pessoas em todo o mundo passam a usar cada vez mais as ferramentas tecnológicas disponíveis no mercado, na maioria das vezes com o intuito de facilitar as atividades diárias estreitando as distancias entre as pessoas. Todavia, nem todos os usuários tecnológicos possuem esta intenção, existem aqueles que que fazem uso da tecnologia, especialmente da Internet para praticar atos ilegais, alguns chegam a criar novas modalidades de delitos e outros expandem crimes que já são tipificados na legislação penal brasileira, o que exige do Direito resoluções para situações que o mesmo ainda se encontrava preparado para resolver (ANDREI, 2019)

É importante entender que mesmo nos dias de hoje o Brasil ainda não possui uma legislação específica referente a crimes cibernéticos, o que demostra uma urgência em regulamentar definitivamente os novos delitos penais, desta forma, estes atos criminais não permaneçam impunes acarretando danos à sociedade (MEDEIROS, 2020).

Os crimes cibernéticos começaram a surgir em meados dos anos 60, quando se tornaram um grave problema em todo o mundo, pois o avanço da tecnologia propiciava ampla facilidade em cometer crimes além de dificultar a identificação do autor do mesmo e especialmente pela ausência de leis eficiente em muitos países (NETO, 2013).

De acordo com Terceiro (2024), todos os crimes são devidamente tipificados por lei, fato que leva os tribunais no Brasil a utilizarem analogias o que é veementemente proibido em matérias penais. Atualmente, o direito penal ainda considera aceitável a utilização da analogia *in bonam partem* que não representem nenhum tipo de prejuízo ao réu, ou seja, são passíveis de punição os crimes que estejam tipificados em alguma lei já existente, isto torna cada vez mais urgente a criação de leis especificas para punição de criminosos cibernéticos.

Vale salientar, que hoje, no Brasil, existem vários projetos de lei que tem como principal objetivo o enquadramento dos crimes virtuais, pode-se destacar o projeto de lei criado pelo Senador Eduardo Azevedo que identifica novos crimes e torna mais rígida a pena a ser aplicada em outros crimes que já existem, todavia, o referido projeto vem sofrendo fortes críticas principalmente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet (Abranet), ao que tange ao armazenamento dos dados dos usuários da Internet pelos provedores, pelo período três anos em caso de necessidade de investigação policial futura.

Desta forma, considerando o conceito analítico de crime, é possível afirmar os crimes virtuais constituem-se em “condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas de informática” (SCHMIDT, 2021, p 216).

Ao se referir aos crimes cibernéticos, fazemos relação com a Convenção sobre Cibercrime do Conselho da Europa, conhecida também como Convenção de Budapeste, que constitui uma declaração de direito internacional público redigida por dois comitês compostos por peritos contando ainda com a participação de países como os Estados Unidos da América, Canadá, Japão e África do Sul.

É muito importante entender o motivo pelo qual os crimes virtuais possuem características capazes de mantê-los impunes no Brasil, fato que colabora significativamente para o baixo índice de punição destes criminosos o que os deixa a vontade os referidos crimes elevando sem delongas o número de suas vítimas.

Segundo Daoun e Lima (2019), o que aconteceu, foi que a legislação brasileira não conseguiu acompanhar as mudanças provocadas pela informatização generalizada, o que obriga os magistrados, sempre que possível, a enquadrar os novos crimes nos tipos de penalidades que já existem, uma vez que os crimes cometidos por meio da internet cresceram mais da metade nos últimos anos, chegando ao número de 156.692 denúncias anônimas no ano de 2020. (GARRETT, 2021). Diante desse cenário de insegurança virtual, além da Lei Karolina Dickmann, a legislação brasileira recebeu, recentemente, duas novas leis que buscam maximizar o alcance da lei penal e processual ao ambiente virtual.

A Lei 14.155/21, que veio modificar e incluir sanções referentes aos crimes de invasão de dispositivos informáticos, furto mediante fraude eletrônica, estelionato m mediante fraude eletrônica dentre outras questões relevantes. E a Lei 14.132/21, que inseriu o Art 147-A, denominado crime de perseguição em ambiente virtual.

Assim, o objetivo do presente estudo consiste em ressaltar a importância da Lei Karolina Dickmann como percursora para o surgimento de novas Leis de combate aos crimes vrtuais.

2 REFERENCIAL TEORICO

2.1 Crimes Cibernéticos

A Internet, como é popularmente conhecida a rede mundial de computadores, surgiu em meio à guerra fria, por volta da década de 60, para atender a necessidade dos militares em estabelecer uma rede de comunicação com a finalidade de tornar a troca de informações mais ágil. Entretanto, foram nos anos 70 e 80 que, além de suprir as necessidades militares, a Internet passou fazer parte da comunicação entre docentes e discentes em todo o mundo, como ferramenta para troca de conhecimentos acadêmicos, e posteriormente para a troca de mensagens e descobertas utilizando as linhas da rede em todo o mundo (WENDT, 2018).

O avanço tecnológico surgiu mediante a criação da *Word Wide Web*, ou seja, da rede mundial de computadores (Internet) sugerida pelo físico britânico Tim Berners-Lee em 1989, todavia, foi somente no ano seguinte, em 1990, que o jovem estudante Robert Cailliau conseguiu realizar a primeira comunicação bem-sucedida entre um usuário chamado de HTTP e um servidor utilizando a Internet (HEITLINGER, 2020).

No Brasil o uso da Internet iniciou-se apenas 1991 por meio da Rede Nacional de Pesquisa (RNP), que consistiu em uma operação acadêmica do Ministério de Ciências e Tecnologia (MCT) (GIMENES, 2019). O principal objetivo da RNP em trazer a Internet para o Brasil foi disponibilizar uma conexão entre as universidades e os centros de pesquisas, entretanto, em pouco tempo os domínios federal e estadual também iniciaram suas conexões.

A Internet ainda era considerada uma experiência, mas no segundo semestre do ano de 1994, a Embratel passou a difundir o seu serviço, já os Ministérios de Comunicação e de Ciências e Tecnologia, em 1995, disponibilizaram comercialmente a Internet, assim os provedores puderam ajustar suas conexões com a RNP, e consequentemente, com a Embratel. Logo depois deste feito, se deu a abertura foi autorizado a exploração da Internet de forma comercial para a população brasileira (ABREU, 2016).

A infraestrutura básica referente a conexão e informação no Brasil ficou sob a responsabilidade da Rede Nacional de Pesquisa, inclusive, controlando o *backbone* (rede de transporte). Atualmente todos os estados brasileiros são interligados por *backbone*, além de várias conexões com outros países (GIMENES, 2019).

> Atualmente estima-se que ao final do ano de 2013 existam 2,7 bilhões de usuários de internet em todo o mundo; destes, 120 milhões são brasileiros. No entanto, conforme apresenta a UIT (União Internacional de Telecomunicações) 4,4 bilhões de pessoas no mundo ainda não possuem acesso à internet. No tocante aos países mais conectados e com as melhores tecnologias de rede, a Coreia do Sul ocupa o topo da lista, seguida de perto por Suécia, Islândia, Dinamarca e Finlândia. Os Estados Unidos ocupam a 17º posição do ranking, enquanto o Brasil está no 62º lugar [...] (ONU...2013).

Assim, percebe-se que a Internet é utilizada como ferramenta responsável por constar e integrar pessoas e empresas, construído ao longo dos anos uma nova forma de comunicação bastante preocupada com a segurança da informação e a privacidade dos usuários.

Com o passar do tempo, pode-se afirmar, que as pessoas que cometem crimes virtuais são bem diferentes das pessoas que faziam o mesmo na década de 70, houve uma evolução sistemática dos usuários, uma vez que atualmente qualquer indivíduo que tenha um conhecimento mínimo de informática e acesso a Internet pode ser um potencial criminoso cibernético.

2.2 Conceito de Internet e Crimes Virtuais

A Internet constitui a Rede Nacional de Computadores que tem como finalidade integrar uma rede de computadores com o objetivo de realizar a troca de informações entre eles, utilizando para sua identificação o endereço de IP, conforme pode ser apresentado abaixo:

> A definição do conceito de internet pode ser apresentada como uma rede de computadores interligada a uma rede de menor porte que se comunica entre si, utilizando um endereço “lógico” chamado de endereço IP, onde diversas informações são trocadas, surgindo daí um problema, pois existe uma infinidade de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à internet, e quando não são disponibilizadas pelo próprio usuário, são procuradas por outros usuários que buscam na rede o objetivo única e exclusivamente de de cometer crimes, os denominados Crimes Virtuais [...]. (FLOR, 2012, p. 3).

Em 1970 aconteceram os registros dos primeiros crimes cibernéticos, e seus autores eram usuários que conheciam profundamente a área da informática, que tinham como principal objetivo invadir os sistemas de segurança de grandes organizações empresariais (DIANA, 2024).

> Os primeiros crimes de informática iniciaram-se na década de 70, sendo executados em sua grande maioria por pessoas especializadas no ramo informático com o objetivo principal de adentrar ao sistema de segurança das grandes empresas tendo como maior foco as denominadas como instituições financeiras. O perfil atual dos criminosos que atuam nessa área foi alterado, já que nos dias atuais qualquer pessoa que tenha um conhecimento, porém não tão aprofundado basta ter acesso a rede mundial de computadores para que consiga lograr êxito na execução de um crime virtual. (CASTRO, 2010, p.9).

Os crimes cibernéticos podem ser conceituados como uma invasão de um sistema de informática quando o invasor não possui a autorização para utilizá-lo, com a notória intenção de subtrair, modificar e danificar dados essenciais para o funcionamento do sistema invadido.

> Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes. (PINHEIRO, 2010, p. 46).

Dentro deste contexto, reafirma-se que o supracitado crime consiste em acessar sistemas da informação não permitidos, com a finalidade de gerar danos e/ou transtornos aos seus proprietários alterando dados pessoais ou empresariais sigilosos.

> As denominações que fazem referência aos crimes praticados no mundo virtual são inúmeras, não há uma concordância referente a melhor denominação para se usar para com os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, fraude informática, assim os conceitos ainda não englobam todos os crimes ligados à tecnologia. (CRESPO, 2011, p. 48).

Vale salientar que diversas pesquisas realizadas em vários países mostram um crescimento alarmante desse tipo de crime.

> [...] o número de vítimas diárias de crimes cibernéticos está ao redor de 1 milhão de pessoas. A sociedade humana global tem um prejuízo anual de US$ 388 bilhões. O Brasil figura como um dos países com elevado prejuízo que se aproxima de R$ 105 bilhões, equivalente a US$ 60 bilhões (MALAQUIAS, 2012, p. 52).

Segundo Fragoso (2020), tão importante quando tudo que já fora mencionado até o momento é salientar que é necessário que a denominação dos delitos seja estipulada conforme o bem jurídico protegido, classificando os crimes na parte

especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.

Desta forma, sugere-se em se tratando de um crime virtual, a princípio analisar se realmente corresponde-se a um cibercrime e posteriormente aplicar a sanção penal adequada, considerando sempre, o bem jurídico tutelado. Frente aos vários pensamentos doutrinários sobre a classificação dos crimes virtuais, encontra-se a seguinte sugestão de Moura referente a classificação dos crimes virtuais:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (MOURA, 2020, p. 261).

Ressalta-se que entre todas as doutrinas existentes utilizadas paras classificar os crimes supracitado, aquela que mais chega próxima da vida real apresenta-se entre crimes virtuais próprios e impróprios.

2.3 Os Desafios na Investigação Criminal

Diante da constante evolução da tecnologia, principalmente da cibernética, como já mencionado, constata-se o elevado crescimento dos crimes praticados por meio de computadores e da internet, os chamados cibercrimes, que acabam por gerar cada vez mais danosos no mundo jurídico. Segundo afirma Verçosa (2020), afirma que as brechas no código penal, no que se diz respeito a crimes cibernéticos, põem os criminosos do ramo mais à vontade para a prática de condutas ilícitas, entretanto, quando se consegue identificar a origem ou autoria desses crimes, ocorre a tentativa de penalização por vias análogas de clássicos e antigos crimes.

Existem muitos desafios que envolvem o decorrer de uma investigação relacionada a crimes cibernético, especialmente as dificuldades do investigador em buscar provas materiais.

Por este e outros motivos, em 2013 o Brasil passou a ocupar o quinto lugar mundial na lista dos países que mais tiveram corporações vítimas de fraudes digitais no mundo, e no ano seguinte, 2014, passou a ocupar o quarto posto da devida lista.

As fraudes digitais vêm crescendo cada vez mais por vários motivos, dentre eles a dificuldade de identificar e localizar seus autores. O primeiro passo em uma investigação para se localizar e identificar o autor de um crime cibernético é a identificação do número IP (Internet Protocol). O IP é um “endereço” utilizado exclusivamente por um determinado usuário, durante o período em que este esteja conectado na rede (PIMENTEL, 2020).

Quando isto acontece, cabe ao provedor de acesso disponibilizar informações suficientes que permitam localizar e identificar o infrator. Porém para que isto se torne realidade se faz necessária que exista mecanismos legais cuja finalidades seja obrigar os provedores de acesso a armazenar e fornecer as informações de seus usuários por um determinado tempo com a finalidade de vincular os provedores ao dever de colaborar no processo. (MEDEIROS, 2020)

Todavia, é lamentável observar que de modo geral os provedores não fornecem as referidas informações sigilosas sem que seja realizado um “*pedido de quebra de sigilo de dados telemáticos”,* uma vez que estes, não são obrigados a guardar os registros de acesso quando um determinado indivíduo acessa a Internet. Esta rotina torna bastante difícil a persecução penal na busca da infração em crimes por computador, notadamente na Internet. (LIRA, CAVALCANTI, 2021, p.17)

Outra questão a ser observada, é que a identificação das máquinas pelo IP permite identificar, em muitos casos, apenas as máquinas, mas não quem provocou o delito, ou seja, nem sempre que se consegue identificar o local ou a máquina através da qual o ato ilícito tenha sido cometido garante a identificação do autor do fato típico (VERSIANNI, 2019).

Sempre que for necessária a aplicabilidade ou não da lei brasileira aos crimes de informática é fundamental levar em consideração as ressalvas dos artigos 5º- o princípio da territorialidade que impõe a aplicação da lei brasileira ao crime cometido no território nacional - e 6º do Código Penal - o princípio da ubiqüidade, que considera lugar do crime tanto aquele da conduta, quanto o do resultado (SANTOS, 2013).

Desta forma, quando o cibercrime tem início, desenvolvimento e seus resultados podem ser verificados no Brasil este ato ilícito deve ser apreciado conforme a legislação brasileira (LIRA, CAVALCANTI, 2021), ou seja, neste coso, a investigação do crime é devidamente atribuída ao Estado onde o mesmo ocorreu e sancionado conforme a legislação do mesmo (BRASIL, 2006).

Vale salientar que o direito digital no Brasil busca a evolução quanto a aplicações de leis e uma nova visão dos juristas para definir a fisionomia da Internet avaliando primeiro se é possível compará-la com outros meios de comunicação conhecidos.

2.4 Tipificação dos Crimes Virtuais

É interessante perceber que o crime virtual é visto como um crime de meio, pois é cometido virtualmente, podem ser divididos em tipos, e os meio mais comuns para se praticar um crime virtual é através do phishing, spam ou malware (VIANNA, 2019.

Desta maneira, pode-se observar que a maior dificuldade em se tipificar os crimes cibernéticos consiste na concretização do indivíduo possuidor de jurisdição adequada para julgar o delito. Levando em consideração, o princípio da territorialidade, que direciona o entendimento de quem deverá solucionar o referido conflito de competência, uma vez que atualmente a legislação específica para as diversas modalidades de delitos ainda é bastante escassa (SANTOS, 2013).

Phishing são caracterizadas por conversas ou mensagens falsas com links fraudulentos que através de e-mail de spam ou outras formas de comunicação que são enviadas com o intento de induzir aqueles que recebem, a fazer algo que prejudique a segurança pessoal ou da organização onde trabalham. Essas mensagens, tendem a conter anexos infectados ou links que redireciona a vítima para sites maliciosos. Já o spear-phishing, que é quando a mensagem enviada vem com o intuito de se passar por uma pessoa influente, como por exemplo o CEO da empresa (SILVA, 2021).

Sending and Posting Advertisement in Mass ou Spam, se trata de mensagens enviadas sem o consentimento do usuário, ou seja, a mensagem chega sem a permissão ou desejo da vítima de receber, apresentando um produto ou serviço com o intuito de que a pessoa se interesse e acaba acessando o link fraudulento. Vale salientar que o Spam ainda ´´e utilizado com o intuito de propagar uma história falsa, e ao clicar, as informações de dados financeiros e pessoais são roubadas (ABREU, 2016).

Os malwares são softwares maliciosos instalados sem permissão do usuário. São conhecidos alguns vírus como cavalos de Tróia, spywares e ransomwares. Um malware é, geralmente, desenvolvido por trackers que, cujo objetivo de ganhar

dinheiro, através da proliferação do próprio malware ou leilão na deep web (ABREU, 2016).

A invasão de dispositivos informáticos está prevista no artigo 154-A do Código Penal, quando um dispositivo de processamento, dispositivos de entrada ou saída são indevidamente violados. A lei 9.610 de 1998 aborda sobre a pirataria de software, que é quando dados são copiados em Cd's, DVD's e outras bases de dados, sem a autorização do autor (PERRIN, 2024).

Outros crimes também ocorrem de modo virtual, tais como a difamação que consiste e imputar a alguém fato, com circunstâncias descritivas, ofensiva a sua reputação, por meio da internet. A calúnia, como por exemplo as fake News, popularmente conhecida atualmente, é a divulgação de notícias falsa (SILVA 2020).

E injúria ou também conhecido no meio virtual como cyberbulliying, é ofender a dignidade de alguém através da internet. Estes crimes estão previstos nos artigos 138, 139 e 140 respectivamente do Código Penal (PERRIN, 2024).

Outra prática muito comum nos dias de hoje, é a divulgação de conteúdo sexual, sem a permissão da pessoa envolvida, podendo ocorrer até mesmo casos de pedofilia. Muitos sites criam conteúdos que abordam explicitamente atos sexuais cujos participantes são menores de idade, além de fotos de nudez e cenas para satisfação de desejos sexuais dos criminosos (TERCEIRO, 2024).

Esses crimes estão previstos nos artigos 241-A e 241-E da lei 8.069/90 onde caracterizam como crime as ações de oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por meio de sistema de informática, fotografia, vídeo ou outro registro que contenha qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais (VERSIANNI, 2019).

3 RESULTAOS E DISCUSSÃO

A Lei nº 12.737/12, conhecida extraoficialmente como Lei Carolina Dieckmann, tem como finalidade agregar ao Código Penal dispositivos legais que tipificam delitos cibernéticos. A referida veio minimizar a lacuna outrora existente na legislação por onde se era permitido que as condutas indesejadas praticadas tanto no ambiente virtual quanto no físico em relação à proteção de dados e informações pessoais ou corporativas se mantivessem impunes. Desta forma é notória que o advento da

supracitada lei representa um avanço considerável na garantia da segurança de dados (WENDT, 2019).

Os artigos 154-A e 154-B foram acrescentados ao Código Penal, fazendo-se referência aos crimes conta a liberdade individual, seção referente aos crimes contra a inviolabilidade dos segredos profissionais, porém, vale salientar que as novas tipificações são colocadas como delito e não como crime. Desta forma, reforça-se a diferença de que o delito (a *deliquendo*) consiste em realizar atos que possam ser considerados como transgressões legais de natureza leve, o interessante é que este conceito é oriundo da Idade Média, onde as escolas clássicas francesas admitiam a divisão tripartite em que crime é transgressão legal de natureza grave, delito é a transgressão legal de natureza leve e contravenção tem natureza levíssima (PESSINA, 2016).

É fundamental eu toda legislação penal atenda ao princípio da legalidade (CF Art. 5º), com este objetivo é necessário que a lei seja o mais clara possível, apresentando-se de forma taxativa, escrita e certa (TOLEDO, 2019). Ressalta-se, então, que a Lei nº 12.737/12 busca tutelar o bem jurídico da liberdade individual, do direito ao sigilo pessoal e profissional, por serem elementos de fundamental importância para o convívio social. Carolina Dieckmann foi apenas uma das inúmeras vítimas de invasão de dispositivos de informática, por se tratar de uma pessoal pública, o fato recebeu uma maior visibilidade ao antigo problema, entretanto, os relatos de abusos no ambiente cibernético são inúmeros e variados.

Têm se observado que as invasões de computadores e dispositivos similares, com finalidades ilícitas, são responsáveis por causarem sérios prejuízos aos direitos individuais e profissionais. É importante compreender que o ato de invadir em si, independente do que se siga após ela, já representa um perigo concreto à privacidade e ao segredo juridicamente protegido. Dessa forma, a prova da invasão já é suficiente para promover a ação contra o agente.

É interessante observar alguns artigos do Código Penal que fazem referência a invasão de dispositivos de informática, tais como:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Tendo como finalidade a proteção do direito ao sigilo de dado e informação pessoal ou profissional, o art. 154-A veio tipificar duas condutas: a principal é invadir dispositivo informático e a acessória é instalar vulnerabilidade. Podem ocorrer na forma simples (com a aplicação da pena básica) ou qualificada (com o agravamento da pena). (TOLEDO, 2019)

O agente ativo dessa conduta pode ser uma pessoa física ou jurídica. Apesar de a lei não tratar essa matéria de forma especial, pois é necessário que haja uma legislação especial sobre o assunto, acredita-se ser esta uma espécie de crime próprio, pois para que o crime seja classificado como eletrônico ou cibernético, é preciso que o agente ativo possua certa habilidade no campo da informática, por mínima que seja, desta forma defende-se que esse não é um crime comum (PERRIN, 2024).

Compreende-se que nem todo mundo seja capaz de praticar o referido tipo de crime, pois ainda são facilmente encontrados os chamados “analfabetos digital”, configura-se o indivíduo que não estabelece nenhum tipo de contato aparelhos eletrônicos. Uma vez que sem que haja o mínimo conhecimento técnico, mesmo que seja o simples fato de saber ligar e desligar um dispositivo informático, a conduta se torna impossível (PECHECO, 2024).

O agente passivo é aquele que é o proprietário do aparelho, podendo ser pessoa física ou jurídica. A administração pública também é considerada como um agente passivo. Seja como for, a sociedade será sempre a vítima permanente dessas condutas, desta forma, cabe ao Estado permanecer presente como agente passivo, uma vez que ele é o titular do direito de punir (*jus puniendi*) (SILVA, 2021).

O objeto material na efetivação do crime é obter por meios ilícitos dados ou informações, por outro lado, pode existir vários objetos jurídicos, ou seja, o bem tutelado, dependendo da finalidade da conduta: no caso de o agente invadir para obter dados bancários e com eles furtar conta bancária, a proteção legal está sobre o sigilo e posteriormente sobre a propriedade. Este é o caso de delito pluriofensivo pois a invasão pode ofender mais de um bem jurídico: a lei protege o direito ao sigilo e a propriedade (material ou imaterial) (SILVA, 2021).

É interessante que se compreenda que “dispositivo informático” é um termo popular utilizado para se referir aos equipamentos eletrônicos que constituem o

Hardware (equipamento físico) e Software (equipamento lógico). Assim, percebe-se que uma quantidade substancial de dispositivos pode ser envolvida por esta lei, e não apenas PC ou notebook (ABREU, 2021).

Quando se utiliza o termo “invadir” o dispositivo informático alheio, é para se referir a conduta do agente. Desta forma, pode-se dizer que esta é uma conduta tipicamente dolosa, uma vez que a ação de invadir depende da vontade, da determinação consciente e livre do agente. Entende-se, neste sentido, que a invasão é só o meio pelo qual o agente utiliza para tirar proveito. Dentro deste contexto, é possível afirmar que quando alguém possui a capacidade técnica para invadir um sistema de informática, ele quer o resultado (Art.18, I, CP). Quem invade um sistema ou instala uma vulnerabilidade, sabe exatamente do resultado que quer obter (ABREU, 2021; SILVA, 2021).

O ato de invadir encontra-se subjugado a utilização de força, artimanha, violação indevido de mecanismo de segurança, ou seja, de atos que por si ultrapassam o limite de autorização fornecida pelo titular do equipamento, constituindo-se na realização de uma conduta proibida do agente.

Desta forma se compreende que a violação sem si, independente do grau de proteção, já se configura delito. Entretanto caso, não haja nenhuma forma de resistência, a invasão não pode ser caracterizada. Assim, o delito em tela é a invasão ou instalação de vulnerabilidade, uma vez que o que se faz após ela não interessa, pois a invasão já consuma o delito (WENDT, 2018).

Na maioria dos casos, as invasões tem como objetivo a finalidade de obter, adulterar ou destruir dados ou informações. Porém, existem situações onde os resultados pode ser naturalísticos, ou seja, permeiam o mundo físico, como foi o caso da divulgação de fotos íntimas da atriz Carolina Dieckmann, pois feriu a honra, a dignidade, a liberdade pessoal da vítima, entretanto a exigência da mesma não é fundamental para a consumação do fato, mas o caráter formal do tipo independe do resultado, o delito se configura com a efetivação da invasão, o que resulta desta invasão é o irá determinar a qualificação do tipo e o mero exaurimento da conduta delitiva.

Uma observação interessante é a que tentativas de invasão não são consideradas como conduta punível, porém pode ocorrer por que a invasão de um “dispositivo informático” se faz mediante preparação. Existe um *iter criminis*, isto é, um

caminho para se chegar ao resultado. Para efetivar a invasão é necessário obter a máquina ou conseguir os meios para acessá-la de forma remota, utilizar programas ou equipamentos, ferramentas que possibilitem o acesso. Pode-se alcançar arquivos de um Disco Rígido (HD) de várias formas: pela própria máquina, extração do HD e instalação do mesmo em outra máquina; acesso do HD a distância e até mesmo o seu controle, instalação de um software espião com a finalidade de copiar dados e os envia para uma máquina remota ou móvel, é possível, ainda extrair dados de um HD que se encontre parcialmente destruído.

Percebe-se que apenas a violação não oferece subsídios para a ocorrência do tipo “invasão”. É necessário que a violação seja indevida. O legislador sugeri que que haja casos de violação devida ou necessária. A ordem judicial é uma das exceções que torna a violação um mal necessário. Quando se ocorre uma violação com a finalidade de manutenção e reparo do equipamento, esta não pode ser alvo de penalização.

A invasão pode ocorrer por meio eletrônico, através do uso da rede mundial de computadores e programas ou dispositivos que permitam o acesso remoto ao dispositivo informático ou por meio físico, isto é, quando o agente tem acesso direto ao equipamento.

É fundamental que se compreende o termo “mecanismo de segurança” de maneira ampla, pois, o contrário torna a lei sem eficácia já que nem sempre o titular de um dispositivo vai colocar senha, antivírus, firewall (software que protege o computador de determinados ataques virtuais) ou outra tecnologia de segurança. Além disso, o artigo torna-se antagônico, se for tomado ao pé da letra: por qual motivo o legislador exigiria ao mesmo tempo a violação indevida de mecanismo de segurança e, a ausência de autorização expressa ao titular do dispositivo? Ora, na violação indevida, como o termo já faz alusão, não houve autorização, e quando se há autorização é impossível cogitar a possibilidade de violação do mecanismo de segurança.

Todavia, é interessante compreender que a ausência de um “mecanismo de segurança” não isenta o agente de responder dentro dessa qualificação penal, entretanto, a depender do caso, a conduta do agente pode se adequar a outros tipos penais já em voga: constrangimento ilegal, ameaça, violação de correspondência, divulgação de segredo, furto, roubo, extorsão, dano, apropriação indébita, estelionato e etc.

Ainda com relação a violação indevida de mecanismo de segurança, é importante considerar o ambiente cibernético, pois o mesmo apresenta inúmeras armadilhas e sofisticadas formas de “invasão” remota dos dispositivos informáticos. Desta forma, este aspecto legal não pode ser absoluto. O ato inconsciente de clicar em um link malicioso, por imperícia ou boa-fé, e ter seus dados furtados, não pode ser excluído do novo tipo penal.

A Lei Geral de Proteção de Dados (LGPD) foi aprovada em 2018 pelo então presidente Michel Temer e estava prevista para entrar em vigor dois anos depois, porém, a medida provisória 959/20 tentou adiar esse prazo, mas acabou sendo derrubada pelo Senado Federal. Dessa forma, a LGPD entrou em vigor, logo que a lei de conversão da Medida Provisória foi promulgada, situação esta que ocorreu no dia 19 de setembro de 2020.

Essa nova lei visa criar um cenário de segurança jurídica, tornando uniforme as normas e práticas, para que possa ser promovida a proteção de forma igual dentro e fora do país, aos dados pessoais de todos os cidadãos que estejam no Brasil. Ela define como dados pessoais todas as informações que possam identificar de forma direta ou indireta um indivíduo vivo, como por exemplo Rg, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via 21 GPS, retrato em fotografia, prontuário de saúde, cartão de banco, renda, histórico de pagamentos, hábitos de consumo, preferencias de lazer, endereço de Protocolo da Internet e cookies, entre outros (SERPRO, 2020).

As crianças e adolescentes merecem um cuidado especial, e por isso ficou definido que esses dados exigem um cuidado ainda mais cauteloso, conhecidos como dados sensíveis e que sejam eles tratados no meio físico ou digital, estando sujeitos a regulamentação.

A LGPD deve ser cumprida independente de a sede da organização ou o centro de dados ser no Brasil ou não, quando o processamento de dados for sobre pessoas que estiverem em solo brasileiro, mesmo que não seja brasileiro e em caso de compartilhamento de dados com organizações internacionais ou outros países, é necessário que tenha protocolos para garantir a segurança e o cumprimento de exigências legais (SERPRO, 2020).

A nova lei trouxe um ponto importante, que é o consentimento, ou seja, para que dados pessoais possam ser tratados, é fundamental que tenha o consentimento do cidadão.

Porém, há exceção para os casos em que for indispensável para cumprir uma obrigação legal, executar políticas públicas prevista em lei, realizar estudos através de órgãos de pesquisa, executar contratos, defender direitos em processo, preservar a vida e a integridade física de uma pessoa, tutelar ações feitas por profissionais das áreas da saúde pública ou sanitária, prevenir fraudes contra o titular, proteger o crédito ou atender a um interesse legítimo, contanto que venha a ferir os direitos fundamentais do cidadão (SERPRO, 2020).

Essa proteção se estende também aos diretos do cidadão, que pode requerer que dados sejam apagados, pode desistir do consentimento, transferir dados para outro fornecedor de serviços, entre outros, além de que o tratamento de dados tem que ser feito respeitando alguns quesitos, como a finalidade e a necessidade, que devem ser acertados e informados ao cidadão antes de ter acesso aos dados.

Ficou estabelecido que o órgão responsável pela fiscalização será a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

Essa instituição ficará responsável pela fiscalização e, em caso de descumprimento da lei, poderá penalizar. Fica a cargo da ANPD também regular e orientar como a lei deve ser aplicada.

E por último, a LGPD tem também o papel de administrar os riscos e falhas, ou seja, os responsáveis por administrar a base de dados pessoais deve elaborar normas de administração, cumprir medidas de segurança e em caso do vazamento dos dados, a ANPD e as pessoas envolvidas devem ser avisados imediatamente.

As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil, e no limite de 50 milhões por infração. Os níveis de penalidades serão fixados pela autoridade nacional de acordo com o grau da falha. E enviará alertas e orientações antes de aplicar sanções as organizações (Serpro, 2020, online).

CONCLUSÃO

Diante o atual cenário onde as transformações digitais são amplas e notórias também há um considerável crescimento da responsabilidade dos profissionais da informação como produtores do conhecimento no campo cientifico, assim como dos profissionais da área jurídica, como interpretadores das leis aplicáveis na comunicação da informação.

Após o presente estudo é possível afirmar que o crime virtual é certamente uma realidade que acontece no espaço cibernético, especialmente diante do crescimento da utilização das tecnologias e do ambiente virtual. Ao longo dos anos, foi possível perceber que cada vez mais os usuários das redes e da Internet no Brasil, são vítimas de condutas lesivas praticadas mediante o uso de computador e/ou da Internet.

Um fato bastante interessante é que em toda a sociedade digital mundial, independente do espaço geográfico, existe uma necessidade de interpretar as leis para aplicação na execução de atos ilícitos.

Diante do mencionado crescimento da utilização da tecnologia e consequentemente, das transformações sócias seguidas pelo aumento descontrolado da informatização se fez necessária a elaboração de uma lei especifica referente a tipificação criminal de delitos cibernéticos.

Tendo em vista tal necessidade, surge a Lei nº 12.737/12, mencionada neste estudo, cuja tipificação do crime denominado “Invasão de dispositivo informático”.

A supracitada Lei ficou popularmente conhecida como “Lei Carolina Dieckmann”, devido ao fato da citada atriz ter suas imagens intimas e pessoais subtraídas do seu computador pessoal durante manutenção da máquina por um técnico em informática e divulgada nas redes sociais seu o devido consentimento da mesma.

Casos como este contribuem para firmar que os benefícios que surgiram com a internet são proporcionais as condutas ilícitas que se seguiram mediante as práticas dos agentes especializados neste campo.

Diante deste contexto, percebe-se que o surgimento da nova Lei nº 12.737/12, representou significativa mudança no nosso ordenamento jurídico, levando em consideração que esta lei tratar de crimes cada vez mais constantes na ocorridos na sociedade, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

Salienta-se que mesmo que a legislação referida tenha o intuito de preencher lacunas outrora percebidas no Direito brasileiro, ainda existem lapsos que necessitam ser devidamente preenchidos no atual ordenamento, uma vez que o texto da Lei em comento permite várias interpretações, além disso, as reduzidas penas aumentam as chances do Estado perder o direito/dever de punir mediante a ocorrência da prescrição.

REFERÊNCIAS

ABREU, L.F. dos **. A Segurança das Informações nas Redes Sociais.** Disponível em: Acesso em: 18 de setembro.2017

ANDREI, L. **A história da internet** – Do Início ao Status Atual da Rede. Web Link, 2019. Disponível em: https://www.todamateria.com.br/referencia-site-abnt/. Acesso em: 03/01/2024;

BRASIL. Ministério Público Federal. Procuradoria da República do Estado de SP. **Crimes Cibernéticos**: manual prático de investigação. São Paulo, 2006. Disponível em: <http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf> Acesso em: 31.out. 2011

CARVALHO, S. de. **Penas e medidas de segurança no direito penal brasileiro:** fundamentos e aplicação judicial. São Paulo: Saraiva, 2018.

CASTRO, J.A.L. (Coord.). **Direito processual:** interpretação constitucional no estado democrático de direito. Belo Horizonte: PUC/Minas, 2010. 1016 p.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Notícia**. 2013. Disponível em: http://www.cert.br>. Acesso em: 23 set. 2015.

CRESPO, M.X.F. de. **Crimes digitais.** São Paulo: Saraiva, 2011.

DAOUN, A.J.; LIMA, G.T. **Crimes Informáticos:** O Direito Penal na Era da Informação. 2010. Disponível em: <http://www.truzzi.com.br/pdf/artigocrimes-informativos-gisele-truzzi-alexandre-daoun.pdf> Acesso em: 30 out. 2011.
DIANA, D. História da Internet. Toda Matéria. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 12/01/2024;

DOTTI, R.A. **Curso de direito penal:** parte geral. 3. ed. São Paulo: Editora Revista dos Tribunais, 2010.

FRAGOSO, H.C. **Lições de direito penal:** parte especial, arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983

FLOR, R. Perspectiva para os novos modelos de "investigação tecnologica" e proteção de direitos fundamentais na era da internet. **Revista Brasileira de Ciências Criminais.** São Paulo: Revista dos Tribunais, v.20, n.99, p. 69-100, nov./dez. 2012.

GIMENES, E. Crimes virtuais. **Revista de Doutrina TRF4**. Ed 55, agos. 2019. Disponível em: www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html#09. Acesso em: 05/01/2024.
LIRA, K.W.C. CAVALCANTI, J.I.N.C. **Crimes Praticados via Internet e suas Consequências Jurídicas. 2021.** Disponível em:

http://manfred.com.br/publico/unerj/tecnologia_em_informatica/seguranca_em_sistemas_de_informacao/extras/Artigo%20-%20Crimes%20Praticados%20via%20Internet%20e%20suas%20Conseq%FC%EAncias%20Jur%EDdicas.pdf Acesso em 31/01/2024;

MEDEIROS, C.L. de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos.** Universidade Estadual do Ceará, 2020. Disponível em: http://www.pgj.ce.gov.br/esmp/publicacoes/edf_2010/artigos/art05ClaudiaMedeiros.pdf Acesso em: 30/01/2024;

MOURA, P.A.R. Crime cibernético e seus aspectos no universo jurídico. Barbacena: [s.n.], 2012. 41 p. **Trabalho Conclusão de Curso** (Bacharelado em Direito) - Universidade Presidente Antônio Carlos. – UNIPAC, 2012.

MORAES. M.C.B. de. **O conceito da dignidade humana:** substrato axiológico e conteúdo normative. In: SARLET, Ingo Wolfgang (Org.). Constituição, direitos fundamentais e direito privado. 3. ed. rev. amp. Porto Alegre: Livraria do Advogado, 2020.

NETO, M.; GUIMARÃES, J. **Crimes na Internet**: elementos para uma reflexão sobre ética informacional. Brasília. 2013.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU): 4,4 bilhões de pessoas permanecem sem acesso à Internet. Artigo. Out.2013. Disponível em: http://blogoosfero.cc/rio-20/noticias-da-onu/onu-44-bilhoes-depessoas-permanecem-sem-acesso-a-internet . Acesso em 22 set. 2015.

PACHECO, W.E.P . **Manual de Responsabilização Penal dos Hackers, Crackers, e Engenheiros Sociais.** Disponível em: http://s.conjur.com.br/dl/guia-crimes-digitais.pdf. Acesso em: 18/12/2024;

PERRIN, S. **O Cibercrime.** Disponível em: https://vecam.org/archives/article660.html>. Acesso em 11/12/2023;

PINHEIRO, P.P. **Direito digital.** 4ª ed. São Paulo: Saraiva, 2010.

PIMENTEL, A.F. **O direito cibernético:** um enfoque teórico e lógicoaplicativo. - Rio de Janeiro: Renovar, 2020;

SANTOS, L.A. dos; CAMARGO, L.H.P.de . **Vírus de Computador:** Uma Abordagem do Código Polimórfico, 2013. Acesso em: 01 de setembro.2017.

SCHMIDT, G. Crimes cibernéticos. **Jusbrasil**, 2021. Disponível em: < http:// gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 20/01/2024;

SILVA, T.V. **Crimes Cibernéticos:** A era da Informação traz ameaça para a sociedade, 2021. Disponível em: http://www.conteudojuridico.com.br/artigo,crimesciberneticos-a-era-da-informacao-digital-traz-ameaca-para-sociedade,56091.html>. Acesso em: 30/12/2023;

TERCEIRO, C.F.V.R. O problema na tipificação penal dos crimes virtuais. Disponível em: O problema na tipificação penal dos crimes virtuais - **Jus.com.b**r | Jus Navigandi . Acesso em: 17/01/2024;

VERÇOSA, B.N. **Novo cenário dos crimes cibernéticos no Brasil e as leis que gerem esse mercado.** Goiás. 2020.

TOLEDO, F.de A. ***Princípios básicos do direito penal*.** 9ª Ed. São Paulo: Saraiva, 2019. Pág. 21-29.

VERSIANNI, J.A.C. **Cooperação Internacional na Investigação de Crimes Cibernéticos**. Rio de Janeiro: Mallet, 2019.

VIANA, T.; MACHADO, F. **Crimes informáticos.** Belo Horizonte: Fórum, 2019.

WENDT, E.; JORGE, H.V.N. **Crimes Cibernéticos**: Ameaças e procedimentos de Investigação. Rio de Janeiro: Brasport, 2018.