



CENTRO UNIVERSITÁRIO DE LAVRAS
CURSO DE GRADUAÇÃO EM DIREITO

Trabalho de Conclusão de Curso

**HISTÓRICO E NECESSIDADE DE IMPLEMENTAÇÃO DE MEDIDAS MAIS
EFICAZES NO COMBATE AOS CRIMES CIBERNÉTICOS**

ELENIR VASCONCELOS DOS SANTOS GUIMARÃES

LAVRAS – MG

2024

ELENIR VASCONCELOS DOS SANTOS GUIMARÃES

**HISTÓRICO E NECESSIDADE DE IMPLEMENTAÇÃO DE MEDIDAS MAIS
EFICAZES NO COMBATE AOS CRIMES CIBERNÉTICOS**

Trabalho de Conclusão de Curso
apresentado ao Centro Universitário de
Lavras, como parte das exigências da
disciplina Trabalho de Conclusão de
Curso (TCC), curso de graduação em
Direito.

ORIENTADORA

Profa. Me. Adriane Patrícia dos Santos Faria.

LAVRAS – MG

2024

Ficha Catalográfica preparada pelo Setor de Processamento
Técnico da Biblioteca Central do UNILAVRAS

G963h Guimarães, Elenir Vasconcelos dos Santos.
 Histórico e necessidade de implementação de medidas mais
 eficazes no combate aos crimes cibernéticos / Elenir Vasconcelos
 dos Santos Guimarães. – Lavras: Unilavras, 2024.

 42f.: il.

 Monografia (Graduação em Direito) – Unilavras, Lavras,
 2024.

 Orientador: Prof.^a Adriane Patrícia dos Santos Faria.

 1. Crimes on-line. 2. Internet. 3. Legislação. I. Faria, Adriane
 Patrícia dos Santos. (Orient.). II. Título.

ELENIR VASCONCELOS DOS SANTOS GUIMARÃES

**HISTÓRICO E NECESSIDADE DE IMPLEMENTAÇÃO DE MEDIDAS MAIS
EFICAZES NO COMBATE AOS CRIMES CIBERNÉTICOS**

Trabalho de Conclusão de Curso
apresentado ao Centro Universitário de
Lavras, como parte das exigências da
disciplina Trabalho de Conclusão de
Curso (TCC), curso de graduação em
Direito.

Aprovado em 22/11/2024

MEMBROS DA BANCA EXAMINADORA

Presidente - Prof. Pós-Dr. Denílson Victor Machado Teixeira / UNILAVRAS

Orientador - Profa. Me. Adriane Patrícia dos Santos Faria / UNILAVRAS

LAVRAS – MG

2024

Aos meus pais e demais familiares.
Vocês foram meu motivo para
chegar até aqui.

AGRADECIMENTOS

A Deus fonte da minha força, que me proporciona através da bíblia, instrução para adquirir conhecimento, entendimento e discernimento.

Aos meus pais e familiares, pelas palavras de incentivo e pelas orações.

Ao meu orientado pelos direcionamentos e orientações dadas durante a realização do meu Trabalho de Conclusão de Curso.

Aos professores, que fizeram parte dessa jornada, transmitindo-me os seus conhecimentos com tanto carinho e esforço, para que eu galgasse novos caminhos do conhecimento.

Aos amigos de sala que sempre contribuíram para tornar essa jornada mais leve.

E por fim a todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa.

“Foi o Senhor que fez isto, e é coisa maravilhosa aos nossos olhos. Este é o dia que fez o Senhor; regozijemo-nos e alegremo-nos nele (SALMOS 118:23-24)”.

RESUMO

Introdução: Nos últimos anos, o uso de tecnologias, principalmente da internet tem aumentado consideravelmente. No entanto, o uso da internet oferece vários riscos, que são considerados crime cibernético. **Objetivo:** Diante disso esse estudo tem por objetivo analisar o método de investigação e prevenção dos crimes cibernéticos e suas complexidades devido à lentidão do sistema judiciário e a constante evolução do crime. **Metodologia:** Para tanto, foi realizado um levantamento bibliográfico, mediante busca na internet de documentos que abordem sobre o tema em questão. A busca foi realizada em sites e bases de dados como o google acadêmico, considerando documentos publicados em inglês e português. **Resultados:** Foi discorrido como tem sido o método de avaliação dos crimes cibernéticos, bem como as práticas que podem auxiliar na prevenção desses crimes. Além disso, foi abordado sobre como ocorre o processo de julgamento e suas complexidades. **Conclusão:** Os dados apresentados poderão serem utilizados como subsídio em futuras tomadas de decisão por parte do poder judiciário, para implementação de políticas públicas que auxiliem nas melhores providencias diante do crime cibernético.

Palavras-chave: Crimes on line; Internet; Legislação.

ABSTRACT

Introduction: In recent years, the use of technologies, especially the Internet, has increased considerably. However, the use of the Internet poses several risks, which are considered cybercrime. **Objective:** In view of this, this study aims to analyze the method of investigation and prevention of cybercrimes and their complexities due to the slowness of the judicial system and the constant evolution of crime. **Methodology:** To this end, a bibliographic survey was carried out, by searching the Internet for documents that address the topic in question. The search was carried out on websites and databases such as Google Scholar, considering documents published in English and Portuguese. **Results:** The method of evaluating cybercrimes was discussed, as well as the practices that can help prevent these crimes. In addition, the trial process and its complexities were discussed. **Conclusion:** The data presented may be used as a subsidy in future decision-making by the judiciary, for the implementation of public policies that assist in the best measures in the face of cybercrime. **Keywords:** Online crimes; Internet; Legislation.

SUMÁRIO

1 INTRODUÇÃO	10
2 REVISÃO DE LITERATURA	13
2.1 DEFINIÇÃO DE CRIME CIBERNÉTICO	13
2.2 SISTEMA JUDICIÁRIO E O CRIME CIBERNÉTICO	15
2.3 MÉTODO DE INVESTIGAÇÃO	23
2.4 MÉTODOS DE PREVENÇÃO	35
3 CONCLUSÃO	38
REFERÊNCIAS.....	40

1 INTRODUÇÃO

Nos últimos anos, houve um crescente avanço no desenvolvimento de tecnologias, das quais merece um grande destaque a internet, tendo em vista que ela gera comunicação global e por meio dela pode-se realizar diferentes atividades e comunicação, até mesmo entre pessoas que não falam a mesma língua. No entanto, o uso da internet oferece vários riscos para quem a utiliza. Os crimes da internet são denominados de crime cibernético (Wendt; Jorge, 2013).

O crime cibernético, ou crime realizado por meio da utilização da internet, está se tornando cada vez mais difundido e, no entanto, a falta de consenso em torno do que constitui um crime cibernético tem um impacto significativo na sociedade, na resposta jurídica e política e na investigação acadêmica. As dificuldades na compreensão do crime cibernético começam com a variabilidade na terminologia e a falta de consistência na legislação sobre crimes cibernéticos entre jurisdições (Phillips, 2022).

A tecnologia digital e o crime cibernético são características generalizadas da vida moderna. Uma grande parte da população, hoje tem acesso à internet e aos aparelhos necessários para seu acesso (Menezes Neto; Moraes, 2018). Essa situação foi acelerada ainda mais com a pandemia da Covid-19, do qual, diferentes setores começaram a operar de forma *online* (Santos, 2021).

A crescente adoção da tecnologia digital provocou uma evolução no comportamento criminoso, resultando no aumento da ocorrência de crimes cibernéticos. No entanto, continua a haver falta de clareza sobre o que constitui exatamente um crime cibernético (Phillips, 2022).

De acordo com Maia (2017) o histórico dos riscos e ameaças computacionais por meio da internet evoluiu rapidamente em poucos anos. Nesse sentido, a autora afirma que há a necessidade de uma interação cooperativa global de combate a esse tipo de delito que não reconhece distâncias, através de Tratados, Convenções e outros mecanismos que sejam menos burocráticos por meio de uma legislação que permita uma celeridade e ao mesmo tempo garanta os direitos humanos.

Phillips (2022) argumentam que um possível fator que leva a dificuldades na estimativa do crime cibernético é a falta de definições bem formadas e sistemas de classificação capazes de dar conta da variedade de crimes cibernéticos existentes.

Este problema é ainda agravado pelo facto da legislação sobre crimes cibernéticos em todas as jurisdições não ser sistemática nem uniforme. Além disso, a própria legislação é frequentemente dispersa por vários estatutos criminais e civis, o que, por sua vez, resulta em esforços internacionais fragmentados para combater o crime cibernético.

Este estudo se justifica pelo fato do crime cibernético ser ainda, nos dias atuais, um crime de difícil apuração, e aponta também a necessidade de estudos e levantamentos sobre o tema em questão, para que as autoridades tenham embasamento para a implementação de futuras políticas públicas voltadas para o tratamento desse crime.

Dada a atual ambiguidade em torno do conceito de crime cibernético e os problemas relacionados com a investigação do crime, este artigo tem por objetivo analisar o método de investigação e prevenção dos crimes cibernéticos e suas complexidades devido à lentidão do sistema judiciário e a constante evolução do crime.

Para tanto, foi realizado um levantamento bibliográfico, mediante busca na internet de documentos que abordem sobre o tema de interesse desse estudo. A busca foi realizada em sites e bases de dados como o google acadêmico, *Web of Science* e *Scopus*.

A busca de informações foi realizada em língua portuguesa e inglesa, tendo em vista que o tema em questão vai além das fronteiras brasileira, e precisa ser tratado globalmente. Não foi colocado um limite da data de publicação do documento para ser utilizado nesse estudo. Além disso, foi realizada buscas também o google para incluir notícias referentes ao tema.

O foco do trabalho foi discorrer como tem sido o método de avaliação dos crimes cibernéticos, bem como as práticas que podem auxiliar na prevenção desses crimes e como esse fator tem sido apresentado no decorrer dos anos e como se apresenta na atualidade. Além disso, almejou-se descrever sobre como ocorre o processo de julgamento e suas complexidades.

Este trabalho encontra-se dividido nessa introdução, do qual é relatado o problema que ocorre para se investigar e julgar crimes cibernéticos, quais desafios são enfrentados e necessitam ser solucionados, bem como a justificativa em se realizar o estudo e seus objetivos, finalizando com uma breve descrição da metodologia empregada para se alcançar o objetivo proposto.

O segundo capítulo é composto pela revisão de literatura, onde será exposto o que foi encontrado na literatura sobre o tema abordado. Por fim é apresentado as considerações gerais, conclusões e as referências utilizadas no estudo.

2 REVISÃO DE LITERATURA

2.1 DEFINIÇÃO DE CRIME CIBERNÉTICO

De acordo com Castells (2003) a revolução tecnológica da informação se originou nos anos 70, desde então, o sistema tecnológico vem apresentando novas invenções, como: o microprocessador (1971), microcomputador (1975), o Apple-II primeiro pc comercial (1977), os primeiros softwares da Xerox Alto (1973), o comutador digital (1997), a produção da fibra óptica em escala industrial (1970), os primeiros videocassetes comerciais produzidos pela Sony. E finalmente, a invenção do TCP/IP, protocolo de interconexão que introduziu a conexão de redes, hoje conhecida como internet.

Segundo Faheem et al. (2018), o ritmo da informação e do desenvolvimento tecnológico nos apresenta um conceito variável e contextual, sendo difícil caracterizar o que é novo tanto em relação a equipamentos quanto aos processos. As estratégias de uso e o desenvolvimento de novos programas e produtos mudam a um ritmo tão intenso que o que é descrito hoje como novo poder estar obsoleto daqui a alguns meses.

O uso dessas tecnologias, principalmente a internet tem promovido o desenvolvimento acelerado dos diferentes setores, fato este que foi mais impactado depois da pandemia da Covid-19, do qual várias áreas passaram a utilizar o modelo *on line* para o desenvolvimento de suas atividades, como o setor educacional e da saúde. Contudo, esse avanço acelerado do uso da internet também trouxe consigo, de sérios riscos para as pessoas (Phillips, 2022).

De acordo com Maia (2017) pela internet é possível se conectar com outras pessoas sem exporem sua identidade, e isso, atrai criminosos, tendo em vista a sua difícil detecção. Assim, as pessoas têm a possibilidade de desenvolverem uma personalidade virtual diferente da vida real. Através desse ambiente tecnológico, alguns indivíduos mostram uma identidade desconhecida para muitos do seu círculo de relacionamentos em ambientes físicos.

A legislação de prevenção e combate ao crime cibernético é uma área em expansão, impulsionada pela dependência crescente da sociedade em relação à tecnologia digital. Governos e organizações internacionais confirmam a necessidade de proteger dados pessoais e garantir a segurança das transações online.

Os crimes que são realizados através da utilização da internet podem ser denominados de crime cibernético, embora este não seja a única denominação para este ato. Segundo Phillips (2022), vários termos têm sido utilizados para descrever o crime cibernético, que são aplicados desde o início deste campo, e continuam a ser utilizados na rotulagem deste fenómeno.

O prefixo 'cibernético' originou-se historicamente na cibernética e teve um significado particular dentro do campo. No entanto, à medida que a popularidade da tecnologia e o uso da tecnologia aumentaram nas décadas de 1980 e 1990, 'ciber' tornou-se uma palavra da moda, pois se tornou sinónimo de quase tudo relacionado a computadores e à Internet, por exemplo, ciberespaço, compras cibernéticas e navegação cibernética (Yar; Steinmetz, 2019).

Maia (2017) afirma que os crimes cibernéticos são delitos que ultrapassam as fronteiras geográficas dos países. Dessa maneira o termo crime cibernético tem sido considerado em diferentes terminologias. Um estudo realizado por Phillips (2022) descreveu pelo menos nove terminologias que esse tipo de crime pode receber: Crime cibernético, Crime virtual, E-crime, Crime na Internet, Crime digital, Crime on-line, Crime virtual, Techno-crime e Crime na rede. No entanto, o autor cita que o termo crime cibernético e crime virtual são os termos mais utilizados na literatura.

O que se percebe é que os problemas na definição do crime cibernético começam pela própria terminologia, do qual é utilizado um verdadeiro arsenal de terminologia, por vezes em combinação com os prefixos cibernético, computador, e-, internet, digital ou informação. Essa variabilidade nos termos e na linguagem do crime cibernético destaca a falta de um vocabulário partilhado entre os profissionais que trabalham na área (Phillips, 2022).

No início, o termo dominante para o uso indevido da tecnologia da informação para realizar algum crime era crime informático ou crime por computador e isso persistiu até aproximadamente o ano 2000. Com o tempo, o termo 'cibernético' passou a ser usado em relação a atividades prejudiciais ou ilícitas (por exemplo, crime cibernético, intimidação cibernética, terrorismo cibernético e perseguição cibernética) (Yar; Steinmetz, 2019).

Devido à amplitude de comportamentos que constituem o 'crime cibernético', também não existe um perfil correspondente óbvio do que constitui um 'criminoso cibernético'. Além disso, não está claro se os ciber criminosos devem ser conceituados como indivíduos, grupos, organizações/instituições ou, mesmo,

estados-nação. As tentativas anteriores de classificar os crimes cibernéticos concentraram-se no próprio ato criminoso; no entanto, poderia obter-se clareza ao ter em conta as características dos perpetradores (por exemplo, indivíduos, grupos do crime organizado e indivíduos coordenados) e as suas motivações.

Portanto, o termo 'crime cibernético' entrou na linguagem pública e internacionalmente, podendo ser esse um problema fundamental, a falta de uma abordagem sistemática e fundamentada na definição e rotulagem do crime cibernético. Assim, para classificar eficazmente os comportamentos desses criminosos existentes e emergentes, é essencial um quadro abrangente, que seja compatível com a legislação ou políticas internacionais e nacionais, o trabalho dos setores de segurança cibernética público e privado, e que possa acomodar resultados de pesquisas futuras à medida que o crime cibernético continua a evoluir (Phillips, 2022).

2.2 SISTEMA JUDICIÁRIO E O CRIME CIBERNÉTICO

Para se viver em uma comunidade é necessário que existam regras, assim, o Direito, tem por função auxiliar a manter um mínimo de ordem, direção e solidariedade, favorecendo assim, o relacionamento íntegro entre as pessoas e os grupos da sociedade no ambiente que ela vive, o que é uma das bases do progresso da mesma (Nader, 2004). Dessa forma, não é possível ter qualquer forma de convivência social sem regras, e nem sociedade sem Direito (Reale, 2002).

Nesse sentido, Maia (2017) ressalta que nos últimos anos tem ocorrido uma instabilidade na execução do direito do cidadão, sendo visualizado um aumento significativo da violência e da impunidade, o que acaba gerando uma insegurança jurídica. Ainda de acordo com a autora, essa situação, na qual as pessoas deixam de acreditar no aparato do Estado e do Direito, é muito perigosa e pode gerar sérios conflitos

Um outro ponto relatado por Maia (2017) é que o Direito deve promover o aperfeiçoamento frente a evolução da sociedade, se não por via legislativa, ao menos por via judicial jurisprudencial, pautando-se na democracia e no respeito à dignidade do ser humano. Assim, no que se refere ao avanço das tecnologias, que tem sido exorbitante, não tem se notado um acompanhamento por parte do Direito (Pádua; de Oliveira Frazão; Assunção, 2022).

Com isso, utilizando as novas tecnologias, diversos crimes têm se propagado, principalmente com a utilização da internet. Os crimes cibernéticos incluem um conjunto diversificado de ofensas e comportamentos prejudiciais. Por isso, existe a necessidade urgente de definições claras da legislação de prevenção e combate ao crime cibernético, principalmente devido a dependência crescente da sociedade pela utilização das tecnologias.

No estudo dos crimes cibernéticos, é necessário entender o que são os hackers e crackers. Estes detêm grandes conhecimentos informáticos, sendo o fator ético o que os diferenciam. Os Hackers são pessoas consideradas do “bem” que possuem grande conhecimento sobre computadores e superam os limites das máquinas. Eles partem do princípio de que todo sistema de segurança possui uma falha, e a função deles é justamente de encontrá-la (Assunção, 2002, p. 82).

Vale destacar que estes profissionais apenas documentam as vulnerabilidades detectadas e as reportam para a empresa contratantes de seus serviços, juntamente com indicações de como solucioná-las, aumentando com isso a segurança da organização, evitando prejuízos. Além disso, auxiliam as autoridades a desvendar delitos praticados no espaço virtual. Já os Crackers são os considerados “maldosos”, possuem alto grau de conhecimento e nenhum respeito, invadem sistemas e podem destruí-los completamente.

A figura 1, traduzida de Phillips (2022) fornece uma lista indicativa de atos e crimes cibernéticos.

Figura 1. Lista ilustrativa para demonstrar o alcance dos atos e crimes cibernéticos.

Redes de bots	Assédio	Material pornográfico
CSAM/CSE	Assédio	Radicalização
Coerção	Discurso de ódio	Ransomware
Falsificação relacionada a computadores	Roubo	Ofensas religiosas
Fraude informática	Roubo de identidade	Turismo sexual
Violações de direitos autorais	Acesso ilegal (hacking/cracking)	Comércio sexual
Comunicações criminais	Aquisição ilegal de dados	Tráfico sexual
Tropas cibernéticas	Jogo ilegal	Sexting
Cyberbullying	Jogo ilegal	Sextorção
Fraude cibernética	Interceptação ilegal	Spam
Guerra cibernética	Abuso baseado em imagem	Perseguição
Interferência de dados	Incitando a violência	Interferência do sistema
Falsificações profundas	Lavagem	Terrorismo
Pirataria digital	Uso indevido de dispositivos	Ofensas relacionadas a marcas registradas
Comércio de drogas	Multa de dinheiro	Trollando
Espionagem	Phishing	Xenofobia
Extorsão (por exemplo, fraude romântica)	Interferência política	

Material de abuso sexual infantil (CSAM); exploração sexual infantil (ESA).

Fonte: traduzida de Phillips (2022)

Essa lista demonstra a gama de crimes que se enquadram neste termo abrangente, incluindo uma combinação de crimes tradicionais, bem como crimes exclusivos do panorama cibernético. E mesmo diante dessa grande diversidade, Phillips (2022) afirma que essa lista não é exaustiva de crimes cibernéticos conhecidos. É provável que isto se deva em parte ao conjunto diversificado de comportamentos abrangidos por este termo, mas também porque o fenômeno está em constante evolução e o campo está em rápida expansão (Rosa, 2019.).

Conforme mencionado no tópico anterior, a dificuldade em classificar os crimes cibernéticos também dificulta a introdução de leis e regulamentos específicos

para esse crime, o que leva a desafios significativos no policiamento e na repressão do crime cibernético devido à compreensão e capacidade limitadas de resposta (Wendt; Jorge, 2013).

As diferentes taxonomias para os crimes cibernéticos conforme definidos pelos estatutos legais, introduz um segundo problema fundamental de não há crime sem lei. No entanto, um quadro baseado em crimes é problemático por três razões: em primeiro lugar, a tecnologia e os comportamentos ciber criminosos irão sempre ultrapassar a literatura acadêmica, as políticas e a legislação; em segundo lugar, o problema da circularidade (uma vez que as definições e classificações do crime cibernético são informadas por estatutos legais, que por sua vez informam os estatutos legais); em terceiro lugar, a falta de aplicabilidade universal, uma vez que a legislação sobre crimes cibernéticos difere entre as jurisdições (Black; Lumsden; Hadlington, 2019).

De acordo com Phillips (2022), conceituações imprecisas de fenômenos do mundo real podem levar a consequências negativas, por exemplo, consequências socioeconômicas para grupos sociais em risco, criminalização excessiva, erros judiciais ou aumento da prevalência de danos online. Dessa forma, a consolidação da terminologia e do âmbito entre disciplinas e jurisdições seria o primeiro passo no desenvolvimento de um sistema de classificação eficaz e uma condição necessária para poder desenvolver uma classificação abrangente e coesa do crime cibernético.

Maia (2017, p. 41) afirma para combater os crimes cibernéticos, é essencial a atuação conjunta da legislação, investigação e perícia, conforme citado abaixo

Entre os mecanismos de combate aos crimes cibernéticos no Direito Penal a legislação, investigação, e perícia assumem posições essenciais para o bom andamento dos processos criminais, tendo como consequência a punição dos indivíduos que se aproveitam dos meios digitais para lesar bens jurídicos tutelados pela esfera penal. Esses mecanismos são aspectos-chaves para inibição do crescimento dessas condutas inadequadas realizadas através da internet (Maia, 2017, p. 41).

Além do já citado, vale ressaltar que a legislação entre jurisdições não é sistemática ou uniforme, resultando em esforços internacionais não uniformes para combater comportamentos online prejudiciais, e isto é agravado pelo fato dos crimes cibernéticos terem pesos diferentes entre jurisdições e mudarem ao longo do tempo. Um outro fator que também tem chamado a atenção na jurisdição para o crime

cibernético é a inclusão de comportamentos prejudiciais realizados pela internet, que ainda não foram legislados. Alternativamente, os futuros sistemas de classificação poderão considerar abordagens alternativas, além de um quadro baseado em infracções; por exemplo, perfis comportamentais ou uma abordagem ontológica.

Os futuros sistemas de classificação devem adotar uma abordagem baseada no espectro para capturar com precisão a complexidade dos crimes cibernéticos e a evolução dos comportamentos ciber criminosos. Além disso, para evitar sistemas de classificação excessivamente simplificados e redutores, devem ser consideradas características definidoras adicionais (por exemplo, as características dos perpetradores, as características das vítimas, as motivações criminosas e os danos resultantes dos crimes) (Phillips, 2022).

Um dos marcos iniciais da legislação contra crimes cibernéticos foi realizada em Budapeste em 2001. Essa convenção foi promulgada o Brasil através do Decreto 11.491/2023. Essa convenção foi realizada devido a necessidade de busca de uma política criminal comum para proteção da sociedade contra o crime cibernético, por meio de legislação apropriada e pela promoção da cooperação internacional. O decreto auxilia na determinação dos crimes cibernéticos e ampliam as ferramentas de combate ao crime cibernético, contudo, também transfere para cada nação a forma de agir para com os diferentes crimes.

Este tratado busca harmonizar as leis de diferentes países sobre crimes cibernéticos, facilitando a cooperação internacional no combate a crimes cibernéticos. A convenção trata de crimes como fraude, pornografia infantil, invasão de dispositivos e acesso ilegal a sistemas, e, embora tenha sido aprovado por mais de 60 países, há críticas sobre sua capacidade de adaptação às novas formas de crime digital e a necessidade de atualização constante.

Nos Estados Unidos, a *Computer Fraud and Abuse Act* (CFAA), de 1986, é uma das legislações mais antigas e abrangentes no combate aos crimes cibernéticos, cobrindo uma ampla gama de atividades criminosas, desde invasões de sistemas até fraudes financeiras online. Nos últimos anos, a CFAA foi atualizada para refletir a evolução das ameaças cibernéticas.

Outro exemplo relevante é a Regulamentação Geral de Proteção de Dados da União Europeia (GDPR), renovada em 2018. Embora o GDPR seja primariamente focado na proteção de dados pessoais e privacidade, ele desempenha um papel fundamental no combate a crimes cibernéticos, especialmente ao proteger os

cidadãos europeus contra vazamentos de dados e atividades criminosas associadas à exploração indevida de informações.

Após a Convenção, no Brasil, a legislação sobre crimes cibernéticos começou a se solidificar e fortalecer nas últimas décadas, com marcos importantes. Em 2012, foi o início com a Lei nº 12.737, Lei Carolina Dieckmann, considerada a primeira legislação específica para crimes cibernéticos no Brasil, essa lei é de regulamentação para crimes de invasão de dispositivos, roubo de dados e divulgação de informações privadas sem autorização.

A lei foi criada após um incidente envolvendo o vazamento de fotos pessoais da atriz Carolina Dieckmann, o que gerou grande repercussão pública e acelerou a implementação da legislação. A Lei Carolina Dieckmann tipifica o crime de invasão de dispositivos eletrônicos (computadores, smartphones, entre outros) com o objetivo de obter dados, informações ou causar danos aos sistemas, sendo punível com prisão de 3 meses a 1 ano, além de multa, conforme citado na Lei

“Invasão de dispositivo informático

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.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

- III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
- IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (Brasil, 2012, s.p.).

De acordo com Pinto Junior, Gonçalves e Wermuth (2021, p. 302), a Lei nº 12.737 possui falha pois se o agente dolosamente invadir dispositivo informático sem que haja “violação de mecanismo de segurança, visualize imagens e documentos da vítima, mas não modificar ou destruir nenhum dado, não se encaixa no art. 154-A, será considerado fato atípico, pois não preenche os núcleos do tipo”.

Posteriormente, em 2018, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), trouxe uma série de regulamentações para o tratamento de dados pessoais no Brasil. Embora focada na proteção da privacidade e na prevenção do uso indevido de dados, a LGPD também tem implicações no combate a crimes cibernéticos, especialmente no que tange ao vazamento de informações e ao uso indevido de dados. De acordo com essa Lei, a disciplina da proteção de dados pessoais tem como fundamentos:

- I - O respeito à privacidade;
- II - A autodeterminação informativa;
- III - A liberdade de expressão, de informação, de comunicação e de opinião;
- IV - A inviolabilidade da intimidade, da honra e da imagem;
- V - O desenvolvimento econômico e tecnológico e a inovação;
- VI - A livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018, S.P.).

O artigo Art. 33 da Lei nº 13.709 trata da transferência internacional de dados pessoais somente é permitida nos seguintes casos:

- I - Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
- II - Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
 - a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - Quando a autoridade nacional autorizar a transferência;

VI - Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - Quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei (Brasil, 2018, s.p.).

Em 2014, o Brasil ainda avançou na criação do Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Entre outros pontos, esta lei determina a responsabilidade dos provedores de internet em casos de crimes cometidos por meio de suas plataformas, como a disseminação de conteúdos falsos, discursos de ódio e crimes relacionados a dados pessoais.

O Art. 3º dispõe sobre a disciplina do uso da internet no Brasil, com os seguintes princípios:

I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - Proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação E garantia da neutralidade de rede;

V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Já o Art. 4º trata da disciplina do uso da internet no Brasil, que tem por objetivo a promoção:

I - Do direito de acesso à internet a todos;

II - Do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - Da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - Da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Assim, observa que o acesso a internet é direito do cidadão. Internacionalmente, associado a esse fator, o combate ao crime cibernético apresenta uma variedade de abordagens, dependendo da legislação de cada país e dos acordos multilaterais.

2.3 MÉTODO DE INVESTIGAÇÃO

Conforme já citado anteriormente, a investigação de crimes cibernéticos não é algo fácil de se fazer, e esta condição não é apenas local, mas vista em todo o mundo. Diante desse grande desafio, a resolução 65/230, de 21 de dezembro de 2010, intitulada 12º Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, previa o estabelecimento de um grupo intergovernamental de especialistas com mandato aberto para a troca de informações sobre boas práticas, bem como sobre legislações nacionais e leis internacionais existentes, incluindo o intercâmbio de informações sobre legislação nacional, melhores práticas, assistência

técnica e cooperação, para realizar um estudo abrangente sobre o problema do crime cibernético (United Nations, 2013).

Dessa maneira, o objetivo foi examinar o contexto relacionados as investigações de crime cibernético e propor opções para fortalecer os já existentes e propor novas soluções jurídicas nacionais e internacionais. Nesse encontro, também foi solicitado uma intensificação dos esforços para concluir esse trabalho e apresentar o resultado do estudo à Comissão de Prevenção do Crime e Justiça Criminal. A primeira sessão desse grupo especializado de peritos ocorreu teve em Viena, em 2011, do qual foram determinados alguns tópicos e metodologia para o estudo (United Nations, 2013).

De acordo com o United Nations (2013), independentemente da forma jurídica dos poderes de investigação, todos os países utilizam busca e apreensão para apropriação física de equipamentos de informática e captura de dados de computador.

A maioria dos países também utiliza ordens para obter dados informáticos a partir da Internet, provedores de serviços, coleta de dados em tempo real e preservação acelerada de dados. Porém, as autoridades responsáveis pela aplicação da lei enfrentam uma série de desafios na prática, incluindo técnicas do perpetrador para ocultar ou excluir dados de computador relacionados a um crime.

O dia 8 de agosto de 2024, a ONU aprovou a proposta que poderá reforçar o enfrentamento aos crimes cibernéticos. Dentre as medidas previstas está a criação de um canal global de pedidos de assistência mútua entre os países. Essa medida foi instaurada levando em consideração também que muitos crimes cibernéticos podem atuar a nível internacional, como tráfico de pessoas, contrabando de migrantes, pedofilia, estelionato e lavagem de dinheiro utilizam diversas tecnologias e a internet. O ciber crime ultrapassa as fronteiras geográficas dos países e essa convenção vai contribuir para a cooperação e a colaboração entre os países no seu enfrentamento”, avalia o secretário Nacional de Justiça, Jean Keiji Uema.

O novo instrumento deverá servir também como base normativa aos países que não têm legislação nacional. O texto aprovado alerta que as nações estão preocupadas com a utilização de sistemas de tecnologias de informação e comunicação pelos criminosos e que isso impacta na rapidez de práticas de crimes como: organizado transnacional, terrorismo, contrabando de migrantes, produção

ilícita armas de fogo, peças e munições e tráfico de pessoas, de drogas e de bens culturais.

A proposta de convenção contra crimes cibernéticos inclui recursos para “aprimorar a cooperação internacional, os esforços de aplicação da lei, a assistência técnica e a capacitação” para o enfrentamento dos delitos. O texto da Convenção da ONU contra Crimes Cibernéticos, aprovado em 8 de agosto, está em consonância com o processo de adesão do Brasil à Convenção de Budapeste sobre Crimes Cibernéticos do Conselho da Europa, aprovada pelo Congresso Nacional por meio do Decreto Legislativo nº 37/2021, e promulgada pelo Decreto nº 11.491/2023.

O Decreto nº 11.491/2023, embora tomou como base à Convenção de Budapeste sobre Crimes Cibernéticos, foram elaboradas medidas a serem adotadas nas jurisdições nacionais, do qual descreve que cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas, conforme os crimes, que é composto por cinco títulos, como segue,

O Título 1 se refere aos crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador, composto pelos artigos 2 ao 6.

Artigo 2 - Acesso ilegal

Artigo 3 - Interceptação ilícita

Artigo 4 - Violação de dados

Artigo 5 - Interferência em sistema

Artigo 6 - Uso indevido de aparelhagem

a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:

i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;

ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e

b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize (Brasil, 2023).

O Título 2 aborda sobre os crimes informáticos

Artigo 7 - Falsificação informática

Artigo 8 - Fraude informática

- a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;
- b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita.

O Título 3 descreve sobre os crimes relacionados ao conteúdo da informação

Artigo 9 - Pornografia infantil

- a. produzir pornografia infantil para distribuição por meio de um sistema de computador;
 - b. oferecer ou disponibilizar pornografia infantil por meio de um sistema de computador;
 - c. distribuir ou transmitir pornografia infantil por meio de um sistema de computador;
 - d. adquirir, para si ou para outrem, pornografia infantil por meio de um sistema de computador;
 - e. possuir pornografia infantil num sistema de computador ou num dispositivo de armazenamento de dados de computador.
2. Para os fins do parágrafo 1, “pornografia infantil” inclui material pornográfico que represente visualmente:
- a. um menor envolvido em conduta sexual explícita;
 - b. uma pessoa que pareça menor envolvida em conduta sexual explícita;
 - c. imagens realísticas retratando um menor envolvido em conduta sexual explícita.
3. Para os fins do parágrafo 2, o termo “menor” inclui todas as pessoas com menos de 18 anos de idade. Qualquer Parte pode, contudo, estabelecer um limite de idade diverso, que não será inferior a 16 anos.
4. Qualquer Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o parágrafo 1, subparágrafos d e e, e o parágrafo 2, subparágrafos b e c.

O Título 4 aborda sobre a violação de direitos autorais e de direitos correlatos

Artigo 10 - Violação de direitos autorais e de direitos correlatos

E por fim, o Título 5 relata outras formas de responsabilidade e sanções, apresentado os três últimos artigos.

Artigo 11 - Tentativa, auxílio ou instigação

Artigo 12 - Responsabilidade penal da pessoa jurídica

- a. no poder de representação da pessoa jurídica;
- b. na autoridade de tomar decisões em nome da pessoa jurídica;
- c. na autoridade de exercer controle interno na pessoa jurídica.

Artigo 13 - Sanções e medidas

O crime cibernético geralmente inclui atividades criminosas que visam um computador ou rede para causar danos ou roubar informações. Inclui também a utilização de computadores para realizar atividades criminosas, como a utilização da Internet para facilitar a venda ou troca de bens ilícitos, como drogas ou armas ilegais. A própria natureza dos crimes cibernéticos torna-os difíceis de rastrear e, por vezes, difíceis de serem detectadas. Através da Internet, os criminosos cibernéticos podem permanecer anônimos. Eles não precisam estar fisicamente próximos de suas vítimas para cometer um crime (Government Accountability Office U.S., 2023).

As informações fornecidas pelas vítimas de crimes são importantes para rastrear e combater os crimes cibernético. Mas algumas vítimas hesitam em se manifestar porque não sabem a quem denunciar um ataque ou o que pode ser feito a respeito. Da mesma forma, algumas empresas também podem não denunciar os crimes para proteger a sua reputação (Government Accountability Office U.S., 2023).

Mesmo quando as autoridades federais recebem informações sobre crimes, enfrentam algumas limitações internas que as impedem de utilizar plenamente essas informações para combater atividades. Por exemplo, as agências federais de aplicação da lei não definem o crime cibernético da mesma forma. O que é considerado crime cibernético em uma agência pode não ser definido como tal em outra. Isto tem impacto na capacidade de cada agência partilhar informações importantes e coordenar esforços. As agências federais também utilizam uma variedade de mecanismos para recolher e relatar a extensão e o impacto do crime

cibernético, tais como portais web para recolher reclamações do público ou relatórios de incidentes cibernéticos (Government Accountability Office U.S., 2023).

No Brasil, existem algumas leis que são ineficientes para combater o crime cibernético, como as Leis 12.735/2012 (Brasil, 2012a), 12.737/2012 (Brasil, 2012b), e 12.965/2014 (Brasil, 2014), isso porque existe uma dificuldade taxativa do Código Penal brasileiro, gerando uma dificuldade de aplicação da analogia aos crimes cibernéticos. As leis de 2012 foram promulgadas por causa da pressão da mídia sobre o legislativo, em detrimento de pedido de justiça por fotos íntimas da atriz Carolina Dieckmann, que foram divulgadas na internet. Na época, os infratores foram localizados e indiciados (Cruz; Rodrigues, 2018).

A Lei 12.737/2012 criminaliza a invasão de dispositivos informáticos, como celulares, tablets e notebooks. Essa lei foi aprovada em um tempo relativamente curto, em menos de dois anos após o computador da atriz ser invadido e suas fotos roubadas. A Lei estabelece princípios, garantias e deveres para o uso da internet no Brasil. Ela também alterou o Código Penal, inserindo o crime de invasão de dispositivo informático no artigo 154-A (Brasil, 2012a).

A pena para a invasão de dispositivos informáticos é de detenção de 3 meses a 1 ano e multa. A pena aumenta se o crime resultar em prejuízos econômicos para a vítima, ou se o conteúdo obtido for de comunicações privadas, segredos comerciais ou industriais.

Outra lei que protege os dados pessoais e a privacidade dos usuários é o Marco Civil da Internet (Lei 12.965/2014). Essa Lei n. 12.965/2014 estabeleceu novos princípios, garantias, direitos e deveres para o uso da internet, para os usuários e para o Estado.

O Art. 7º da Lei 12.965/2014, relata sobre os direitos dos usuário da internet:

- I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
- II - inviolabilidade E sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
- III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
- IV - Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
- V - Manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais.

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Essa lei veio para complementar as Leis de 2012. Porém, após a sua promulgação, ainda foram observadas lacunas para a sua aplicação nos casos concretos.

Em 2018, foi aprovada a Lei n. 13.709, dispondo sobre o tratamento de dados pessoais de usuários por empresas públicas e privadas, garantindo proteção jurídica sobre os dados dos cidadãos. Nessa Lei também foram esclarecidos o que e quais são os dados pessoais, banco de dados, titular dos dados, agentes de tratamento dos dados, sendo essa definição necessária para a aplicação da lei (Brasil, 2018).

I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - Agentes de tratamento: o controlador e o operador;

X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; Vigência

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Ainda de acordo com a Lei n. 13.709, Art. 7º, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - Mediante o fornecimento de consentimento pelo titular;

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (Redação dada pela Lei nº 13.853, de 2019)
Vigência

IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Portanto, não existe uma legislação específica para o crime cibernético no Brasil, o que leva as autoridades a julgarem como algum tipo de crime já existente na legislação, como: Pedofilia; Interceptação de comunicações de informática; Pirataria, Calúnia, Difamação, Injúria e Ameaça. Contudo, com essas vastas opções de crimes, as autoridades não direcionam eficientemente seus recursos para combater os crimes cibernéticos (Cruz; Rodrigues, 2018).

Porém, existem crimes cibernéticos que vão além das fronteiras e podem trazer prejuízos catastróficos para os afetados. Nesse caso, existe a necessidade de investigação envolvendo profissionais qualificados de agências como FBI, NSA, Serviço Secreto e outros. Estas agências utilizam análise forense digital para rastrear, analisar e dismantelar tipos de crimes cibernéticos e ameaças cibernéticas (Pinheiro, 2013). A ação dessas agências requer uma colaboração público-privada e cooperação internacional para superar desafios como questões jurisdicionais e a evolução contínua da tecnologia utilizada pelos criminosos cibernéticos (Borges, 2024).

Nesse sentido, as estratégias de prevenção e resposta são essenciais para mitigar os riscos de crimes cibernéticos, incluindo a implementação de medidas de segurança, como o desenvolvimento de planos de resposta a incidentes, a educação das partes interessadas e a manutenção de plataformas robustas de denúncia de crimes cibernéticos, como o IC3 (Internet Crime Complaint Center).

De acordo com Borges (2024) as investigações dos crimes cibernéticos se inicia com uma avaliação completa das circunstâncias, identificando possíveis evidências e protegendo os dispositivos relevantes. Ordens legais podem ser obtidas para facilitar a investigação e obter informações adicionais. Estas etapas são fundamentais para identificar e processar criminosos cibernéticos transnacionais responsáveis por vários crimes cibernéticos.

Assim, as investigações de crime cibernéticos são constituídas de: Identificação, análise e rastreamento de evidências digitais para descobrir os

perpetradores e seus motivos (Wendt; Jorge, 2013). Esse processo envolve algumas ações, como? Conhecer o caso e avaliar a situação; Conduzir a investigação inicial; Identificar as potenciais evidências; Apreender e proteger dispositivos; Obtenção de ordens judiciais; Análise de resultados junto ao Ministério Público. A investigação emprega técnicas investigativas tradicionais, planejamento meticuloso, coleta de informações, processamento de evidências e manuseio adequado de evidências digitais.

As evidências eletrônicas são de fundamental importância para as investigações, pois podem conter informações e dados de valor investigativo que são armazenados ou transmitidos por um dispositivo eletrônico. Visam identificar a origem do crime, recolher provas e apresentá-las de uma forma adequada aos procedimentos judiciais para processar o autor do crime. A complexidade dos crimes cibernéticos, tal como o grande número e as jurisdições internacionais envolvidas, exige técnicas e ferramentas especializadas para a recolha e análise de provas (Wendt; Jorge, 2013).

Borges (2024) afirma que a investigação é como montar um quebra-cabeça complexo, exigindo atenção meticulosa aos detalhes e habilidade analítica. O processo também envolve o uso de ferramentas e técnicas específicas. A perícia digital desempenha um papel crucial nas investigações de crimes cibernéticos, coletando, preservando e analisando evidências digitais. Os métodos usados para identificar software malicioso envolvem ferramentas de detecção de malware, como software antivírus, sistemas de detecção de invasões e ambientes sandbox para análise dinâmica de malware.

Contudo, Borges (2024) também relata que as investigações cibernéticas envolvem múltiplos desafios, como as questões jurisdicionais, pois determinam a autoridade para investigar e processar o crime com base na localização dos infratores, das vítimas e dos impactos do crime cibernético. Além disso, a natureza global dos crimes cibernéticos exige cooperação internacional, o que coloca dificuldades na identificação de suspeitos, na garantia da extradição e na escolha de uma jurisdição apropriada.

Outro desafio citado por Borges (2024) é a rápida evolução da tecnologia. À medida que a tecnologia evolui, também evoluem as táticas e ferramentas utilizadas pelos criminosos cibernéticos. Isto exige que os investigadores se mantenham a par dos novos desenvolvimentos tecnológicos e ajustem as suas técnicas de

investigação em conformidade. Assim, estes profissionais devem estar em constantes aprimoramento e atualizados, no que se refere às tecnologias.

Combater o crime cibernético não é um esforço individual é realizado em equipe, com cada parte interessada trazendo habilidades e perspectivas únicas para se desvendar o crime. Estas parcerias contribuem para o desenvolvimento de legislação alinhada com as normas internacionais. Apesar dos potenciais conflitos setoriais e das capacidades limitadas das agências responsáveis pela aplicação da lei, estas colaborações provaram ser uma estratégia eficaz no combate do crime cibernético (Phillips, 2022).

No que se refere as ferramentas e técnicas utilizadas na investigação do crime cibernético. Borges (2024) aponta a análise forense digital, que envolve a coleta, preservação e análise de evidências digitais, rastreamento de software malicioso e analisando transações financeiras. Cada ferramenta e técnica desempenha um papel crucial na descoberta dos crimes cibernéticos. As ferramentas ajudam os investigadores a identificar, analisar e recuperar dados forenses que podem servir como evidência digital de um crime.

A análise forense digital é como a análise de DNA do mundo cibernético, desempenhando um papel fundamental na investigação de crimes cibernéticos, na prevenção de violações de dados e na ajuda às autoridades policiais na localização dos perpetradores. Envolve a identificação, preservação, análise e documentação de provas digitais para uso em tribunal (Borges, 2024).

Dados eletrônicos como documentos de computador, e-mails, mensagens de texto e instantâneas, transações, imagens e históricos de internet dos dispositivos envolvidos no crime são coletados como parte de evidências digitais. Preservar essas evidências envolve proteger o estado atual do dispositivo, desligá-lo adequadamente e duplicar todos os dispositivos de armazenamento de dados pertinentes para manter a integridade das evidências (Borges, 2024).

O rastreamento de software malicioso, ou *malware*, é uma técnica fundamental nas investigações de crimes cibernéticos. Ajuda a identificar a origem e distribuição de *malware*, auxiliando na identificação e repressão de criminosos cibernéticos. A análise de transações financeiras nas investigações de crimes cibernéticos é outra ferramenta vital. Abrange a identificação de atividades cibernéticas fraudulentas, que envolve perdas financeiras e o uso de diversas ferramentas e métodos para analisar transações financeiras suspeitas. Diversas

metodologias são empregadas para esse tipo de análise, como análise forense, técnicas de monitoramento de transações, análise de rede, aprendizado de máquina e mineração de dados. As transações financeiras examinadas nas investigações de crimes cibernéticos abrangem o tráfico de dados financeiros roubados, a lavagem de dinheiro e outros crimes cibernéticos relacionados (Cruz; Rodrigues, 2018).

De acordo com Borges (2024) a análise de transações financeiras é utilizada para rastrear criminosos cibernéticos por meio de várias técnicas, incluindo rastreamento de transações *Bitcoin*, emprego de técnicas supervisionadas com modelos de previsão de fraude, revisão e análise de transações financeiras para identificar possíveis fraudes, aproveitamento de ferramentas analíticas de *blockchain* para investigação e condução de análise forense de criptomoedas no *blockchain*. Vale ressaltar que o setor de serviços financeiros é o principal alvo de atores mal-intencionados que realizam os crimes cibernéticos.

Uma outra questão importante sobre os crimes cibernéticos, é que a maioria das pessoas não sabem o que fazer caso sejam vítimas desse crime. Correia, Terron e Correa (2020) relatam os procedimentos que devem ser realizados em casos de serem vítimas de crime cibernético. A princípio deve-se identificar qual a modalidade de crime ocorreu. Quando envolver um provedor, esse deverá ser notificado. Dessa maneira, a empresa é obrigada a retirar a ofensa e/ou obter os dados da ação do criminoso, identificando o número de IP utilizado, a fim de identificá-lo.

Destaca-se que é essencial preservar s todas as provas, como as conversas que foram realizadas em aplicativos de comunicação, mensagens de correio eletrônico, conteúdos de páginas, dentre outros. Para se formalizar a denúncia, é preciso se dirigir a uma delegacia, após este procedimento, a Polícia Civil aplicará todos os recursos de Polícia Judiciária viáveis ao caso. Geralmente existe a indicação de ter auxílio de um advogado, pois muitos dos delitos eletrônicos podem ser requeridos indenização.

2.4 MÉTODOS DE PREVENÇÃO

Conforme já citado acima, os crimes cibernéticos podem trazer sérios prejuízos para as vítimas, não somente financeiros, mas danos morais, sociais, políticos, dentre outros. Assim a melhor forma de evitar esses danos é se prevenir.

Existem estratégias que podem ser empregadas para prevenir e responder ao crime cibernético. Isso inclui a implementação de medidas de segurança, o desenvolvimento de um plano de resposta a incidentes e a educação das partes interessadas.

No Brasil, existem algumas políticas públicas voltadas para prevenção dos crimes cibernéticos, como a Estratégia Nacional de Segurança Cibernética – E-Ciber. A elaboração desse documento foi realizada com a cooperação de órgãos e entidades

governamentais, instituições privadas e o setor acadêmico. Foram definidos objetivos e ações para tratar questões relacionadas a segurança cibernética no país. Dentre os pontos abordados estão o de tornar o ambiente virtual do Brasil mais confiável, ampliar a resistência à ameaças cibernéticas, fortalecer a atuação do país em segurança cibernética internacional e realizar investimentos na educação dos usuários (Brasil, 2019).

Além das ações promovidas por entidades, Borges (2024) ressaltam que o próprio cidadão pode adotar medidas de segurança e melhores práticas para evitar os crimes cibernéticos, dentre as medidas recomendadas pelo autor, cita-se: habilitando a autenticação multifatorial; atualizando o software regularmente, ter cuidado ao clicar em links ou baixar anexos, monitorar o tráfego de rede e as atividades do usuário utilizando firewalls, implementando mecanismos de controle de acesso, empregando criptografia, fornecendo treinamento de segurança para funcionários, protegendo informações, computadores e redes contra ataques cibernéticos, usando gerenciadores de senhas, ser cauteloso com e-mails suspeitos, restringindo o acesso a dados críticos, fazendo backup de dados regularmente.

De acordo com o citado acima, existem diferentes maneiras para os usuários de tecnologias se protejam contra os crimes cibernéticos. No entanto, há a necessidade de investimento em treinamentos desses usuários, tendo em vista que muitos deles não têm conhecimento suficiente para entender o que são e como realizar as ações citadas acima.

Borges (2024) ressalta que a educação é uma ferramenta poderosa na luta contra o crime cibernético. O autor descreve algumas razões pelas quais é essencial educar as partes interessadas, como funcionários e consumidores, sobre ameaças cibernéticas e estratégias de prevenção:

- Reduz o risco de crimes cibernéticos ao capacitar os indivíduos a tomar decisões informadas e a tomar medidas proativas para proteger a si próprios e à organização.

- Ajuda a reduzir o erro humano, que muitas vezes é um fator importante nos ataques cibernéticos.

- Melhora a resiliência cibernética geral, criando uma cultura de consciência e vigilância em matéria de segurança.

- Ao investir na educação e formação em inteligência contra ameaças, as organizações podem melhorar significativamente a sua capacidade de prevenir e responder a ameaças cibernéticas.

Correia, Terron e Correa (2020) frisam que para as pessoas que se utilizam de tecnologias, é essencial o uso de antivírus, pois ele é a ferramenta primária na prevenção e segurança da informação. A instalação do antivírus pode ser realizada em aparelhos celulares, em computadores, dentre outros. Esse programa pode detectar vírus e até mesmo ligações indesejadas. Porém, vale ressaltar que é importante manter o antivírus atualizado, pois novos vírus são lançados a todo momento.

Nessa mesma linha de raciocínio, devido a inovação constante e a inserção de novas ferramentas no crime cibernético, é indispensável que haja atualização constante por parte dos profissionais que atuam nessa área, tanto para combater, bem como para promover novas estratégias de prevenção.

3 CONCLUSÃO

Nessa revisão foi abordado sobre os crimes cibernético e os processos que envolve a investigação e a prevenção para não ser vítima de crimes cibernético. Verificou-se que ainda faltam leis específicas para julgarem casos dessa natureza, e um empenho internacional é importante para atuarem contra esse crime, tendo em vista, que não existe limites geográficos para a atuação dos ciber criminoso.

Conforme identificado nesta revisão, as abordagens sobre crime cibernético são fragmentadas e falhas, e esse fator não apenas no Brasil, mas por se tratar de um tema de interesse mundial, essa falta de definição do termo é global. Portanto, uma recomendação fundamental para trabalhos futuros é desenvolver um sistema de classificação sistemático, objetivo e holístico, que seja baseado em evidências, flexível, prontamente atualizado, apoiado por uma iniciativa de pesquisa dedicada e que incorpore contribuições multidisciplinares e cooperação internacional.

Além disso, é necessária maior transparência para justificar as decisões que sustentam o desenvolvimento de sistemas de classificação de crimes cibernéticos, para avaliar e atualizar significativamente os quadros estabelecidos e para ter em conta os principais desafios. Nesse sentido, vale ressaltar que o tema ainda continua em debate e sendo pauta de reuniões promovidas com a participação de todos os países, como a recentemente realizada pela ONU, das quais trouxe importantes diretrizes para o tema.

Diante da complexidade judicial do crime cibernético, o melhor caminho é a prevenção. Quando se utiliza de aparelhos como celulares, computadores, tablets, dentre outros uma das indicações é a utilização de antivírus e este deve ser constantemente atualizado, tendo em vista os ataques cibernéticos se inovam a cada dia. Porém, os meios de prevenção devem ser melhores divulgados para a população, tendo em vista que muitos usuários não têm acesso as informações de como se prevenirem desse crime

Nesse sentido, um outro fator importante na prevenção é a educação da população, porque muitos desses criminosos se utilizam da falta de conhecimento das pessoas para dar golpes por meio da internet, principalmente golpes financeiros.

Assim, é recomendável que as autoridades governamentais invistam em treinamentos e até mesmo na educação da população de maneira a promover uma ação preventiva quanto aos crimes cibernético.

REFERÊNCIAS

ASSUNÇÃO, M. F. A. **O Guia do Hacker Brasileiro**. Editora: Visual books, 1 de janeiro de 2002.

BLACK, A.; LUMSDEN, K.; HADLINGTON, L. 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim when Responding to Reports of Interpersonal Cybercrime. In; Lumsden, K.; Harmer, E. (Eds.). **Exploring violence and discrimination on the web**. Basingstoke, UK: Palgrave Macmillan, 2019. p. 355–378.

BORGES, E. **Essentials of cyber crime investigation**. Disponível em: <https://www.recordedfuture.com/threat-intelligence-101/incident-response-management/cyber-crime-investigation>. Acesso em: 10 abr. 2024.

BRASIL. **Decreto Nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 10 abr. 2024.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 de abr. 2024.

_____. **Lei nº 12.735, de 30 de novembro de 2012**. 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 10 abr. 2024.

_____. **Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckman)**. 2012b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2012/lei/l12737.htm. Acesso em: 10 abr. 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2024.

_____. **Lei 13.853, de 8 de julho de 2019**. Altera a Lei de Proteção de Dados; e dá outras providências. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 08 abr. 2024.

_____. **ONU aprova proposta que poderá reforçar o enfrentamento a crimes cibernéticos**. Gov.br, 2024. Disponível em: <https://www.google.com/search?q=onu+aprova+proposta+que+poder%C3%A1+crimes+ciber%C3%A9ticos&oq=onu+aprova+proposta+que+poder%C3%A1+crimes+cib>

er%C3%A9ticos&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQIRgKGKAB0gEJMT
EzMzlqMGo0qAlAsAIA&sourceid=chrome&ie=UTF-8. Acesso em: 11 out. 2024.

CASTELLS, M. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. 1. ed. Rio de Janeiro: Jorge Zahar, 2003.

CORREIA, T. M.; TERRON, L. L. S.; CORREA, R. A. Cibercrimes: aspectos panorâmicos dos crimes informáticos mais praticados e as condutas de prevenção. **E-Civitas**, v. 13, n. 1, p. 119-135, 2020.

CRUZ, D.; RODRIGUES, J. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, v. 13, p. 1-18, 2018.

FAHEEM, M. et al. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. **Computer Science Review**, v. 30, p. 1-30, 2018.

GOVERNMENT ACCOUNTABILITY OFFICE U.S. **The U.S. is less prepared to fight cybercrime than it could be**. 2023. Disponível em: <https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be>. Acesso em: 101 abr. 2024.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. 2017. 111 f. Trabalho de Conclusão de Curso (graduação em Direito) – Universidade Federal do Ceará, Faculdade de Direito, Fortaleza, 2017.

MENEZES NETO, E J.; MORAIS, J. L. B. A fragilização do estado-nação na proteção dos direitos humanos violados pelas tecnologias da informação e comunicação. **Revista Direitos Fundamentais & Democracia**, v. 23, n. 3, p. 231-257, 2018.

NADER, P. **Introdução ao Estudo do Direito**. 24. ed. Rio de Janeiro: Forense, 2004.

PÁDUA, T. P.; DE OLIVEIRA FRAZÃO, C. G. X.; ASSUNÇÃO, R. A. L. A Revolução tecnológica e os delitos digitais: uma análise da (in) suficiência legislativa brasileira. **Revista de Criminologias e Políticas Criminais**, v. 7, n. 2, p. 23-38, 2022.

PHILLIPS, K. et al. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. **Forensic Science**, v. 2, p. 379–398, 2022.

PINHEIRO, P. P. **Direito digital**. 5. ed. rev., atual. e ampl. São Paulo: Saraiva, 2013.

PINTO JUNIOR, A. O.; RIBEIRO, L. G. G.; WERMUTH, M. A. D. **Direito penal, processo penal e constituição II**. Florianópolis: CONPEDI, 2021. Disponível em: <http://site.conpedi.org.br/publicacoes/7x02k736/x477p663/p4IKh1B9SScT53NP.pdf>. Acesso em: 13 nov. 2024.

REALE, M. **Lições preliminares de direito**. 27. ed. São Paulo: Saraiva, 2002.

ROSA, A. M. A questão digital: o impacto da inteligência artificial no Direito. **Revista de Direito da Faculdade Guanambi**, v. 6, n. 2, p. 1-18, 2019.

SANTOS, C. COVID-19 e saúde mental dos adolescentes: Vulnerabilidades associadas ao uso de Internet e mídias sociais. **Holos**, v. 3, p. 1-14, 2021.

UNITED NATIONS. **Comprehensive Study on Cybercrime Draft**. New York: United Nations, 2013.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 2. Ed.. Brasport, 2013.

YAR, M.; STEINMETZ, K. F. **Cybercrime and Society**. 3. ed. London, UK: SAGE Publications Ltd, 2019.