CENTRO UNIVERSITÁRIO UNDB
CURSO DE DIREITO

**DICKSON CARVALHO GONÇALVES DA SILVA**

# **CRIMES CIBERNÉTICOS:** LIMITES E DESAFIOS DA INVESTIGAÇÃO

São Luís
2022

**DICKSON CARVALHO GONÇALVES DA SILVA**

# **CRIMES CIBERNÉTICOS:** LIMITES E DESAFIOS DA INVESTIGAÇÃO

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientador(a): Prof. Me. Mari-Silva Maia da Silva

São Luís

2022

Dados Internacionais de Catalogação na Publicação (CIP)

Centro Universitário – UNDB / Biblioteca

Silva, Dickson Carvalho Gonçalves da

Crimes cibernéticos: limites e desafios da investigação. / Dickson Carvalho Gonçalves da Silva. __ São Luís, 2022.

68 f.

Orientador: Profa. Me. Mari-Silva Maia da Silva.

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2022.

1. Crimes cibernéticos. 2. Investigação criminal. 3. Convenção de Budapeste. I. Título.

CDU 343.4:007

**DICKSON CARVALHO GONÇALVES DA SILVA**

# **CRIMES CIBERNÉTICOS:** LIMITES E DESAFIOS DA INVESTIGAÇÃO

Monografia apresentado ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientador: Prof. Me. Mari-Silva Maia da Silva

Aprovado em: 23/06/2022

BANCA EXAMINADAORA

_____

**Profa. Me. Mari-Silva Maia da Silva** (Orientadora)

UNDB

_____

**Adv. Esp. Mariana Weba Lobato Vaz** (Examinadora)

UNDB

_____

**Prof. Me. José Murilo Duailibe Salém Neto** (Examinador)

UNDB

## AGRADECIMENTOS

Aos meus pais, pelo amor, incentivo e apoio incondicional.

A minha orientadora, Mari-Silva Maia, pela paciência, confiança e apoio durante todo o tempo.

Agradeço ainda, aos meus amigos, Dayana, Hellen, Gabriele, Simone, Ellen Rose, Cláudio, Thaynara, Israel, Maria Eduarda, Corina, Marcos, Julyanna, Larissa, Raquel, Amanda, Giulia, Mateus, Onna e Vitória, por toda a ajuda durante o percurso acadêmico.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

## RESUMO

Os crimes cibernéticos se multiplicam a cada instante, sendo necessária, na mesma proporção, a sua devida investigação e combate. O presente estudo busca apresentar a importância de se entender o processo de investigação e suas dificuldades, Primeiramente, foi realizado um breve relato histórico dos crimes cibernéticos da sua origem, principais tipos e o processo realizado durante a investigação, sendo demonstrada em seguida, como objetivo central, as principais dificuldades encontradas durante as investigações dos crimes cibernéticos, como o uso do Mutual legal assistance treaty (MLAT) para obter informações localizadas em servidores estrangeiros, o acesso aos dados cadastrais, registros de acessos, o uso de criptomoedas, a dificuldade de apreensão nesses crimes e por fim, serão apresentadas algumas mecanismos que podem solucionar as dificuldades encontradas, como a Convenção de Budapeste, cooperação internacional e a melhor integração entre os órgãos policiais. A questão demanda um olhar mais focado, visto que o crime cometido nas redes não atinge um único sujeito passivo, mas se reveste em crime que termina por atingir toda a sociedade, deixando, ainda, a falsa sensação de que o crime realmente compensa. A pesquisa foi realizada através de uma pesquisa bibliográfica, com o intuito de buscar na literatura, as bases necessárias para o melhor desenvolver da linha de raciocínio escolhida. Neste sentido, relacionou-se as informações sobre o tema encontradas em livros, artigos, periódicos, através do método exploratório e dedutivo. Tais informações permitiram que se fizesse possível o melhor entender da questão-problema levantada no interior.



**Palavras-chave:** Crimes Cibernéticos. Investigação Criminal. Convenção de Budapeste.

## ABSTRACT

Cybercrimes are multiplying at every moment, requiring, in the same proportion, their due investigation and combat. The present study seeks to present the importance of understanding the investigation process and its difficulties, in the current conjuncture of internet globalization. Firstly, a brief historical account of cybercrimes was carried out, its origin, main types and the process carried out during the investigation, being then demonstrated the main difficulties encountered during cybercrimes investigations. such as the use of the Mutual legal assistance treaty (MLAT) to obtain information located on foreign servers, access to registration data, access records, etc., and finally, some tools will be presented that can solve the difficulties encountered, such as the Budapest Convention. The issue demands a more focused look, since the crime committed in the networks does not affect a single person, but it is a crime that ends up reaching the whole society, leaving, still, the false sensation that crime really pays. The research was carried out through a bibliographical research, in order to search in the literature, the necessary bases for the best development of the chosen line of reasoning. In this sense, the information on the topic found in books, articles, periodicals, etc. Such information made it possible to better understand the problem-question.



**Key-words:** Cyber Crimes. Criminal investigation. Budapest Convention.

## LISTA DE SIGLAS

| | |
|---|---|
| Ameripol | Comunidade de Polícias das Américas |
| CERT no Brasil | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança |
| CGI.br | Comitê Gestor da Internet no Brasil |
| ECA | Estatuto da Criança e do Adolescente |
| Europol | Agência da União Europeia para a Cooperação Policial |
| Interpol | Organização Internacional de Polícia Criminal |
| IP | Internet Protocol |
| IPv4 | Internet Protocol versão 4 |
| IPv6 | Internet Protocol versão 6 |
| MLAT | Mutual Legal Assistance Treaty |

**SÚMARIO**

# 1 INTRODUÇÃO

Com o desenvolvimento da tecnologia, as pessoas estão cada vez mais conectadas através da internet ao mundo, tornando-as mais vulneráveis aos crimes cibernéticos que representam o futuro de uma nova modalidade de crimes praticados pelos meios eletrônicos, e que aumenta o alcance dos demais crimes antes restritos a um pequeno grupo de pessoas.

Não obstante de ocorrerem no mundo virtual, os crimes virtuais costumam causar danos de forma muito mais ampla na sociedade, uma calúnia publicada por meio de uma rede social, acessível mundialmente, possui muito mais alcance do que se proferida pessoalmente, ou o roubo de dados bancários que pode atingir milhares de vítimas, que necessitam da devida proteção.

Diante da fragilidade dos mecanismos existentes para a proteção, os criminosos se aproveitaram e se multiplicaram, cometendo cada vez mais crimes cibernéticos, utilizando da falsa sensação de anonimato e impunidade no ambiente virtual, dessa forma, sempre buscando novas formas de obter lucro, ou de atingir outras pessoas.

A investigação de Crimes Cibernéticos, é a única forma de encontrar e responsabilizar os indivíduos responsáveis pela prática desses crimes, porém, há diversas dificuldades nesse processo, entre eles, a falta de cooperação internacional, empresas internacionais que atuam no Brasil que se recusam em fornecer as informações solicitadas, a identificação do responsável pelo IP (Internet Protocol), entre outros motivos. (BRAIDA, 2020)

Para a execução metodológica do trabalho, utilizou-se a modalidade de pesquisa bibliográfica com o intuito de buscar na literatura, as bases necessárias para o melhor desenvolver da linha de raciocínio escolhida para a apresentação da monografia. Neste sentido, relacionou-se as informações sobre o tema encontradas em livros, trabalhos científicos, artigos, periódicos etc. Tais informações permitiram que se fizesse possível o melhor entender da questão-problema levantada no interior deste trabalho.

A justificativa acadêmica, desse projeto tem como base que os crimes cibernéticos são fenômenos poucos discutidos, podendo ser constatado através da insuficiência de artigos acadêmicos em comparação a outros temas do direito, demostrando ser um tema que merece destaque no meio acadêmico, justamente por

abranger uma nova área de conhecimento do direito que se relaciona com outros ramos de estudo. Sendo o seu debate em meio acadêmico algo essencial para que o ordenamento jurídico se mantenha atualizado e informado com as mudanças que vem surgindo.

Esse tema é importante de ser abordado devido ao impacto que o fenômeno dos crimes cibernéticos possui na sociedade, ou seja, sua grande relevância num contexto social que influencia na vida das pessoas, levando-se em consideração que esse tipo de acontecimento está sujeito a acontecer com qualquer pessoa.

Diante deste cenário, este trabalho tem como objetivo central apresentar questões que se relacionam diretamente com a investigação dos crimes cibernéticos, como o contexto histórico, o processo realizado durante a investigação para a identificação da autoria dos responsáveis por esses crimes, bem como os principais desafios encontrados na investigação, além de mecanismos utilizados no enfrentamento dessas dificuldades.

A estrutura dessa pesquisa foi estruturada em três capítulos, que trazem um panorama geral da investigação de crimes cibernéticos, no primeiro capítulo, apresenta-se um panorama acerca da origem dos crimes cibernéticos, suas principais formas e o processo de investigação que é realizada para identificar a autoria, demonstrando que que o crime cibernético tem um longa caminho a ser realizado na obtenção de provas.

No segundo capítulo, serão apresentadas as dificuldades encontradas durante a investigação dos crimes cibernéticos, principalmente, em relação ao uso do Mutual legal assistance treaty (MLAT), o acesso aos dados cadastrais e registros de acesso, que contém o endereço de IP, informação essencial em uma investigação para identificar os responsáveis pelos crimes cibernéticos, além das dificuldades devido ao uso de criptomoedas que se tornaram mais comuns.

No terceiro capítulo, serão apresentadas mecanismos e possíveis soluções para diminuir as dificuldades encontradas durante a investigação, tais como a Convenção de Budapeste, a prevenção através da educação digital, bem com os investimentos na capacitação e de integração entre os órgãos de investigação.

# 2 CRIMES CIBERNÉTICOS: PANORAMA DA ORIGEM À INVESTIGAÇÃO

A proposta deste capítulo é de apresentar um breve relato sobre a origem e o histórico dos crimes cibernéticos, através do surgimento da Internet, as facilidades criadas decorrentes da popularização da Internet, que são utilizadas pelos cibercriminosos, bem com as principais legislações sobre o tema, além do crescimento e migração de crimes tradicionais para o meio cibernético, nesse sentido, serão apresentadas ainda os principais tipos de crimes cibernéticos e suas características, como a pornografia infantil, cyberstalking, e etc.

Além disso, será apresentado todo o processo realizado para identificação da autoria dos responsáveis pelos crimes cibernéticos, primeiramente, por meio de uma apresentação dos conceitos fundamentais para compreensão do processo de investigação, as fases que são realizadas para obtenção das provas, e consequentemente, as formas utilizadas para garantir a preservação das evidências encontradas.

## 2.1 Origem e histórico dos crimes cibernéticos

Com o surgimento da internet que foi criada para facilitar o compartilhamento de informações, mas com o tempo, acabou se tornando uma extensão natural da forma que utilizamos para nos comunicar, hoje tornou-se algo presente em diversas esferas das nossas vidas, criando diversas oportunidades e benefícios, devido a facilidade e rapidez proporcionados.

Consequentemente, houve o surgimento de uma nova modalidade de crime, os chamados crimes cibernéticos, crimes informáticos ou crime virtuais, o termo varia entre os diversos autores que abordam o assunto, devido as formas que podem ser utilizadas para praticá-los, podendo utilizar a internet somente como um meio para a prática do crime ou sendo a única forma de praticá-lo.

Nesse sentido, Rossini (2004, p. 13) conceitua crime virtual ou cibernético da seguinte forma:

> Alcança não somente aquelas condutas praticadas no âmbito da Internet, mas todo e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível 'conexão' à Rede Mundial de Computadores, ou a qualquer

> outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da Internet, também seria alcançada pelo que se denominou 'delitos informáticos'.

Dessa forma, segundo o autor, o crime cibernético pode ser entendido como algo amplo, não sendo necessário que tenha sido praticado diretamente através de um equipamento informático ou por meio da Internet, há somente de observar se houve relação entre a prática do crime e a utilização de meios eletrônicos com o objetivo do cometimento do crime cibernético.

Ampliando o conceito de crime cibernético, tem-se a lição de Barreto e Brasil (2020, p. 28), em referência ao conceito jurídico do crime, dizendo que tal ilícito é revestido da seguinte maneira

> Conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Ainda merece destaque, para o mais amplo entendimento dessa modalidade criminosa cibernética, o entendimento de WENDT e JORGE (2013, p. 30) ao explicar afirmando que crimes virtuais podem ser categorizados como em crimes cibernéticos abertos e crimes exclusivamente cibernéticos, os crimes cibernéticos abertos são aqueles cometidos por uso do computador e meios tradicionais, sendo caracterizados por crimes contra a honra, ameaça, importunação ofensiva ao pudor, estelionato, furto mediante fraude, apologia de crimes ou criminoso, racismo, dentre outros.

Já os denominados de crimes exclusivamente cibernéticos, são apenas os que são cometidos por computadores, sendo mais pontuais os crimes de pornografia infantil online, corrupção de menores, pirataria através da violação dos direitos do autor, inserção de dados falsos em sistema de informação e crimes contra equipamentos de votação. (WENDT; JORGE, 2013, p. 30), dessa forma, sendo indispensável o uso de um computador.

Segundo Siena (2013), aponta que uma das dificuldades no combate aos crimes virtuais é a mutação que eles passam, tendo em vista que a evolução da Internet é rápida, e que os crimes cibernéticos estão em pleno alinhamento com as mudanças tecnológicas mundiais, causando mudanças a todo momento, além do grande conhecimento que os chamados, cibercriminosos têm do assunto, tornando a

investigação algo difícil e complexo de ser realizada, considerando a carência de recursos para essas investigações e outras dificuldades inerentes.

Nesse sentido, temos o entendimento de Jesus e Milagre (2016, p. 72), ao afirmarem que: “[...] alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos roubar informações criptografadas, como já havia sendo feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão. ”. Esses indivíduos específicos receberão popularmente a denominação de hackers, quando praticavam os crimes cibernéticos, devido ao seu grau de conhecimento.

Porém, Barreto e Brasil (2016, p. 45) apresenta uma mudança nesse tipo de sujeito.

> Hoje, no entanto, esses estereótipos foram quebrados. Qualquer um pode vir a ser criminoso especializado, até porque a própria internet ensina as técnicas dos mais diversos crimes, indo desde a captura de senhas e identidades às grandes fraudes em sistemas, passando por tráfico de drogas e de armas, contratação de assassinos profissionais, divulgação e prática de pornografia infanto juvenil, etc.

Segundo Jesus e Milagre (2016, p. 95), muitos desses crimes, como a invasão de computadores ou a disseminação de vírus, não existiriam se não fosse pela evolução da tecnologia da computação. Dessa forma, à medida que a tecnologia se tornou mais avançada, o mesmo aconteceu com as atividades ilegais, novas modalidades de crimes cibernéticos estão constantemente surgindo através do uso da tecnologia e da Internet.

Porém, afirma ainda que, não apenas novos crimes surgiram, mas alguns crimes mais tradicionais também foram transformados para o novo meio. Crimes tradicionais como fraude, roubo, estelionato, perseguição e ofensas, que fazem parte de nossa sociedade há anos, agora ocorrem de novas maneiras, o comércio de drogas ilegais e pornografia infantil, que existiam antes do desenvolvimento da tecnologia de rede, agora são vendidas pela Internet e distribuídas em escala mundial, sem muitas dificuldades.

Assim, a evolução dos crimes cibernéticos atingiu seu ponto mais alto com a quando os criminosos observaram que com a amplitude da internet, as pessoas passaram a preferir a comodidade de não se deslocar para bancos e, por isso, utilizaram formas eletrônicas para efetuarem compras, pagamentos, e etc., dessa forma, passando a se a usar a internet e o celular como meios facilitadores.

(CASSANTI, 2014)

As transações financeiras, por exemplo, uso indevido de cartões de crédito e crimes de lavagem de dinheiro evoluíram para novas formas de crime. Em alguns casos, a Internet tornou a prática desses crimes muito mais simples. Esses novos crimes estão ocorrendo porque são relativamente fáceis de cometer, visto que muitas das vezes basta enganar a vítima ou obter acesso ilegal ao seu dispositivo eletrônico. (CASSANTI, 2014)

Ademais, os cibercriminosos podem facilmente invadir sistemas de computador em qualquer lugar do mundo com baixo custo e pouco risco de serem pegos, podendo alterar registros e informações, roubar dinheiro ou roubar as identidades de vítimas inocentes, com intuito de obter vantagens, outros tipos de cibercriminosos podem publicar mensagens e divulgar informações pessoais com a intenção de prejudicar a imagem e a honra de pessoas, somente por satisfação pessoal.

Consequentemente, devido à facilidade com que esses crimes podem ser cometidos, eles estão em ascensão, além do perigo para as pessoas comuns, eles também podem ser muito perigosos para a economia em si, segundo Jesus e Milagre (2016, p. 23), a Polícia Federal em 2004, divulgou que oito em cada dez hackers do mundo viviam no Brasil, e conforme dados da Federação Brasileira de Bancos, o prejuízo teria sido de 900 milhões em fraudes, evidenciando que os crime cibernéticos é um dos maiores riscos para a estabilidade política e financeira global, os cibercriminosos têm o potencial de prejudicar a economia de um país.

A situação no Brasil é extremamente preocupante, devido a lucratividade com atividades ilícitas é de grande potencial, podendo obter grandes quantia de uma única vez, fazendo com que a vontade de ganho fácil de forma fraudulenta seja amplificada, expandindo-se também para o tráfico de drogas por meio de aplicativos, dentre outros tipos de crimes que ocorrem todos os dias.

Essa característica atual alcançou mais proporções após o aparecimento da pandemia da Covid-19, quando se passou a ter necessidade maior de realizadas atividades através de celulares e computadores, as pessoas que resistiam em realizar atividades financeiras no ambiente digital, tiveram que se adaptar à nova realidade, as demais tiveram que ampliar o uso de ambiente digitais. (SANTOS, 2021, p. 53)

Anteriormente a pandemia da Covid-19, toda esta situação de crescimento dos crimes cibernéticos fez com que se tornasse necessária uma resposta do

legislador, o qual passou a apresentar normas atualizadas que visem a prevenção e investigação contra os criminosos que se espalham pela internet, nas últimas duas décadas houve o surgimento de legislações sobre o tema. (SANTOS, 2021, p. 53)

Pode-se pontuar, as principais legislações sobre o tema, como momento inicial dessa nova demanda legislativa, o surgimento da Lei nº 9.296/96, segundo Wendt e Jorge (2012, p. 122) que passou a regulamentar as interceptações telefônicas e telemáticas, permitindo que fosse aplicada na interceptação da caixa de e-mails de investigados, desse modo, que fosse possível receber uma cópia dos e-mails em tempo real.

Para Carvalho (2018), apesar da importância da Internet, e sua rápida evolução, a legislação não acompanhou o mesmo ritmo, tendo sido deixada de lado pela maior parte do Poder Legislativo, que deveria exercer papel de protagonismo na formulação da legislação contra os crimes cibernéticos, apesar da existência de diversos projetos de leis, no qual podemos citar principalmente o Projeto de Lei do Senado n° 76, de 2000, que foi um dos primeiros sobre os crimes cibernéticos e previa diversas modalidades de crimes cibernéticos, mas não obteve sucesso em avançar no Congresso Nacional, sendo arquivado posteriormente. (BRASIL, 2000)

A Lei 12.737/12 conhecida popularmente como “Lei Carolina Dieckmann" entrou em vigor com o objetivo de punir os criminosos virtuais, que divulgaram fotos íntimas da atriz Carolina Dieckmann, tendo sido apresentada e sancionada em menos de um mês após o ocorrido, demonstrando como rápida foi elaboração, e as consequências que isso teria no futuro, a lei foi uma das primeiras e poucas iniciativas para punir quem pratica esse tipo de crime, e pretendia preencher a lacuna que existia na legislação do Brasil, a lei adicionou ao Código Penal, a punição por invasão de dispositivos informáticos. (BERNARDO, 2016).

Posteriormente, surgiu o Marco Civil da Internet, Lei 12.965/14, que em seu preâmbulo, afirma que somente estabelece princípios, garantias e direitos, ou seja, não apresentava punições concretas, somente diretrizes e garantias no uso da internet, estabelecendo que os usuários devem ter proteção, em suas comunicações e informações pessoais. Na prática, se apresentou insuficiente para o combate aos crimes cibernéticos, mas foi um marco na proteção de dados pessoais pelas multas e demais punições contra provedores de dados que violem os direitos dos usuários.

Porém, apesar dessas legislações se fez necessário o uso de analogias para esses tipos de crimes utilizando o Código Penal. Nesse sentido, cabe citar,

segundo (MENDES; VIEIRA, 2012), “Não podemos afirmar que o espaço virtual não tenha nenhuma proteção jurídica, apesar da escassez dessa proteção, por ainda faltar uma lei específica que regule a matéria, alguns crimes cibernéticos podem e devem ser punidos. “, tal posicionamento demonstra o impacto que os crimes cibernéticos podem ter na sociedade, diante da sua evolução.

## 2.2. PRINCIPAIS TIPOS DE CRIMES CIBERNÉTICOS

### 2.2.1 Crimes contra a honra

A internet possibilitou a existência das chamadas rede sociais e aplicativos de comunicações, as quais se desenvolveram de tal forma que se torna quase impossível impedir as publicações e seus compartilhamentos no mundo virtual, em consequências, os crimes contra honra antes limitados ao espaço físico, alcançaram também o espaço virtual, aumentando seu potencial de propagação, existindo atualmente diversos crimes que atingem a sociedade com mais frequência. (CRESPO, 2011, p. 48)

Nesse sentido, temos o entendimento de Patrícia Peck Pinheiro (2013, p. 149), in verbis;

> Como sabemos, o efeito de um conteúdo mentiroso ou calunioso na Internet pode ser muito mais devastador do que em qualquer outro veículo. Mesmo que uma notícia falsa possa ser rapidamente apagada de um site, por exemplo, ela já pode ter sido copiada inúmeras vezes e disponibilizada em muitas outras páginas. Assim como é difícil valorar um conteúdo virtual, é igualmente difícil valorar o tamanho do dano causado por um conteúdo quando passa uma informação errada, calúnia, ou manifesto contra determinada empresa. Ou seja, é praticamente impossível mensurar a extensão do dano; não há controle de tiragem e nem se sabe quantas vezes esse conteúdo foi duplicado [...]

Um dos principais crimes cibernético mais praticado é aquele denominado de crime de difamação, previsto no artigo 139 do Código Penal, segundo (WENDT, JORGE, 2013, p. 102), no qual consiste de uma pessoa divulgar fatos que ofendam a reputação de uma pessoa, levando à perda do respeito social, independentemente de ser verdadeiro ou falso, os fatos alegados, tendo o objetivo definido em atingir a honra, causando prejuízos na vida pessoal e social.

Deve-se destacar, que dentre os crimes contra a honra o mais grave é aquele que se denomina de calúnia, previsto no artigo 138 do Código Penal Brasileiro,

visto que o criminoso atribui diretamente sobre a vítima fato de natureza criminosa, visando amplamente causar-lhe agravos de todas as espécies, não é difícil de encontrar relatos de publicações em redes sociais, que sem provas, atribuem a realização de crimes a pessoas inocentes, colocando inclusive a vida desta pessoa em risco, visto que pode levar a vítima a ser alvo de linchamentos virtuais e físicos. (WENDT; JORGE, 2013, p. 101)

As publicações virtuais criminosas deste tipo são cometidas, quase sempre de forma clandestina ou mesmo utilizando-se de sites que oculte a identidade ou através de perfis falsos, que dificultam sua identificação, posto que o seu autor tem pleno conhecimento da ilegalidade da sua conduta que está a cometer, utilizando-se da clandestinidade para sua consumação, (WENDT; JORGE, 2013, p. 101)

Por fim, temos o crime de injúria, previsto no artigo 140 do Código Penal que tem como objetivo difundir qualidades negativas contra uma pessoa, geralmente através de xingamentos, atacando-a moralmente, desse modo, ofendendo a sua dignidade e decoro, sendo consumada quando a vítima fica ciente do fato, não sendo necessário que outras pessoas tomem conhecimento. (WENDT; JORGE, 2013, p. 102)

Como consequência, os crimes citados anteriormente, em conjunto ou em separado, terminaram por gerar uma modalidade de crime que se passou a chamar de cyberbullying, que nada mais é do que utilizar a internet para difamar de forma irracional a vida social da vítima, estas condutas criminosas geraram inúmeras situações de constrangimento e depressão das vítimas, podendo inclusive, levar ao suicídio, evidenciando o potencial que estes crimes têm na vida pessoal das vítimas. (PINHEIRO, 2013, p. 150)

### 2.2.2 Engenharia social

Segundo Wendt e Jorge (2013, p. 20), a engenharia social é a utilização artifícios ou procedimentos utilizados por golpistas que possui o objetivo de manipular pessoas, e consequentemente obter dados pessoais, informações de empresas, ou a execução de uma tarefa específica, para que seja possível obter uma vantagem, a principal diferença das ameaças cibernéticas existentes é que o foco da ação é na vítima.

Em geral, nesses crimes o autor busca obter a confiança da vítima através

de suas propostas, tendo o foco principal na concentração das vulnerabilidades da vítima, que pode ser a ganância, amizade, confiança, e etc., nesse sentido “nestas situações o ponto nevrálgico é a falta de conscientização do usuário [...], onde alguém faz uso da persuasão [...] para obter informações que podem ser utilizadas para ter acesso não autorizado a computador e informação” (WENDT; JORGE, 2013, p. 20).

Geralmente, por meio da utilização da utilização de informações disponíveis publicamente ou obtidas de forma ilegal, com o objetivo de dar maior credibilidade as suas afirmações, o criminoso busca atrair a vítima sem que ocorra nenhuma desconfiança, utiliza-se a identidade de empresas de cartões de créditos, bancos, e órgãos do Governo, como a Receita Federal ou Banco Central. (CRESPO, 2011, p. 86)

Esses atos são praticados, geralmente, com auxílio de falsos perfis, falsos e-mails, falsos suportes técnicos, dentre outros meios ilícitos, desse modo, a engenharia social não segue uma regra específica de cometimento, ela se renova, um modelo de abordagem pode não ser ideal para uma determinada vítima, devendo os criminosos sempre se adaptar nos métodos utilizados para que consiga o êxito, sendo necessária sempre criar novas formas de enganar as vítimas. (CRESPO, 2011, p. 87)

Ademais, o principal meio utilizado para engenharia social é através do método conhecido como “phishing“, tal conduta consiste em enviar mensagens eletrônicas, principalmente por e-mail, em grande quantidade, contendo links de páginas falsas de bancos ou similares, com o objetivo de enganar a vítima a fornecer suas informações bancárias, como senhas e dados dos cartões de créditos, para que seja efetuado compras e transferências. (MILAGRE; JESUS, 2016, p. 135)

### 2.2.3 Pornografia infantil

Diante do rápido avanço que a internet teve na sua expansão e capacidade de aproximar as pessoas, facilitou que criminosos que possuem como alvo crianças e adolescentes, pudessem se aproximar das suas vítimas de forma que fiquem fora da vista da maioria das pessoas, ademais, a facilidade de compartilhamentos de arquivos, como fotos e vídeos, permitiu que o dano causado seja devastador, com o compartilhamento de imagens de crianças e adolescentes. (BEZERRA; AGNOLETTO, 2019, p. 46)

Deve-se ressaltar primeiramente que a pedofilia é um distúrbio sexual, no

qual um adulto se sente atraído pela prática sexual contra crianças e adolescentes, não sendo um crime em si, pois não há tipo pena por ter esse distúrbio, sendo que é necessário a verbalização de determinadas condutas, como produzir, gravar, compartilhar, comprar ou armazenar de crianças e adolescentes. (CANÇADO, 2019, p. 89)

Os atos de pedofilia, em qualquer das condutas, se traduzem em crime de natureza grave e que deve ser punido de forma rigorosa pelo Estado, tendo em vista que a vítima sempre é o ser mais vulnerável da relação social, nesse caso, as crianças e adolescentes, os quais são vítimas fáceis para os criminosos virtuais que fazem de tudo para obter fotos, vídeos e etc, que permitam obter lucros com vendas de material pornográfico e outros objetivos. (CASSANTI, 2014, p. 56)

Esse crime não atinge somente uma vítima diretamente, ele vai muito mais além, atingindo inúmeras vítimas indireta, uma coletividade, que são os pais, parentes ou amigos vitimados por esta modalidade de ilícito, com a globalização da internet este crime ganhou um maior número de criminosos que acreditando na capacidade de anonimato, se sentem protegidos para a devida prática criminosa, geralmente, utilizando redes complexas de diferentes camadas e que dificultam a localização de seus atos criminosos. (ALBUQUERQUE, 2019)

Em 2008, como uma forma de combater a evolução do alcance desse tipo de crime, diante da diminuição da distância entre as vítimas e os criminosos pela internet, e o aumento de casos, foi aprovada a Lei nº 11.829/2008, que inclui diversos dispositivos no Estatuto da Criança e do Adolescente (ECA), tal alteração, tipificou condutos que não eram previstas na legislação anteriormente, como por exemplo, armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. (BEZERRA; AGNOLETTO, 2019)

O Estatuto da Criança e do Adolescente (ECA), no artigo 240 e 241-E, prevê as tipificações de forma alcançar os criminosos que se utilizam de meios eletrônicos para a execução da pornografia. Dessa forma, uma das medidas mais eficazes contra estas ações criminosas é a rápida atuação da polícia na busca de identificar o provedor de serviços e requerer as informações necessárias para a identificação do dispositivo e consequentemente de seu usuário, tudo como forma de combater e punir estas ações criminosas contra as crianças e adolescentes. (SANTOS, 2019, p. 47)

Por ser um crime que impacta a vida de crianças e adolescentes, os investigadores deverão através da identificação do criminoso; rastrear o fluxo de compartilhamento de arquivos de material sexual, para que seja possível juntar as provas necessárias para a comprovação do ato ilícito, localizar e identificar os conteúdos armazenados para a devida apreensão, seja fisicamente ou remotamente, além de identificação de demais envolvidos. (VELLOSO, 2015).

### 2.2.4 Cyberstalking

Segundo CASTRO e SYDOW (2021, p. 52), Cyberstalking é o ato de contato persistente e indesejado de perseguir alguém online. Podendo ser de várias formas, incluindo ameaças, calúnia, difamação, assédio sexual ou outras ações para controlar, influenciar ou intimidar sua vítima. Um perseguidor cibernético depende totalmente do anonimato dado pela internet, que permite que eles persigam sua vítima sem serem detectados, ou identificados.

O termo “Cyberstalking” tem origem na palavra “Stalking”, que segundo NAVAS JUNIOR (2020, p. 87), tem a seguinte definição, in verbis;

> O “STALKING” deriva do termo “stalk”, que numa tradução livre seria algo como “perseguição furtiva”, embora seja traduzido em adaptação livre para “ato de perseguir alguém, de forma continuada e reiterada, ameaçando sua integridade física e psicológica, com restrição à liberdade de locomoção ou invasão à liberdade ou privacidade de outra pessoa. ”

Umas das diferenças entre a perseguição tradicional, conhecida como stalking e a perseguição cibernética, conhecida como cyberstalking, se apresenta na proximidade geográfica entre o ofensor e a vítima. Em um caso tradicional de perseguição, o perseguidor segue consistentemente uma pessoa em todos os lugares, podendo ser no caminho para casa, mercado, e etc, enquanto os perseguidores cibernéticos podem assediar a vítima de outra cidade, estado ou outro país, através da internet. (NAVAS JUNIOR, 2020, p. 87)

A perseguição cibernética pode ser cometida por estranhos que obtiveram informações pessoais das vítimas na Internet. Vítimas involuntárias podem postar diversos dados de identificação pessoal em sites de redes sociais, incluindo idade, números de telefone, interesses pessoais e fotografias. Os perseguidores cibernéticos podem usar os mecanismos de pesquisa da Internet para descobrir informações adicionais que podem usar para assediar suas vítimas. (NAVAS JUNIOR, 2020, p. 87)

Em 2021, o crime de “stalking” foi adicionado ao Código Penal Brasileiro através da Lei 14.132/21 que incluiu o artigo 147-A, sua redação permitiu a aplicação tanto para a perseguição tradicional, como a cibernética, in verbis; “ Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. ” (BRASIL, 1940). A criação da tipificação supriu uma lacuna legal que existia, permitindo a proteção das vítimas, algo extremamente necessário devido à expansão deste tipo de crime. (CASTRO; SYDOW, 2021, p. 52)

Desse modo, demonstra-se que a Internet é particularmente atraente para perseguidores cibernéticos e outros predadores online, simplesmente porque muitos são atraídos por seu custo relativamente barato, facilidade de uso e, como mencionado anteriormente, seu anonimato ao procurar vítimas e evitar serem descobertos, e responsabilizados.

## 2.3 A investigação de crimes cibernéticos

A investigação dos crimes cibernéticos possui papel fundamental para que seja possível alcançar os responsáveis pela prática desses crimes, e se tornou cada vez mais relevante diante do avanço da tecnologia, os crimes cometidos através da internet são mais complexos do que os que são denominados de crimes físicos, por isso Wendt e Jorge (2012, p. 51) afirma que na investigação cibernética existem duas fases distintas: a fase técnica e a fase de campo. Na fase técnica são realizadas ações com o objetivo de reunir informações para localizar o computador ou dispositivo utilizado para a prática da ação criminosa.

Uma das primeiras diferenças da investigação tradicional e a investigação cibernética é que um dos pontos iniciais, é realizada através da identificação do IP (Internet Protocolo), obtido através dos registros de acesso, desse modo, se fará possível entender os movimentos efetivados por aquele que praticou o crime, nesta fase a investigação busca a localização do equipamento utilizado para a execução da ação criminosa. (WENDT; JORGE, 2012, p. 53). É neste momento que o investigador irá analisar as informações fornecidas pela vítima e passará a traçar os possíveis caminhos utilizados pelo criminoso no sentido identificá-lo.

Neste momento, para melhorar a compreensão, deve-se explicar alguns relevantes conceitos da investigação, segundo BARRETO e BRASIL (2016, p. 91), um deles é que os registros de acesso são informações que os provedores de aplicações de internet, são obrigados armazenar, e que permitem a identificação dos usuários, conforme o artigo 5, VIII da Lei 12.965/14, conhecida como Marco Civil da Internet, a definição de registro de acesso é “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. ” (BRASIL, 2014). São consideradas aplicações de internet, os sites, aplicativos, redes sociais e etc.

Consequentemente, permitindo que a autoridade policial com uma ordem judicial, solicite tais informações, e posteriormente, identifique o responsável através de solicitação para o provedor de conexão (fornecedor do serviço de internet.), responsável por atribuir o endereço de IP e conectar o usuário à Internet, que informará qual indivíduo estava utilizando aquele endereço de IP, na data e horário específico. (BARRETO; BRASIL, 2016, p. 91)

Outro conceito de suma importância é o endereço de IP, para Teixeira (2013, p. 43), pode ser definido nas seguintes palavras, “O endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando”, ademais, exemplifica, WENDT e JORGE (2012, p. 53), quando um dispositivo ou computador se conecta à Internet, um endereço de IP é designado para o usuário, dessa forma, não é possível que existam dois usuários com o mesmo endereço, enquanto utiliza a Internet.

Nesse sentido, afirma Maia, a importância do endereço de IP para a investigação (MAIA, 2017, p. 70).

> No caso da Internet, o endereço IP é um importante dado para investigação pois embora o criminoso oculte seus dados cadastrais de um determinado provedor de serviço, seu endereço IP utilizado para acesso a esse serviço pode ficar registrado nesse provedor. Esse endereço IP pode nos auxiliar a rastrear o local e a máquina de onde partiu determinado ataque criminoso. [...]

Ademais, segundo leciona Patrícia Peck Pinheiro (2013), destacando a importância e confiabilidade dessas informações.

> A testemunha do crime é aquele que detém os protocolos IP´s, aquele que armazena os dados sobre as transações ocorridas eletronicamente. Da mesma forma, as provas eletrônicas – que muitos hesitam em aceitar juridicamente, alegando que são altamente adulteráveis – podem passar por perícia técnica rigorosa para serem aceitas em processos. [...] com profundo conhecimento da tecnologia, é possível ter prova virtuais muito mais confiáveis que as do mundo real.

Sob essa ótica, Vecchia exemplifica, (2015), toda vez quando um usuário acessa aplicativos, e-mails, redes sociais, blogs, e etc., o endereço de IP, junto com outras informações é registrado em um servidor (computador responsável por manter essas informações), tendo como exemplo, quando um indivíduo utilizando um perfil falso, envia uma mensagem de calúnia ou de ameaça, as empresas que fornecem o serviço armazenam as informações referente a mensagem, como o conteúdo, data, horário, e endereço de IP, responsável pelo conteúdo e conexão.

Nesse sentido, uma das primeiras etapas a ser realizada após a ocorrência do crime, é a solicitação de preservação de dados, considerando que o ambiente virtual é de rápida mutação, as evidências podem desaparecer devido à natureza do meio empregado, o sucesso de uma investigação de crimes cibernéticos depende da coleta e preservação destas, a solicitação da preservação de conteúdo pode ser realizado diretamente ao responsável pela guarda, tal solicitação pode ser feita de forma online, através de formulários eletrônicos disponibilizados pelas empresas ou por meio de ordens judiciais (BARRETO, 2020, p. 141)

Conforme Barreto e Brasil (2016, p. 53), a autoridade policial e o Ministério Público podem realizar a solicitação de preservação dos registros, com base no Marco Civil da Internet, que estabelece que os prazos podem variar entre seis meses e um ano, destaca também que a solicitação de preservação perderá eficácia, se não houve o protocolo de uma representação judicial em prazo hábil.

Ademais, segundo Barreto e Caselli, (2017, p.120), há outros meios de preservação, como através de uma captura de tela, ou que a preservação seja feita por um escrivão de polícia, devido a sua fé pública, que poderá elaborar um termo, demonstrando que teve acesso ao material, outra possibilidade é por meio de uma ata notarial, realizada por um tabelião, com base no artigo 384 do Código de Processo Civil.

Realizado a fase de preservação, conforme já mencionado, será necessário obter uma ordem judicial, para que sejam fornecidos os registros de acessos, no qual inclui principalmente o endereço de IP, informação essencial em uma

investigação de crime cibernético, após sucesso no pedido da ordem judicial, será necessário encaminhar para o provedor de acesso, que deverá responder dentro do prazo, os dados solicitados. (LESSA; VIEIRA, 2017, p. 7).

Com os referidos dados em mãos, a autoridade policial, poderá requerer, os registros de conexão para o provedor de conexão, responsável por fornecer o serviço de acesso à internet aos indivíduos, tal requisição não necessita de ordem judicial, conforme o Marco Civil da Internet, visto que somente contém os dados cadastrais armazenados pelos provedores de conexão, sendo as informações; nome, CPF, endereço e filiação, não incluindo dessa forma, o conteúdo das comunicações. (SILVA; BARRETO; KUFA, 2021, p. 147),

Segundo Silva, Barreto e Kufa (2021, p. 148), é obrigação do provedor de conexão, com base no Marco Civil da Internet, adotar providências com o objetivo de que os usuários sejam identificados, por meio do armazenamento das informações durante o prazo legal, evitando assim o anonimato, e permitindo que seja possível responsabilizar os usuários por suas condutas.

Posteriormente aos passos citados e com a devida identificação do IP e seu responsável, passa-se para a fase de campo, onde serão realizadas as devidas diligências necessárias para que sejam ratificados com os indícios e as informações iniciais colhidas na primeira fase da investigação, com a necessidade de deslocamento das autoridades policiais para que seja realizada a apreensão física de evidências e as posteriores diligências. (WENDT; JORGE, 2013, p. 52). Deve-se observar, a necessidade de obter uma medida processual penal cautelar, em geral, um mandado de busca e apreensão, com fundamento nas informações obtidas pelo provedor de conexão.

Dentre as diligências cabíveis e possíveis após a obtenção das evidências físicas, pode-se citar as denominadas de periciais, que se caracterizam por sua importância na realização de exames nos vestígios deixados pelos criminosos virtuais, visto que, através da ação pericial o que antes se traduzia em indícios aos poucos pode ir tomando caracterização de evidências digitais, as quais são importantes para a comprovação da materialidade do crime. (WENDT; JORGE, 2013, p. 210)

Deve-se fazer uma ressalva, conforme destaca Vianna e Machado (2013, p. 74), quanto à forma de apresentação das provas, deve ficar claro que a investigação de crimes cibernéticos admite que as provas sejam apresentadas por todos os meios legais, ou seja, podem ser utilizadas provas documentais, depoimentos e provas

periciais. Todas essas premissas podem ser admitidas e utilizadas para caracterizar a substância e autoria dos crimes cibernéticos, porém, no contexto de tais crimes, a prova pericial tem papel principal.

Desse modo, a importância das evidências digitais nas investigações cibernéticas, bem como a sua anterior preservação, é destacada;

> A evidência digital é de grande valia e deve ser tratada da mesma forma que a de outro local de crime. Caracteriza-se por ser volátil, anônima (em princípio), alterável e/ou modificável, bem como pode ser eliminada a qualquer instante. Arquivos temporários, cookies, horário de inicialização de um computador e logs de acesso são exemplos de evidências digitais. A preservação da evidência em crimes praticados na internet é uma das grandes dificuldades com que a investigação depara. O caminho é bem longo desde a procura da vítima na delegacia de polícia até a expedição da ordem judicial determinando ao provedor a disponibilização dos registros de conexão e acesso a aplicações de internet. (BARRETO e BRASIL, 2016, p. 53)

Concluída todas as etapas, através da análise das evidências e indícios coletados, forma-se o conjunto probatório que permitiram a responsabilização do criminoso, porém, a investigação dos crimes cibernéticos nem sempre segue um caminho rápido, decorrente das características dessas evidências digitais, além das dificuldades que podem surgir no decorrer da investigação, que acabam por tornar cada vez mais desafiador esse caminho.

# 3 DIFICULDADES NAS INVESTIGAÇÕES DE CRIMES CIBERNÉTICOS

Neste capitulo serão abordadas as dificuldades encontradas durante as investigações de crimes cibernéticos, como a burocracia no uso do Mutual Legal Assistance Treaty (MLAT), um tratado firmado entre o Brasil e o Estados Unidos, que nos dias atuais burocratizou o acesso a informações importantes para a investigação, como mensagens, fotos e vídeos, enviados através da Internet, exigindo a realização de um procedimento demorado e que pode demorar meses para ser concluído.

Em seguida, serão apresentadas as consequências decorrente do surgimento do Marco Civil da Internet, no acesso aos dados cadastrais e registros de acessos, com os entraves criados pelos provedores estrangeiros que costumam negar o acesso aos dados, apesar de dispositivos legais permitirem o acesso por parte das autoridades, sem a necessidade de ordem judicial, e ainda, será demonstrada a importância que a disponibilização dessas informações possuem para a celeridade da investigação.

Por fim, as dificuldades encontradas no uso de criptomoedas em crimes cibernéticos, seu surgimento, bem como suas características que permitem o anonimato na sua movimentação, além das dificuldades para realizar a apreensão desses ativos.

## 3.1 A BUROCRACIA NO USO DO MUTUAL LEGAL ASSISTANCE TREATY (MLAT) NA INVESTIGAÇÃO

Em 1997, diante da necessidade de facilitar a cooperação internacional em matéria penal entre o Brasil e o Estados Unidos, é assinado em Brasília, o Mutual Legal Assistance Treaty (MLAT), em tradução, tratado de assistência jurídica mútua, um tratado que tem como seu objetivo instituir diversas formas de cooperação, conforme redação presente no preâmbulo do acordo, como forma de “facilitar a execução das tarefas das autoridades responsáveis pelo cumprimento da lei de ambos os países, na investigação, inquérito, ação penal e prevenção do crime por meio de cooperação e assistência judiciária mútua em matéria penal” (BRASIL, 2001), seu uso principal, evidenciou em facilitar a troca de informações entre ambos os países, apesar da sua importância na época, o tratado só foi aprovado pelo Congresso em 2001, tendo entrado em vigor no mesmo ano. (SOUZA, 2015, p. 164)

Em 2014, no Marco Civil da Internet, o artigo 11, §2, estabeleceu a obrigatoriedade da aplicabilidade da legislação brasileiras frente aos provedores de conexão ou de aplicação de internet, podendo ser nacionais ou estrangeiros, devendo cumprir um dos requisitos; disponibilizar serviço ao público brasileiro ou que possuam filial no País, apesar de existir tal disposição na legislação, o dispositivo esbarra na resistência dos provedores e nas respectivas legislações das localizações de suas sedes. (ARAÚJO, 2019, p. 105)

No Brasil, há uma pluralidade de provedores de conteúdo que são estrangeiros, entre os principais, estão o Google, Facebook, Instagram e Whatsapp, tendo como sua sede principal os Estados Unidos, dessa forma, alegam que os dados dos usuários estão armazenados fora da jurisdição do Brasil, não sendo possível cumprir ordens judiciais emitidas no Brasil, apesar de manterem filiais brasileiras no País. (IMAY; GARCIA, 2021)

É o que pontua também, Jesus e Milagre (2016, p. 194)

> Não incomum, os agentes buscam praticar delitos por meio de sistemas hospedados no exterior. Nestes casos, a investigação, no Brasil, necessita da cooperação de provedores (de serviço e de conexão) de fora do país, o que não é uma tarefa fácil, **considerando que parte dos provedores costuma alegar que não estão sujeitos às ordens da jurisdição brasileira** (isto passa a se relativizar com a aprovação do Marco Civil da Internet). (grifo nosso)

Conforme estabelecido pelo Marco Civil da Internet, os dados cadastrais, que são o e-mail, telefone, logs de conexão contendo os IP's, que possibilita identificar o responsável pelo acesso à internet, tais dados que são básicos, e conforme estabelecida pela legislação brasileira, o delegado pode requisitar diretamente dados cadastrais, porém, os provedores insistem em exigir uma ordem judicial, sendo necessário da autoridade policial enviar uma representação policial para que a autoridade judicial, autorize o seu acesso. Diante da ordem judicial devidamente expedida, as empresas não costumam negar a entrega dos dados cadastrais. (IMAY; GARCIA, 2021)

Porém, a necessidade do uso do MLAT, segundo Jorge (2018, p. 32) ocorre quando há necessidade de acessar o conteúdo das informações, que na maioria das vezes, trata-se da comunicação sigilosa dos usuários, podendo ser, as mensagens trocadas, fotos, publicações, vídeos, áudios, e demais informações, que não são entra no rol de dados cadastrais. Em uma investigação policial, as informações mais

importantes para elucidação de um caso, podem estar justamente no conteúdo das informações trocadas, tal tese é defendida por diversos autores.

Nesse sentido, leciona Fernandes (2018, p. 225):

> [...] a relação com os servidores internacionais que, muitas vezes, arguindo privacidade de seus clientes, se recusam a cooperar no fornecimento de dados e informações, como no caso da utilização de "proxies" **ou do fornecimento do conteúdo dos perfis nas redes sociais**, principalmente nos casos envolvendo crimes de pedofilia, bem como a utilização pelo investigado do armazenamento de informações nas nuvens ou servidor localizados em outro país, tornando-se necessária a cooperação internacional, adiando a conclusão das investigações.
> Nos crimes de pedofilia praticados pelas redes sociais, o pedófilo com frequência solicita ao menor que apague as conversas com o autor, esvaziando-se a materialidade do crime praticado**, sendo necessário nesses casos que a Empresa forneça o conteúdo das conversas daqueles perfis**, o que não vem ocorrendo com regularidade, dificultando o prosseguimento das investigações. (grifo nosso)

Cabe destacar, é cediço a proteção da Constituição Federal ao sigilo das comunicações e o direito da privacidade, existente também no direito constitucional de outros países, porém, diante da necessidade de obter evidências necessárias para elucidação de um crime, devidamente aprovada por uma autoridade judicial, não se obstem haver empecilhos no seu acesso.

Considerando que o uso do MLAT é facilitação da cooperação em matéria penal, em sua grande maioria de casos, em uma investigação criminal, é de esperar que o processo fosse simples e rápido, porém, não é o caso, o processo deverá passar por diversas etapas, entre os países, esse processo demorado, coloca em risco uma investigação, diante do risco da perda das informações, fato que será explicado de forma sucinta, nos próximos parágrafos. (BARRETO; WENDT, 2015)

Conforme Versianni, (2020, p. 159), uma das primeiras etapas a serem realizadas pela autoridade, quando deparado com a necessidade de utilizar o MLAT, é solicitar a preservação dos dados que serão requisitados, a solicitação muitas vezes, podem ser feitas diretamente por meio de ferramentas online disponibilizadas pelos responsáveis dos dados, tal etapa é essencial para garantir que as informações não serão perdidas, devido ao lapso de tempo necessário para que o processo seja concluído, que pode ser superior ao tempo que as empresas são obrigadas a manter os dados.

A solicitação para o uso do MLAT, deve ser dirigida ao Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), órgão vinculado

ao Ministério da Justiça, sendo a autoridade responsável por realizar e acompanhar a tramitação dos pedidos de MLAT no Brasil, encaminhando os pedidos para os países que fazem parte do acordo de cooperação. (VERSIANNI, 2020)

Conforme disposto no próprio Manual de Cooperação do DRCI (BRASIL, 2014), a autoridade responsável pela investigação deverá encaminhar o pedido de cooperação em duas vias, sendo uma em português e outra na língua oficial do país que será requerido, não sendo responsabilidade do DRCI, a realização da tradução, ou seja, caberá ainda a autoridade realizar a tradução do pedido, que dependendo da localização dos dados requeridos, pode a autoridade não ter conhecimento linguístico necessário para elaborar a tradução, criando um empecilho no pedido, estando os requisitos cumpridos, a solicitação será enviado para o País, que realizará a sua avaliação. (LEITE, 2012, p. 10)

Ademais, segundo Souza (2020) ressalta que o tempo de resposta dos MLATs, é demasiadamente elevado para uma investigação criminal, devido ter sido pensado para o acesso de dados e produção de provas, em um tempo que a Internet não era tão difundido como nos tempos atuais, destaca ainda que o prazo atual de resposta é incompatível com uma investigação, chegando a demorar 10 (dez) meses em média para ser obtida uma resposta.

Nesse sentido, Domingos e Roder (2018, p. 34),

> Tais pedidos, conhecidos como Mutual Legal Agreement Treaties (MLATs) – Acordos de Assistência Mútua em Matéria Penal, tradicionalmente têm um processamento muito lento, pois dependem de que os pedidos sejam feitos de forma correta, de que sejam traduzidos e enviados pelas autoridades competentes, para que uma autoridade no país requerido dê início à execução do pedido. **Esse procedimento protocolar, que já se apresentava por demais demorado para os pedidos tradicionais, é no mais das vezes inócuo em face da volatilidade das provas digitais e da necessidade de investigação célere**, não estando adequado às novas tecnologias. (Grifo nosso)

Somado a todos os fatores citados, há o pior obstáculo no uso do MLAT durante uma investigação, que são os casos em que não há resposta por parte das autoridades dos Estados Unidos, conforme o ex-Ministro da Justiça do Brasil, Sérgio Moro, em audiência pública revelou que no período de 2016 a 2019, 74% dos pedidos de cooperação não foram respondidos, sendo 5,2% cumpridos de forma parcial, e apenas 20,8% dos pedidos foram cumpridos integralmente. (VALENTE, 2020)

Ademais, conforme Castro (2020), um dos maiores motivos para a negativa das solicitações de cooperação, é pela ausência da chamada causa provável (probable cause), prevista na 4ª emenda da Constituição do Estados Unidos, ou por violar a liberdade de expressão da 1ª emenda, naturalmente existe uma incompreensão do Brasil quanto ao direito estrangeiro que difere dos requisitos necessários.

Desse modo, a causa provável, pressupõe demonstrar a conexão que o crime está sendo cometido, com os fatos e as circunstâncias demonstrando a necessidade do deferimento da medida solicitada (CASTRO, 2020). A necessidade de estabelecer a probable cause e a exigências estabelecidas, é uma das dificuldades das autoridades brasileiras, segundo responsáveis pelo DRCI, Junior e Carneiro (2018, p. 24), in verbis: “Os níveis de exigência da probable cause da lei norte-americana muitas vezes inviabilizam por completo o próprio pedido de cooperação brasileiro, até porque eventualmente tais dados sejam inacessíveis Às autoridades nacionais. ”. Dessa forma, demonstra-se que acessar dados de conteúdo não é uma tarefa fácil em uma investigação, tornando-se muitas vezes inviáveis.

Em 2017, o Superior Tribunal de Justiça aplicou o entendimento que as empresas internacionais possuem a obrigação de cumprir ordens judiciais emitidas no Brasil, sendo desnecessário a utilização do MLAT, tendo inclusive fixado multa ao Facebook pelo descumprimento da decisão anterior.

> RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. QUEBRA DE SIGILO TELEMÁTICO. CUMPRIMENTO INCOMPLETO DE ORDEM JUDICIAL. APLICAÇÃO DE MULTA DIÁRIA À EMPRESA RESPONSÁVEL PELO FORNECIMENTO DE DADOS (FACEBOOK). POSSIBILIDADE. VALOR DAS ASTREINTES. RAZOABILIDADE E PROPORCIONALIDADE. 1. Situação em que a FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. impugna decisão judicial que, em sede de inquérito, autorizou a interceptação do fluxo de dados telemáticos de contas Facebook de investigados, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais). 2. Não há ilegalidade ou abuso de poder a ser corrigido, pois fica claro o cumprimento incompleto da decisão judicial que determinara o fornecimento de dados de contas perfis no Facebook de investigados, já que não foram trazidas todas as conversas realizadas no período de 13/10/2015 a 13/11/2015, tampouco as senhas de acesso, o conteúdo completo da caixa de mensagens, o conteúdo da linha do tempo (timeline) e grupos de que participam, além das fotos carregadas no perfil com respectivos metadados. 3. A mera alegação de que o braço da empresa situado no Brasil se dedica apenas à prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade e suporte de vendas não exime a organização de prestar as informações solicitadas, tanto mais quando se sabe que não raras vezes multinacionais dedicadas à exploração de serviços prestados via internet se valem da escolha do local de sua sede e/ou da

> central de suas operações com o objetivo específico de burlar carga tributária e ordens judiciais tendentes a regular o conteúdo das matérias por elas veiculadas ou o sigilo de informações de seus usuários.
> 4. Por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo.
> [...]
> 10. Recurso ordinário em mandado de segurança a que se nega provimento. (BRASIL, RMS 55.109/PR, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 07/11/2017, DJe 17/11/2017)

Diante do entendimento firmado pelo Superior Tribunal de Justiça, que obrigava as empresas fornecer as informações sem a utilização do instrumento do MLAT, estas recorreram ao Supremo Tribunal Federal, questionando tal decisão, por meio da Ação Declaratória de Constitucionalidade 51, que encontra-se pendente de julgamento. (CASTRO, 2020, p. 27)

Conclui-se, que as diversas dificuldades e burocracias impostas ao acesso do conteúdo de usuários em provedores estrangeiros, que apesar de prestarem serviços para brasileiros, não se submetem as legislações brasileiras e as ordens judiciais que autorizam o acesso a tais dados, consequentemente os prejuízos para uma investigação, é o risco da perda das informações necessárias, demonstra-se como o MLAT, tornou-se uma forma ultrapassada e ineficiente de obtenção de provas. (CERQUEIRA; ROCHA, 2013, p. 25).

## 3.2 As consequências do Marco Civil da Internet na investigação e as dificuldades no acesso de dados cadastrais e registros de acesso

Diante da falta de regulamentação de diversos pontos da legislação brasileira, surge a Lei 12.965/14, conhecida como Marco Civil da Internet, que em seu preâmbulo esclarece o seu objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Apesar de não tratar especificamente da investigação de crimes cibernéticos, sua promulgação trouxe diversos impactos neste tema, sendo responsável por estabelecer prazos, requisitos e limitações da investigação. (BARROSO, 2019, p. 40)

Uma das dificuldades ocasionadas pelo Marco Civil, é o acesso aos dados cadastrais e registros de acesso, primeiramente, deve-se esclarecer a diferença entre ambos, dados cadastrais conforme o Decreto 8.771/16, que regulamenta o Marco Civil da Internet, em seu art. 11, § 2º, e especificou a quais informações são referentes, a

filiação, endereço, a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário. (BRASIL, 2016). Estas informações, não violam o direito à privacidade dos usuários e nem constituem violação do sigilo de comunicação, sendo meras informações de identificação. (BARRETO; BRASIL, 2016, p. 103)

Conforme Junior (2020), anteriormente, a entrada em vigor da supracitada norma, diferentes leis abordaram o poder de requisição de dados cadastrais pelas autoridades policiais, nos quais podemos citar, a Lei de Organizações Criminosas (Lei 12.850/2013), Lei de Lavagem de Dinheiro (Lei 9.613/1998), e especialmente a Lei 12.830/2013, que trata da investigação criminal pelo Delegado de Polícia, não limitando o poder requisitório necessariamente há um crime específico, permitindo o acesso para a investigação em qualquer tipo de crime, tais leis, não deixam dúvidas sobre esta possibilidade.

Ademais, segundo leciona (PEREIRA, 2013) que destaca a importância do poder requisitória da autoridade policial, decorre da necessidade de fazer a coleta de provas de forma rápida, que possibilitaram a elucidação dos fatos investigados, a legislação presente possibilita que nem todas os atos de investigação, precisem passar pela tutela do judiciário, desse modo, permitindo a requisição de dados existentes em banco de dados ou em outras fontes, desde que não viole o direito ao sigilo de dados ou comunicações, nesse caso, especificamente, os dados cadastrais.

Nesse sentido, o Marco Civil, abordou o tema ratificando o previsto em Leis anteriores, em seu artigo 10, §3, in verbis:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 3º O disposto no caput não **impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei,** pelas autoridades administrativas que detenham competência legal para a sua requisição. (BRASIL, 2014, grifo nosso)

Porém, segundo leciona o Delegado Fernandes (2019, p. 72), apesar dos inúmeros dispositivos que permitem a requisição somente de dados cadastrais sem a necessidade de uma ordem judicial, as grandes empresas estrangeiras possuem o costume de não fornecer tais informações, alegando que se aplicam somente a crimes específicos e impondo a necessidade de ordem judicial, consequentemente causando atrasos desnecessários em investigações.

Nesse sentido, pode-se observar a resposta de um provedor de aplicação de internet estrangeiro, referente às restrições impostas em fornecer dados cadastrais (informações básicas de usuário), in verbis:

> Primeiramente, o WhatsApp fornecerá informações básicas de usuário à polícia sem ordem judicial em determinadas circunstâncias, dentre as quais quando o requerimento policial indicar expressamente que a investigação em curso relaciona-se a (i) crime previsto na Lei de Organizações Criminosas (Lei Federal n. 12.850/2013); (ii) crime previsto na Lei de Lavagem de Capitais (Lei Federal n. 9.613/1998); (iii) pornografia infantil; (iv) sequestro ou cárcere privado; (v) redução a condição análoga à de escravo; (vi) tráfico de pessoas; (vii) extorsão mediante sequestro; (viii) extorsão qualificada; (ix) tráfico internacional de criança ou adolescente; ou (x) terrorismo. Por gentileza, note que é necessária uma ordem judicial para disponibilização dos endereços de IP dos usuários. (Anexo A - Whatsapp Records, 2019)

Conforme leciona ALBERTO (2020 p. 331), tal posicionamento dos provedores em relação aos dados cadastrais, pode configurar crime, conforme previsto no Artigo 21 da Lei 12.850/13, que se refere a recusa ou omitir dados cadastrais requisitados por uma autoridade durante uma investigação, destacando que a legislação foi clara em possibilitar o acesso aos referidos dados sem reserva de jurisdição.

Ademais, outra dificuldade é em relação aos registros de acesso, decorrente de uma das modificações trazida pelo Marco Civil, conforme o artigo 10, §1, estabeleceu que o provedor responsável por armazenar os dados, são obrigados a disponibilizar os registros, que permitam a identificação de usuário, somente mediante ordem judicial, dessa forma, tornando necessário a intervenção do judiciário, toda vez que a autoridade policial deseja obter os referidos registros. (BRASIL, 2014)

Porém, com a referida novidade legislativa, houve uma maior burocracia e atraso na investigação, visto que anteriormente, não havia diferença entre dados cadastrais e registros de conexão e acesso, permitindo que as autoridades com base nos dispositivos de acesso aos dados cadastrais, obtivessem os registros de acesso, visto que a jurisprudência anterior entendia que incluía o endereço de IP, nos dados cadastrais, podendo requisitar diretamente as informações. (SOARES; ZANIN, 2015, p. 6).

Cabe destacar, que segundo Zanin e Soares (2015, p. 6), anteriormente ao Marco Civil da Internet, a jurisprudência possuía o entendimento que a legislação permitia o acesso de dados cadastrais, pois os dados do endereço de IP e outras informações, estariam incluídos nos dados cadastrais, dessa forma, dispensando a

necessidade de uma autorização judicial para acessar e consequentemente, permitia uma celeridade na investigação, devido a facilidade no acesso.

Segundo Bezerra e Agnoletto, (2019, p. 169), ressalta que apesar da Constituição Federal, estabelecer no artigo 5, inciso XII, o princípio da inviolabilidade da intimidade, sigilo de dados e comunicações que visam garantir a privacidade dos indivíduos, esta faz uma ressalva a vedação do anonimato, desse modo, os dados cadastrais não estariam protegidos pela proteção constitucional, pois essa abrange somente o conteúdo.

Conforme Jorge e Wendt, afirma as consequências devido tal dispositivo. (2012, p 180), que a necessidade de uma ordem judicial para obter qualquer informação relacionados a uma investigação de crime cibernético, in verbis, “O requisito de ordem judicial para obtenção de toda e qualquer informação relativa a um crime cibernético é outra questão que atravanca a investigação e representa uma das facetas do excesso de burocracia, que apenas prejudica e/ ou retarda o esclarecimento desse tipo de delito. [...]” desse modo, permitindo que os criminosos se beneficiem dos atrasos na investigação. (WENDT; JORGE, 2012, p. 180)

A importância de permitir a autoridade policial o acesso aos registros de acesso, sem obtenção de ordem judicial, é a única e fundamental forma de identificar os autores, desse modo, a exigência de sempre precisar dessa ordem, dificulta ainda mais os trabalhos dos órgãos de investigação, consequentemente, equivale à morte prematura da investigação, por falta de linha de investigação. (BERGMANN, 2020)

Outra problemática, é o armazenamento e o fornecimento das chamadas “portas lógicas", que permitem a identificação de usuários, quando há o compartilhamento de um mesmo endereço de IP com outros usuários, os provedores de aplicação alegam que pelo Marco Civil, não são obrigados a armazenar esses dados, pois o texto da lei não faz nenhuma menção às "portas lógicas”, desse modo, se recusam em fornecer tais informações para as autoridades. (BARRETO; KUFA; SILVA, 2021, p. 148)

O surgimento das portas lógicas decorre do rápido crescimento da Internet no Brasil, que possibilitou que diversos dispositivos se conectem a Internet, com isso houve o esgotamento de endereços de IPs utilizados pela tecnologia IPv4 (Internet Protocol versão 4), comum no país, diante disso, o Comitê Gestor da Internet permitiu que um mesmo IP fosse compartilhado com vários usuários, sendo identificados

somente pela porta utilizada que serão diferentes. (BARRETO; KUFA; SILVA, 2021, p. 148)

Apesar de já existir uma nova tecnologia, chamada de IPv6 (Internet Protocol versão 6), que criou novos endereços de IP, sendo capaz de suprir a demanda, os provedores de conexão estão realizando a transição de forma lenta, devido ao custo e a complexidade, sendo necessário que até que haja a migração, torna-se necessário que os provedores de aplicações fornecessem a porta lógica, que não acontece atualmente.

Conforme ensina Jorge (2020), em decorrência do impasse gerado pela a obrigatoriedade ou não de armazenar e fornecer as portas lógicas, há um comprometimento de uma investigação, pois não é possível individualizar de forma adequada o usuário responsável pelo acesso à Internet em decorrência de diversos usuários estarem usando o mesmo endereço de IP, consequentemente, permitindo o anonimato e a impunidades de criminosos que utilizam a Internet.

Conforme destaca Blum (2016), o legislador não é capaz de prever todas as evoluções da Internet, entre eles, o surgimento de compartilhamento dos IPs, porém, o Marco Civil prevê a obrigatoriedade de identificação como uma de suas finalidades, sendo necessário que ocorra a individualização dos usuários, e a obrigatoriedade no fornecimento dessas informações, desse modo, se ocorreu uma mudança na sistemática de identificação, as empresas devem se adaptar a essa nova conjectura para que estejam em conformidade com a Lei.

Segundo Zanin e Soares (2015, p. 5), fica evidente perceber que o Marco Civil da Internet foi extremamente excessivo, na questão da privacidade e proteção das informações dos usuários da internet, tal motivação apesar de aparentar somente o respeito à proteção da privacidade e dos direitos fundamentais, teria também outros motivos, o Projeto de Lei, teria sido realizado pelo Comitê Gestor da Internet no Brasil (CGI.br), formado por diversos membros, entre eles, representantes de empresas de Internet.

Diante disso, a presença e a força que os representantes dessas empresas possuem é grande no legislativo, ressaltando que a necessidade de atender as requisições de autoridades policiais em investigação, gera um maior custo para essas empresas, visto a necessidade de estrutura de armazenamento e prestação de serviço para as autoridades, ademais, a proteção do anonimato seria um fator

responsável por aumentar o lucro e a demanda pelo serviço. (ZANIN; SOARES, 2015, p. 5)

Nesse sentido, tal motivação de lucro é compartilhada pela Delegada Sabrina (MIRANDA, 2020), ratifica que há um interesse financeiro das empresas em não querer estruturar uma unidade com pessoal e recursos para atender às solicitações das autoridades policiais em tempo hábil. Desse modo, demonstrando o interesse somente no lucro, e não se importando com as responsabilidades decorrentes do seu ramo.

Segundo Zanin e Soares (2015, p. 7), o Marco Civil na questão de regulamentação da Internet foi uma notória evolução, porém em se tratando da investigação, foi um retrocesso. Alinhado com a falta de pessoal especializado e a grande quantidade de crimes cibernéticos, faz com que a escolha dos crimes que serão investigados seja baseada na relevância social do crime e na facilidade da obtenção de indícios de autoria e materialidade.

Ademais, conforme críticas de Bergmann (2020, p 37), a dificuldade criada nos acessos aos registros, demonstra a imaginação do legislador de que vivemos em um mundo distópico, no estilo George Orwell, “A corrente que prevaleceu durante a elaboração da Lei parte do pressuposto que as autoridades públicas estão a serviço de um Estado Totalitário e opressor dos direitos e liberdades individuais e por isso não deveriam ter acesso aos registros de acessos ou conexão. ”. Isso seria também decorrente da falta de conhecimento sobre os registros de acesso, e sua função.

Desse modo, denota se às dificuldades causados pelo Marco Civil na investigação de crimes cibernéticos, conforme expostos, a separação de dados cadastrais e registros de acessos, consequentemente causando problemas na obtenção de dados cadastrais, a impossibilidade de acesso ao endereço de IP diretamente pela autoridade, tornando necessário sempre o uso de ordem judicial, o impasse no entendimento sobre porta lógicas pelos provedores da obrigação de individualização imposta por lei, tais dificuldades demonstram os prejuízos causados pelo Marco Civil da Internet, em partes decorrentes do poder econômico das empresas do setor na criação da legislação.

Conclui-se, a necessidade do acesso aos dados cadastrais sem que haja a imposição de restrições pelos provedores, respeitando o poder de requisição das autoridades policiais previsto em lei, o acesso ao endereço de IP, com base no entendimento que é um dado cadastral, e não há violação da privacidade dos

usuários, e a necessidade de que os provedores forneçam as portas lógicas, enquanto não realizar a migração para a nova tecnologia, são formas de solucionar as dificuldades encontradas em uma investigação de crimes cibernéticos.

### 3.3 Dificuldades devido ao uso de criptomoedas em crimes cibernéticos

Um dos novos desafios na investigação de crimes cibernéticos é a popularização das chamadas criptomoedas ou criptoativos, que se assemelham as moedas digitais, fornecendo um meio de troca através de criptografia, sua essência basicamente permite a transferência de ativos de forma anônima, conforme exemplifica Ulrich (2014, p. 111), in verbis ” de forma geral, são uma forma de dinheiro, como as outras moedas existentes, destacando-se por ser totalmente eletrônicas e não ser controlada por um Banco Central.”, a Receita Federal adota o seguinte conceito para as criptomoedas;

> A representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal. (BRASIL, 2019)

Desse modo, as criptomoedas por serem um tipo de ativo virtual, se diferem das representações tradicionais de moedas, não possuindo status legal de moeda em curso na maioria dos países, em vez disso, o valor de troca da moeda virtual geralmente é baseado em um acordo ou a confiança entre uma comunidade na criptografia, desse modo, podendo ser convertidas em uma moeda real, possuindo assim o mesmo valor equivalente de uma moeda ou atuando como o substituto para uma moeda real. (FILHO, 2019)

O termo “criptomoedas’ se referem a qualquer tipo de moeda virtual, a grande maioria das criptomoedas são descentralizadas, ou seja, não dependem de um Banco Central para emiti-las, ou manter seus registros, utilizando somente uma blockchain, devido ao ser caráter inovador e único, atualmente existem milhares de criptomoedas, mas a maioria é semelhante, e possui como base a primeira criptomoeda, que foi totalmente implementada, o Bitcoin, que se tornou a mais popular. (ALVES; SILVA, 2018, p. 6)

O surgimento do Bitcoin ocorreu em 2008, quando uma pessoa, utilizando o pseudônimo de “Satoshi Nakamato” publicou um trabalho referente ao Bitcoin, descrevendo o funcionamento da rede, a privacidade, segurança, e expos a necessidade de uma moeda que não fosse controlada por Governos, e que realizasse sua própria regulação, tendo obtido sucesso em demonstrar sua importância e viabilidade. (ALVES; SILVA, 2018, p. 7)

Em geral as criptomoedas usam um sistema de redes conhecidas como “ponto a ponto” através de criptografia, para distribuir uma cópia para todos os participantes da rede, um “livro razão público” que possui todas as transações registradas e verificadas, este “livro razão” é conhecido como Blockchain que garante que as transações não sejam duplicadas, nem falsificadas, o seu uso significa que todas as transações são registradas publicamente, assim podendo garantir que Bitcoins não sejam "gastos duas vezes”, um antigo problema, que impediu que a tecnologia das criptomoedas surgisse antes. (GAMA, 2021, p. 33)

Ademais, o armazenamento das criptomoedas é realizada através de um par de chaves, a chave pública e a privada. A chave pública funciona como um endereço público dessa carteira, uma forma de receber recursos, já a chave privada é como se fosse a senha de acesso, devendo ser guardada em um lugar seguro, não podendo ser perdida ou exposta, visto que uma terceira pessoa pode utilizá-la para ter o controle da carteira e movimentar os ativos livremente de qualquer lugar do mundo. (GAMA, 2021, p. 32)

Como as criptomoedas não dependem do uso de instituições financeiras para realizar as transações, portanto, se tornam uma forma para os criminosos para financiar suas atividades ilegais, não há instituições oficiais envolvidas, órgão fiscalizador ou a possibilidade de as transações suspeitas serem detectadas, aumentando assim também as chances de roubos das moedas ou a sua perda, sem possibilidade de recuperação.

Nesse sentido, destaca Cintra (2020, p. 175)

> Frise-se, ainda não existe norma penalizante a respeito da posse e negociação de criptoativos ou de atividades acessórias como a mineração de criptomoedas. De fato, a simples posse ou negociação com criptomoedas, e também a atividade na mineração de criptomoedas não são ilícitos, O que se deve ser levado em consideração é o contexto probatório que as envolvem e como estão sendo empregadas [...]
> Embora o manuseio de criptoativos, a desrespeito dos riscos inerente, não seja ilegal, é forçoso reconhecer que criptomoedas podem ser instrumentalizadas na atividade criminosa assumindo, assumindo papel

> assessoria ou sucessivo a pratica de delitos, entender o contexto ao redor das evidencias será crucial para distinguir as situações fáticas como lícitas ou não e a partir daí adotar as medidas pertinentes de interesse da investigação criminal ou da instrução processual.

Desse modo, o uso das criptomoedas se torna extremamente atrativo aos criminosos devido ao menor risco de serem identificados durante uma transferência, o uso dessa nova tecnologia torna a resolução desses crimes mais complexo, decorrente de não deixar vestígios comuns que as autoridades policiais possam obter ou possuírem o treinamento adequado, além das dificuldades inerentes da investigação de crimes cibernéticos. (SHIMABUKURO, 2018, p. 70)

Segundo Andrade, (2017, p. 18), um dos usos dos criminosos para as criptomoedas é a lavagem de dinheiro que ocorre quando um indivíduo realiza ações para ocultar, dissimular a natureza, origem, ou movimentação, com o objetivo de evadir-se da fiscalização com o dinheiro obtido ilicitamente, de forma a dar impressão que os ativos são de origem lícitas.

Tradicionalmente, a lavagem de dinheiro era realizada através de transferências bancárias, empresas fantasmas e outros meios, porém, agora as criptomoedas estão substituindo as tradicionais formas de lavagem de dinheiro, dando aos criminosos uma forma de evitar deixarem uma trilha dos seus passos, tornando necessários que as autoridades se adaptem à nova realidade e criem novos meios de investigação. (ANDRADE, 2017, p. 19)

Conforme leciona, Cintra (2020, p. 173) as autoridades responsáveis por forças tarefas, já vem alertando sobre o uso das criptomoedas na lavagem de dinheiro;

> O GAFI/FATF (2014) já vem alertando as nações quanto ao grande potencial que as criptomoedas representam para a lavagem de dinheiro e para o financiamento do terrorismo. A descentralização do sistema, o acesso por dispositivos conectados à internet em qualquer lugar do planeta, a impossibilidade de se monitorar operações suspeitas, o anonimato e a conversibilidade em outras espécies de ativos, fazem das criptomoedas o ativo perfeito para a transferências ilícitas, para a evasão de divisas e para o branqueamento e ocultação de capitais. No mesmo sentido, a ENCCLA, desde 2017, vem pactuando e ações e meta com o foco em criptoativos, buscando aprofundar estudos e apresentar propostas de regulamentações e alterações legislativos para coibir seu uso criminoso.

Além das dificuldades naturais das criptomoedas, há o uso de websites de misturadores de criptomoedas, conhecidos como “Mixers” e “tumblers”, que são empresas que oferecem serviços que buscam dificultar a origem ou o dono das criptomoedas, funcionando como “lavanderias”, umas de suas características é não

solicitar dados pessoais, manter registros de conexão ou a comprovação de licitude da origem das criptomoedas. (ZUMAS, 2020)

Dessa forma, mediante o pagamento de uma taxa, o cliente pode enviar as criptomoedas para uma carteira específica de propriedade dos misturadores, que então, fazem o “embaralhamento” com as criptomoedas de outros usuários, antes de enviar para uma carteira nova, removendo assim os rastros anteriores de origem ou dono, permitindo a lavagem do dinheiro. (ZUMAS, 2020)

Há ainda a dificuldade na apreensão desses ativos, em decorrência da natureza digital das criptomoedas, somente as chaves que permitem acesso as carteiras podem estar no meio físico, e considerando que essas chaves das carteiras podem ser armazenadas em computadores, dispositivos removíveis, ou até mesmo em uma folha de papel, a autoridade durante a apreensão deverá localizar as chaves públicas e privadas, responsáveis por controlar a carteira, sem elas, não é possível realizar a apreensão dos ativos. (BRASIL, 2019)

Em caso de sucesso na localização das chaves, deve-se efetivar a apreensão de maneira rápida, enviando os ativos para outra carteira controlada pelo Estado, de forma a evitar que o próprio investigado ou conhecidos, que tenham cópias das suas chaves, movimentem para outras carteiras fora do controle do Estado, Portanto, criminosos poderiam esvaziar suas carteiras, antes que a polícia pudesse concluir as investigações, tornando ineficaz toda a apreensão e mantendo todo o patrimônio ilícito obtido, desse modo é necessário a compreensão das autoridades envolvidas para o êxito na apreensão. (BRASIL, 2019)

Há outras dificuldades que podem ser encontradas durante o caminho da investigação e podem não ser previsíveis pelas autoridades, é o que conclui Cintra (2020, p. 187):

> Advirta-se que, em situações práticas, outros obstáculos podem surgir como por exemplo, moedas virtuais desconhecidas ou novas, que não disponham de aplicações de código aberto para propiciar a imediata criação de carteiras e a realização de carteiras de transações para acautelar os valores em uma carteira segura, ou ainda, surgir a necessidade apreender equipamentos de informática ou de acessar serviços de terceiros armazenados em nuvem, Situações como estas necessariamente carecem de autorização judicial, para que não ocorra contaminação das provas colhidas e derivadas, e também para a preservação da cadeira de custodia.
> Em situações claras de usos de criptoativos, p. ex., uma pirâmide financeira, esses problemas podem ser antecipados e serem objetos de um provimento jurisdicional abrangente em caso de um mandando de busca, todavia, podem ocorrer situações em que acontecerá um encontro fortuito, p. ex, ao cumprir busca domiciliar em face de investigado por tráfico de drogas e a equipe

> descobre, no local da busca, que o alvo também negocia drogas na internet e recebe pagamento em bitcoins.

Conclui-se, o uso das criptomoedas está se tornando cada vez mais popular, em decorrência da sua natureza independente, por não serem controladas pelos bancos centrais dos países, ademais, ao contrário do dinheiro físico, no qual as autoridades policiais já estão acostumadas, o uso das criptomoedas desafiam essas autoridades, visto que um simples arquivo ou papel, pode conter as chaves de um patrimônio ilícito, sendo necessário o conhecimento técnico para identificar e localizá-las.

Desse modo, as autoridades devem ser manter bem informadas sobre as mudanças que estão surgindo, e as tecnologias que estão se popularizando, sendo essencial que essas autoridades se adaptem mais rapidamente às novas mudanças, o uso das criptomoedas apesar de estar em estágios iniciais de popularidade, sua expansão é cada vez mais certa, e o risco de serem usadas ainda mais em atividades criminosos.

# 4 MECANISMOS E SOLUÇÕES NO ENFRENTAMENTO DAS DIFICULDADES DE INVESTIGAÇÕES DOS CRIMES CIBERNÉTICOS.

A proposta deste capítulo, é de apresentar mecanismos e soluções que podem colaborar no processo de investigação dos crimes cibernéticos, nesse sentido, será destacado a importância do processo de adesão a Convenção de Budapeste, ratificado recentemente pelo Brasil, e as consequência dessa adesão para a investigação, ademais, serão apresentados mecanismos que facilitam o enfrentamento dos crimes cibernéticos, como a utilização da perícia digital, a prevenção através da educação digital, entre outras formas.

## 4.1 A importância e as consequências da adesão à Convenção de Budapeste para o aperfeiçoamento da investigação.

A Convenção de Budapeste (Decreto Legislativo nº 37), popularmente conhecido como “Convenção sobre o Cibercrime” foi um dos primeiros tratados internacionais sobre crimes cibernéticos, criado em 2001 pelo Conselho Europeu, tendo atualmente 66 países signatários, com o objetivo de padronizar a legislação, aumentando a capacidade de investigação e a cooperação entre os países signatários, visando aumentar a cooperação internacional, permitindo que seja realizado um combate adequado aos crimes cibernéticos em nível internacional e de forma integrada. (SILVA, 2013).

Uma das características do cibercrime é o seu caráter transnacional, podemos observar que neste novo mundo, com as pessoas cada vez mais conectadas, devemos dar a importância esse fato e buscar novas ferramentas que auxiliem a solucioná-los, tais questões já foram debatidas e incluídas na Convenção de Budapeste, que possui o compromisso em combatê-lo. (KUNRATH, 2017)

Nesse sentido, deve-se ressaltar o preâmbulo que destaca seu compromisso;

> Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes na presente Convenção; Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade do cibercrime, nomeadamente através da adopção de legislação adequada e do fomento da cooperação internacional; Conscientes das profundas mudanças provocadas pela digitalização, pela

> convergência e pela globalização permanente das redes informáticas; (Convenção de Budapeste, 2001)

Ademais, esclarece Brito (2013, np), referente aos objetivos principais da Convenção;

> A Convenção possui três objetivos específicos, a saber: (a) harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; (b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; (c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade informática.

A importância da convenção é reconhecida internacionalmente, por ter harmonizado diversas legislações sobre o tema, tipificando de formas objetivas diversos crimes e por ter estabelecido a possibilidade da cooperação internacional, segundo Kunrath, (2014, p. 87), devido ao progresso da internet desde a década de 80, houve a percepção da comunidade internacional de prevenir os crimes virtuais, visto que os governos e a sociedade dependiam cada vez mais do seu uso, o uso cada vez maior de transações bancárias e de cartões de créditos realizadas através da Internet, evidenciaram a necessidade de uma legislação especializada sobre o tema.

Conforme Cançado (2019, p. 99), a discussão e a negociação de um tratado iniciaram-se no ano de 1997 na Europa, devido a percepção do Conselho da Europa, uma organização internacional, que os crimes virtuais deveriam ser abordados de forma conjunta globalmente, em decorrência das diversas discussões, em 23 de novembro de 2001, na Hungria, foi criada a Convenção, sendo aberta para que países participasse da sua assinatura, antes de efetivamente entrar em vigor, que ocorreu somente em 1 de julho de 2004.

Conforme BRASIL, (2016, p. 322), os países que aderem a Convenção, possuem o dever de estabelecer a tipificação especificamente condutas ilícitas que são realizadas através da Internet, além de ser necessário adotarem políticas públicas estabelecidas no seu teor referente a cooperação, entre os países membros podem ser citado principalmente os países que compõe a União Europeia, além, do Canadá, Estados Unidos, Austrália, África do Sul, Argentina, Chile e outros.

Entretanto, apesar de sua relevância e a participação de diversos países, o Brasil não participou de sua elaboração, porém, tal fato não se trata de um impedimento, pois é permitido o ingresso de qualquer país, mediante convite,

possibilidade expressa na própria Convenção, no qual permite o Conselho da Europa, convidar qualquer país aderir a referida Convenção. (BUDAPESTE, 2001), diversos outros países já manifestaram interesse na participação ou estão em processo de adesão. Porém, enquanto o processo de adesão não ocorre, nada impede que os países criem ou aperfeiçoem sua legislação acerca do tema, sendo ratificado posteriormente a convenção. (SOUZA; PEREIRA, 2009).

Em 2019, o Brasil foi convidado pelo Comitê de Ministros do Conselho da Europa para aderir à Convenção, tendo o Brasil aceitado o convite e iniciado o processo para adesão através das providências legislativas necessárias. Devido a atrasos no procedimento de adesão, o Procurador-Geral da República, solicitou ao Presidente do Senado, agilidade na tramitação da ratificação, defendida desde 2011 pelo Ministério Público Federal. Em dezembro de 2021, houve a promulgação da Convenção por meio do Decreto Legislativo nº 37 de 2021 do Congresso Nacional. (BRASIL, 2021)

Segundo Jorge e Wendt (2012, p. 182), afirma a importância de o Brasil ser signatário da Convenção, pois o número de casos de criminosos ou informações vitais que permitiram solucionar a autoria do crime, estarão cada vez mais no exterior, dessa forma a cooperação internacional por meio da Convenção se torna fundamental para a busca da verdade, ou para que se alcance o esclarecimento de um crime e suas circunstâncias.

O Ministério Público Federal, em 2018, divulgou uma nota técnica em que apresentava em diversos pontos a importância da adesão do Brasil a Convenção, relatando os desafios encontrados no combate aos crimes cibernéticos tendo sido criados diversos grupos especializados para lidarem com o assunto e o aumento na quantidade de crimes cibernéticos praticados, destacando a migração dos crimes comuns, entre eles o estelionato, ameaças e extorsões, para os meios eletrônicos, (BRASIL, 2018)

A Convenção de Budapeste pode ser dividida em duas estruturas, a primeira que aborda as adequações necessárias que deverão ser realizadas pelos Países, os tipos penais que deverão ser criados, as providências de matéria processual, e principalmente, a segunda que trata da cooperação internacional, estabelecendo diretrizes para que os países firmem acordos de cooperação. (VERONESE, 2021)

Um dos principais pontos, é a obtenção de provas de crimes cibernéticos que se tornou algo essencial, assim como em outros crimes, conforme Nucci (2008, p. 172), é através das provas que buscamos a verdade, conhecida como material, real ou substancial, e os crimes na Internet geram diversas provas, nesse sentido, conforme afirma Bezerra e Agnoletto (2016, p. 176), in verbis “A Internet é um local de crime real, e portanto, deixa vestígios como registros de conexão à Internet, registros de utilização de serviços na Internet, [...] além, obviamente dos próprios computadores utilizados para a prática criminosa.”, sendo necessário que as autoridades possua os meios adequados para obtê-las.

Importante destaca que um dos benefícios também reside na questão da apreensão de computadores ou dispositivos eletrônicos, em que os dados são armazenados em servidores que estão localizados em outro país, existindo a dificuldade na obtenção da cooperação internacional onde estão localizados os servidores, criando uma demora ou a impossibilidade, a Convenção de Budapeste, possui instrumentos que facilitam essa cooperação.

Conforme o artigo 19 da Convenção, que descreve as medidas que devem ser adotadas, in verbis;

> Artigo 19.º – Busca e apreensão de dados informáticos armazenados
> 1. Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a efetuar buscas ou de outro modo aceder:
> a) A um sistema informático, ou a parte do mesmo, bem como aos dados informáticos nele armazenados; e
> b) A um suporte informático de dados que permita armazenar dados informáticos no seu território. (Convenção de Budapeste, 2001)

Nesse sentido, na nota técnica do Ministério Público Federal, foi apresentado a importância da Convenção na investigação na obtenção de provas, como sendo;

> Convenção do Cibercrime é útil não somente para a persecução de crimes cibernéticos, **mas principalmente para a obtenção de provas digitais que estão presentes em quase todos os delitos**. Nos casos em que o crime cometido extrapola a jurisdição brasileira, a obtenção dessas informações depende de cooperação internacional, que precisa ser ágil e eficiente a fim de que as provas não pereçam ou sejam omitidas. (BRASIL, 2018, grifo nosso)

Entre as consequências da adesão a Convenção, podemos citar a facilitação de troca de dados entre os países membros, visto que a cooperação é uma

das bases principais da Convenção, permitindo uma rápida troca de informações, fator importante quando se trata de crimes cibernéticos, considerando que podem ser praticados de qualquer lugar do mundo, essa troca de dados é necessária e vital, sendo explícita, no artigo 18 da Convenção. (JESUS; MILAGRE, 2016)

A realização de capacitações e treinamentos é um dos pontos presente na Convenção, permitindo a troca de técnicas de investigação, inovações legislativas e tecnológicas, segundo (BRASIL, 2018, p. 3), as Polícias Civis e os Ministérios Públicos encontram diversas dificuldades, sendo necessário urgentemente apoio tanto em conhecimentos, como em novas tecnologias, dessa forma, existem diversos projetos em andamento realizados através do escritório C-PROC, criado pelo Conselho da Europa, permitindo a capacitação desses profissionais envolvidos no combate aos crimes cibernéticos, com técnicas utilizadas ao redor do mundo.

No artigo 9, é abordado os crimes relacionados com a pornografia infantil, no qual estabelece que o termo “menor” abrange qualquer pessoa com idade inferior a 18 anos, permitindo, porém, que os países exijam um limite de idade inferior, que não poderá ser inferior a 16 anos, segundo FERNANDES, (2019, p. 190), tal limite de idade, apesar de aparentar ser genérico, supre uma brecha existente no artigo 241-D, do Estatuto da Criança e Adolescente, visto que por falha do legislador, tipificou somente a aliciação ou assedio contra crianças, deixando os adolescentes desprotegidos, e possibilitando que o criminoso fique isento de uma punição.

A definição da competência entre as partes, com base na cooperação, encontra-se presente no Artigo 22, que estabelece que as partes em casos de conflitos de jurisdição, deverão realizar uma consulta entre si para definir qual é a jurisdição mais adequada para a tramitação da ação penal, nesse sentido, o artigo 24 aborda a possibilidade de extradição desde que as infrações sejam puníveis na legislação das duas partes, possibilitando ainda, que a Convenção seja utilizado como fundamento legal para a realização da extradição, caso não haja nenhum tratado prévio de extradição entre as partes, facilitando a investigação e a consequente ação penal. (BEZERRA; SOBRAL, 2020)

No artigo 35, é previsto a criação da rede 24/7, no qual estabelece a obrigação dos países signatários da convenção em criar uma rede de atendimento mundial que funcione de forma ininterruptamente, possibilitando a solicitações a qualquer hora de pedidos de preservações de dados em outros países, permitindo

que as autoridades não percam os dados, enquanto obtém um pedido de cooperação formal. (BRASIL, 2016, p. 338)

Ademais, a obrigatoriedade da modernização da legislação, através da criação de novos tipos penais, com o objetivo de suprir lacunas existentes na legislação brasileira, e consequentemente a harmonização da legislação brasileira com a legislação dos países membros da convenção, facilitando sua cooperação e diminuindo os obstáculos existentes na investigação e a punição dos responsáveis. (KUNRATH, 2017)

Nesse sentido, outra consequência da adesão do Brasil é a necessidade de criminalizar a xenofobia e o racismo realizado através da Internet, considerando que atualmente não há punição específica no País para quem pratica tais crimes por meio de forma eletrônica, nesse sentido, conforme o Protocolo Adicional implementado na Convenção em 2003, este em seu preâmbulo dos artigos prever essa condição, “Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para tipificar, no seu direito interno, como infracção penal, quando praticada intencional e ilegitimamente, a seguinte conduta”, (BUDAPESTE, 2003), o artigo 5, do Protocolo Adicional, tipifica o insulto com motivação racista virtual e xenófoba, de forma mais específica que a legislação brasileira, permitindo o seu aperfeiçoamento.(CRESPO, 2011, p. 142)

Portanto, podemos concluir, que há inúmeros benefícios na adesão do Brasil a Convenção de Budapeste, e a outros tratados que versem sobre o tema, ademais, cabe ressaltar que, segundo Lopes, (2014) “A criação de tratados e convenções internacionais em matéria penal contribuiu de forma significativa para a diminuição dos empecilhos existentes pela diversidade de legislações entre os países, e possibilitou uma maior integração entre eles“. Ou seja, um combate eficiente dessa modalidade de crimes se faz necessária através da adesão aos Tratados e Convenções disponíveis sobre o assunto, sendo a Convenção de Budapeste uma ferramenta importante nessa questão.

### 4.2.1 MECANISMOS E SOLUÇÕES ADICIONAIS NO COMBATE AOS CRIMES CIBERNÉTICOS

## 4.2 A perícia digital como forma de garantia da cadeia de custódia

A perícia digital ou forense computacional é fundamental no contexto de combate aos crimes cibernéticos, devido a sua importância na realização dos exames periciais que são realizados nos vestígios deixados pelos criminosos, visto que é através da perícia que os indícios obtidos durante uma investigação, torna-se evidências digitais, que são fundamentais para a comprovação da materialidade um crime.

Conforme leciona Wendt (2013, p. 210), a lógica aplicada na perícia forense digital é a mesma de outras perícias forenses, pois utiliza-se o princípio conhecido como “troca de Locard”, no qual afirma que toda pessoa ao passar pela cena de um crime acaba deixando ou levando algo, desse modo, de forma semelhante, a pessoa ao cometer um crime cibernético acaba por deixar vestígios que podem ser encontrados, em computadores, pen drives, celulares, e outros dispositivos, consequentemente, permitindo que seja rastreado e identificado.

Dessa forma, segundo Pires (2003), a perícia forense pode ser definida da seguinte forma, “conjunto de técnicas, cientificamente comprovadas, utilizadas para coletar, reunir, identificar, examinar, correlacionar, analisar e documentar evidências digitais processadas, armazenadas ou transmitidas por computadores”, sendo uma sequência procedimentos importante na segurança das provas.

Nesse sentido, explica Carneiro (2017, p. 38)

> [...] as investigações de crimes cibernéticos demandam a perícia de informática com vestígios efetivamente deixados pela ação criminosa. Os computadores e mídias, nesses casos, contêm arquivos, registros de sistema, entre outras informações, que são evidências do crime e podem servir de prova material**. O exame pericial e o laudo produzido servirão de esclarecimento e convencimento para o juízo sobre o conteúdo ilícito**, tal como sobre o meio e método utilizados para se cometer o crime denunciado. (grifo nosso)

Segundo Patrícia Peck (PINHEIRO, 2013, p. 206), deve-se considerar que todas as investigações, incluindo as de crimes cibernéticos possuem como base a coleta de evidências ou informações, apesar da legislação brasileira não estabelecer uma hierarquia entre as provas, a prova pericial acaba tendo um valor maior comparado com as outras, em decorrência da sua base na fundamentação científica, que não depende de interpretações que possam ser subjetivas, sendo somente objetivas.

Segundo WENDT, BARRETO e CASELLI (2017, p. 237), um aspecto relevante, é a questão jurídica, pois para que haja a validação da evidência digital

exige-se que a técnica pericial permita preservar a capacidade da prova de forma a preservar sua autoria e integridade. Além disso, que haja possibilidade de realização de perícia e auditoria, sem, no entanto, esquecer do aspecto fundamental da segurança da informação.

Dessa forma, temos a chamada cadeia custódia, que é um processo projetado para registrar toda a história cronológica das evidências eletrônicas para garantir a sua completude, disponibilidade e idoneidade em todas as fases da perícia computacional, para que possa ser usado como prova em tribunal, com a utilização de procedimentos padrões de coletas que devem ser utilizados. (WENDT; JORGE, 2016, p. 192)

Em 2020, a Lei nº 13.964/2019, que alterou a legislação penal e processual pena, disciplinou a cadeia de custódia e as perícias em geral, em seu artigo 158-A, a sua definição;

> Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. (BRASIL, 2019)

Nesse sentido, Sousa destaca (2020, p. 173), a cadeia de custódia é fundamental na investigação dos crimes cibernéticos, visto que todo o trabalho realizado na investigação para obter uma determinada evidência digital, seria perdida, caso não fosse possível comprovar a metodologia utilizada na coleta, evitando afirmações de manipulações indevidas.

Dessa forma, a perícia forense deve ser promovida no Brasil, visto que é ponto fundamental no desenvolvimento da ação penal, sendo necessário garantir um maior investimento em seus recursos, incluindo através da contração de novos profissionais, e aumento do orçamento dos órgãos, com o objetivo de aumentar a qualificação das investigações criminais e consequentemente uma maior eficiência da atividade, a utilizações de experiência e boas práticas que são adotadas no Brasil e no exterior são meios necessários para estabelecer e consolidar mecanismos e procedimentos de forma a aprimorar a perícia forense no Brasil. (WENDT; JORGE, 2020, p. 201)

### 4.2.2 Prevenção dos crimes cibernéticos através da educação digital

Umas das principais formas de combate aos crimes cibernéticos, é através da prevenção, conforme, CRESPO afirma (2011, p. 115), quanto maior a educação dos usuários que utilizam a Internet, diminuírem a chance dos cibercriminosos se aproveitem das situações de riscos criadas por esses usuários, permitindo o amadurecimento e o conhecimento de usuários sobre os riscos que existem atualmente.

Nesse sentido, o Marco Civil da Internet em seu artigo 26, estabelece o dever do Estado na educação do uso consciente da Internet, devendo ser realizada em todos os níveis da educação do País, desse modo, o artigo 27, prevê a realização de iniciativas públicas de fomento à cultura digital, com foco na promoção da inclusão e redução das desigualdades. (BRASIL, 2014)

> Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.
> Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:
> I - promover a inclusão digital;
> II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso;
> III - fomentar a produção e circulação de conteúdo nacional.

Segundo entendimento KUNRATH (2017, p. 87), não é suficiente somente a elaboração de uma legislação que criminalize condutas ilícitas para a realização da persecução penal, sendo necessário que seja realizado uma política de prevenção aos crimes cibernéticos, tendo como base a educação, através da inclusão social e da melhoria da de vida, de forma a ensinar os cidadãos a prevenção, e formas segura de navegação na Internet.

Ademais, que a prevenção deve ter como foco a conscientização, sendo necessário a participação dos pais e das escolas nesse processo, como forma de alertar que não é suficiente não abrir a porta para estranhos, e sim os e-mails de estranhos, também não devem ser abertos. Além da utilização de cartilhas e materiais com foco na segurança digital e em boas práticas.

Conforme Patrícia Peck (PINHEIRO, 2013, p. 452) que compartilha o mesmo pensamento a educação digital dos usuários deve ser realizada na mesma medida da inclusão digital, como forma de ensinar aos mais velhos que estão tendo o primeiro contato com a tecnologia, bem como ensinar aos jovens, que nasceram

durante essa nova realidade de um mundo mais conectado, e que ainda estão em processo de aprendizado sobre ética e moral.

> Educar na sociedade digital não é apenas ensinar como usar os aparatos tecnológicos ou fazer efetivo uso da tecnologia no ambiente escolar. Educar é preparar indivíduos adaptáveis e criativos com habilidades que lhes permitam lidar facilmente com a rapidez na fluência de informações e transformações. É preparar cidadãos éticos para um novo mercado de trabalho cujas exigências tendem a ser maiores que as atuais. (PINHEIRO, 2013, p. 452)

O Ministério Público Federal, criou em 2015, o projeto “Ministério Público pela Educação Digital nas Escolas” um projeto realizado em parceria com outras organizações de educação digital, com foco na capacitação de agentes multiplicadores de conhecimento, através do incentivo à educação e a prevenção, como forma de ensinar as crianças e adolescentes o uso da internet da forma correta, além da forma adequada de encaminhamento de denúncias. (OLIVEIRA; MORGADO, 2018, p. 255)

No Brasil, há diversas organizações relacionada à educação digital, permitindo a conscientização dos usuários através de campanhas e recebimento de denúncias, como por exemplo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), mantido pelo Comitê Gestor da Internet no Brasil ou a SaferNet Brasil, uma associação civil sem fins lucrativos. (WENDT; JORGE, 2013. p. 241)

Para Wendt e Jorge (2013, p. 241), a conscientização é um processo de ensinamento, não devendo ficar restrita às organizações de prevenção e educação, cabe também as autoridades responsável pela repressão, sendo realizada quando estas detalham aos usuários, os tipos de crimes cibernéticos mais comum, a forma utilizada pelos criminosos para enganar as vítimas, permitindo que os usuários possam se proteger e não serem vítimas fáceis.

A conclusão que se chega até aqui é a de que a prevenção é uma das formas mais efetivas contra os crimes cibernéticos, a internet cada vez mais será ampliada, novas tecnologias surgiram e mais pessoas estarão conectadas, devendo esses novos usuários estarem preparados para os desafios presentes futuros, principalmente os jovens que deverão aprenderam a responsabilidade que existe no ambiente virtual e suas consequências na vida real.

### 4.2.3 Investimentos na capacitação e de integração entre os órgãos dos Estados.

Devido às características dos crimes cibernéticos de constante evolução, é necessário que haja sempre a necessidade de investimentos na capacitação dos profissionais que lidam com esse tipo de crime, a capacidade de compreender o funcionamento dos crimes cibernéticos é essencial, além do trabalho conjunto entre as autoridades responsáveis pelo combate.

Conforme leciona JORGE e WENDT (2013, p. 237), é necessário a integração entre os órgãos de investigação presentes no Brasil, através da criação de uma cultura de compartilhamento de informações sobre os criminosos virtuais, de forma a contrapor as atuações integradas que os criminosos possuem, além da centralização de investigações em um único departamento em cada Estado, permitindo a criação de uma atuação de forma padrão em um mesmo Estado, um exemplo adotado pelo Paraná, que apresentou resultados positivos na aplicação dessa metodologia.

Em 2012, a Lei 12.735/2012, conhecida como Lei Azeredo, em seu artigo 4, determina a criação de unidades especializadas no combate aos crimes cibernéticos pelos estados, “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. ” (BRASIL, 2012)

Segundo Jorge e Wendt (2013, p. 237), o Brasil em 2013, possuía delegacias especializadas somente nos estados do Rio de Janeiro, São Paulo, Minas Gerais, Pará, Rio Grande do Sul, Paraná, Espírito Santo, Sergipe, Piauí e Bahia, dessa forma, menos da metade dos estados brasileiros. Em 2017, a quantidade de delegacias alcançou 14 dos 27 estados, incluindo o Distrito Federal, um pequeno aumento, mas, ainda inferior à demanda necessária, que precisa ser ampliada para todos os Estados, de forma que a cooperação seja efetiva. (VIDAL; BALDISSERA, 2017)

Uma das alternativas na identificação de autores de crimes contra a honra na internet, é através de uma ação judicial, solicitando os dados do responsável pelo crime, porém, conforme BARRETO e BRASIL, (2016, p. 158), há falta de estrutura na maioria dos juizados que não possuem os meios técnicos ou conhecimento para

atender a demanda dos casos envolvendo crimes cibernéticos, sendo necessário a capacitação de forma permanente dos servidores, para conseguir compreender e solucionar o problema da vítima.

> [...] a falta de capacitação dos atores da persecução penal representa um grande desafio, na medida que pode impedir a punição dos cibercriminosos, e, por consequência, causar impunidade. **A capacitação deve ser realizada continuamente, por profissionais especializados, de modo que os órgãos da persecução possam reprimir e acompanhar a evolução desses crimes**. Os integrantes desses órgãos devem ser estimulados por políticas internas a participarem destas capacitações. Ademais, políticas públicas nacionais, voltadas aos órgãos de segurança pública, são bem-vindas e motivarão os estados a investirem na qualificação de seus quadros. (WENDT, JORGE, 2020, p. 200, grifo nosso)

Há ainda a necessidade de compreender as novas dificuldades presentes, como o uso dos criptomoedas em crimes cibernéticos e as formas adequadas de lidar-las, dessa forma, torna-se necessário que seja realizado investimento na capacitação de todos os agentes envolvidos, como forma de diminuir as consequências da expansão dos crimes cibernéticos, também por meio da ampliação da estrutura física da investigação de crimes cibernéticos se torna extremamente necessária.

### 4.2.4 Cooperação Internacional entre órgãos policiais

A cooperação internacional é uma importante ferramenta para contrapor as dificuldades encontradas no combate aos crimes cibernéticos, visto que não necessita de decisões judiciais ou do uso de mecanismos de cooperação penais tradicionais, como o MLAT, que podem levar meses para serem concluídas, sendo assim uma das formas mais célere de obter apoio nas investigações, permitindo garantir o enfrentamento aos crimes de forma rápida e efetiva, diversos Estados se uniram e surgiram organizações que visam garantir acesso a ferramentas e mecanismos para uma melhor investigação.

> A diminuição quase total dos limites fronteiriços para a prática criminosa ocasionou acrescente ampliação da delinquência transnacional. Isso fez com que as autoridades estatais responsáveis pela condução de investigações criminais, pela persecução e pelo julgamento de processos penais percebessem o consequente aumento da necessidade de obtenção de diligências e elementos probatórios no exterior, a fim de colaborar com a elucidação da autoria e materialidade de determinada conduta criminosa e com a apuração da verdade dos fatos. (SILVA, 2021, p. 203)

Nesse sentido, a cooperação entre os órgãos de investigação internacionais, é fundamental, visto que permite a obtenção de provas, identificação de testemunhas, intercâmbio de informações de inteligências, identificação e realização da oitivas de testemunhas, entre outras formas de cooperação, existem no mundo diversas organizações multinacionais policiais, como a Interpol (Organização Internacional de Polícia Criminal), Ameripol (Comunidade de Polícias das Américas) ou Europol (Agência da União Europeia para a Cooperação Policial), deve-se ressaltar que essas organizações não possuem todas as informações que são solicitadas para as investigações, apenas funcionam como intermediários, entre as diversas polícias existentes no mundo. (BARRETO; BRASIL, 2016, p. 82)

Atualmente, uma das maiores organizações e mais utilizada por todo o mundo, é a Interpol, idealizada em 1914, porém efetivamente, somente criada em 1923, com a participação inicial de 20 países membros, atualmente possui a participação de 186 países-membros, com escritórios regionais localizados em diversos países. (MELO, 2010, p. 4)

A INTERPOL, trabalha de forma integrada com os países membros, no qual providencia ferramentas e serviços para as atividades de investigação, por meio de capacitação, acesso a banco de dados e canais de comunicações, e outras formas de cooperação, no Brasil, todo o processo é realizado por intermédio da Polícia Federal, por meio do Serviço de Cooperação. (BARRETO; BRASIL, 2016, p. 82)

No estatuto da Interpol, em seu artigo 2º, dispõe sobre a função da instituição, que tem como base conseguir e desenvolver, a mais ampla assistência recíproca das autoridades de polícia criminal, além de estabelecer e desenvolver todas as instituições que podem contribuir para a prevenção e a repressão das infrações de direito comum. (BARRETO; BRASIL, 2016, p. 82)

Conforme destaca BLATT (2020, p. 8), a importância da cooperação entre os órgãos de investigações e a INTERPOL e suas consequências em uma investigação, como por exemplo o acesso a um banco de dados de pornografia infantil, que facilita a identificação de responsáveis por esses crimes, visto que os crimes cibernéticos podem ocorrer em qualquer país.

> A Interpol dispõe de uma excepcional base de dados internacionais com milhares de imagens sobre delitos contra menores, as quais têm sido enviadas por organismos encarregados da aplicação da lei em todo o mundo. Essa base de dados foi concebida para facilitar a identificação das vítimas e dos agressores. Permite centralizar os dados enviados por países membros

> e facilita a coordenação das investigações, evitando a duplicação de tarefas. Sua análise ajuda a localizar os produtores e distribuidores de imagens sobre delitos contra menores. (FILHO, 2014 apud BLATT, 2020, p. 8)

Diante o exposto, é possível observar a importância da cooperação internacional, considerando o aumento dos crimes cibernéticos no Brasil e no mundo, torna necessário o enfrentamento de organizações criminosas com atuação internacional, o apoio de organizações como a INTERPOL se torna essencial, devido às ferramentas e informações que providenciam.

# 5 CONCLUSÃO

Não há como negar os benefícios que a Internet trouxe na nossa sociedade, permitindo que as pessoas possam ter um maior acesso a informações, novos recursos e a comunicação entre as pessoas. Porém, o desenvolvimento da Internet, acabou por criar novos riscos a nossa sociedade, sendo utilizado também por criminosos que se utilizaram das características desse ambiente, que não possui limites físicos, para praticar diversos crimes, causando prejuízos que crescem a todo momento.

O desenvolvimento do presente estudo possibilitou compreender o processo de investigação dos crimes cibernéticos, além das dificuldades encontradas durante a investigação, devido as características inerentes do ambiente virtual, os mecanismos existentes atualmente não são suficientes para permitir que seja realizado um combate efetivo aos crimes cibernéticos, visto que não acompanharam a velocidade que esses crimes evoluíram.

Nesse sentido, foi apresentada umas das principais dificuldades encontradas durante a investigação, o uso do MLAT, que se tornou burocrático e excessivamente demorado para a obtenção de provas, criada em uma época que a Internet não era tão popular como os dias atuais, além das recusas das empresas estrangeiras em cumprir as ordens judiciais, exigindo o uso do MLAT para todas as solicitações, acaba por prejudicar as investigações no acesso as informações importantes.

Outra problemática, estão nas consequências do Marco Civil da Internet na investigação, que, não obstante ratificou o poder de requisição de dados cadastrais as autoridades, sem a necessidade de interferência do poder judiciário, conforme estabelecido em leis anteriores. Porém, o Decreto 8.771/16, que regulamentou artigo 11, §2 do Marco Civil da Internet, como forma de garantir o direito à privacidade, especificou que os dados cadastrais não incluíam o endereço de IP, tal alteração foi em sentido contrário ao que a jurisprudência entendia, que o endereço de IP estava incluindo nos dados cadastrais, que dispensava a necessidade de ordem judicial.

Consequentemente, devido a nova interpretação adotada pelo Marco Civil, a necessidade de obter o endereço de IP, somente através de ordem judicial, tornou a investigação mais lenta, visto que o endereço de IP é fundamental na identificação

dos criminosos virtuais e não possuí informação que viola a privacidade dos indivíduos, sendo apenas uma mera forma de identificação.

Ademais, foi apresentada as dificuldades encontradas devido ao uso das criptomoedas, que por oferecer a possibilidade do anonimato, favorecem o uso para a lavagem de dinheiro relacionado aos crimes cibernéticos, a falta de conhecimento na forma correta de apreensão desses ativos, que por serem digitais, podem ser movimentados para qualquer local do mundo, tornando necessário o conhecimento sobre a forma como funcionam.

Cabe ressaltar, que o presente trabalho não tem como objetivo apresentar todas as dificuldades encontradas durante uma investigação de crimes cibernéticos, mas somente algumas das mais comuns, que acabam por prejudicar a investigação, e consequente a identificação e punição dos responsáveis.

Nessa perspectiva, foi apresentada algumas das possíveis soluções para diminuir as dificuldades encontradas, como a importância e consequência da Convenção de Budapeste, que possibilitara o acesso mais rápido na obtenção de provas localizadas em servidores estrangeiros, e a necessidade de harmonizar a legislação brasileira com os requisitos da Convenção, consequentemente, melhorando a legislação.

Por fim, foi abordado mecanismos adicionais no combate aos crimes cibernéticos, que se tornam importantes para suprir as dificuldades, como a utilização da perícia digital para a garantia das provas, a prevenção através da educação, evitando o surgimento de mais vítimas, investimentos na capacitação e integração dos órgãos de investigação, e a utilização da cooperação internacional entre órgãos policiais. Conclui-se, a importância do conhecimento sobre como funcionam a investigação dos crimes cibernéticos, bem como as dificuldades encontradas, para que seja possível corrigi-las.

# REFERÊNCIAS

ALBERTO, Márcio. **A quebra do sigilo das comunicações telefônica. Combate as Organizações Criminosas**: 12.850 - A Lei que mudou o Brasil (Doutrina e Prática) / organizador: Clayton da Silva Bezerra / Giovani Celso Agnoletto. 1˚ ed. - São Paulo: Editora Posteridade, 2020.

ALBUQUERQUE, Paula Mary Reis de. **Exploração sexual de crianças e adolescentes na internet.** In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Pedofilia: repressão aos crimes de violência sexual contra crianças e adolescentes. Rio de Janeiro: Mallet, 2019.

ALVES, Alexandre Ferreira de Assumpção. SILVA, Priscilla Menezes. **Exequibilidade da penhora de criptomoedas no processo de execução brasileiro**. Revista de Processo, Jurisdição e Efetividade da Justiça | e-ISSN: 2525-9814 | Salvador | v. 4 | n. 1 | p. 70 – 90 | Jan/Jun. 2018.

ANDRADE, Mariana Dionísio de. **Tratamento jurídico das criptomoedas**: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017.

ARAUJO, Fábio Lucena de. **Aspectos Jurídicos no Combate e Prevenção ao Ransomware**. Revista do Ministério Público do Estado do Rio de Janeiro nº 71, jan./mar. 2019.

BRAIDA, Fernando Henrique Menezes da Silva. **Crimes cibernéticos: tipificação e legislação brasileira.** Conteúdo Jurídico, Brasília-DF: 11 maio 2020. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/54506/crimes-cibernticos-tipificao-e-legislao-brasileira. Acesso em

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet.** 1. ed. Rio de Janeiro: Brasport, 2016.

BARRETO, Alessandro Gonçalves. **Utilização de fontes abertas na investigação policial**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BARRETO, Alessandro Gonçalves. WENDT, Emerson; CASELLI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017.

BARROSO, Carolina Rodrigues de Carvalho. **Meios de investigação e produção de provas nos crimes cibernéticos**. Universidade Federal Fluminense, Niterói, 2019.

BERGMANN, Pablo Barcellos. **Aspectos penais do marco civil da internet**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime

cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BERNARDO, Felipe Henrique dos Santos. **Crimes cibernéticos e o que diz a nossa legislação.** Conteúdo Jurídico, Brasília-DF: 14 nov. 2016. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.57045&seo=1>. Acesso em: 21 abr. 2019.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao crime cibernético:** Doutrina e prática (A visão do Delegado de Polícia). 1ª Ed. Rio de Janeiro, 2020.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Considerações sobre investigação de crime de abuso sexual contra crianças e adolescentes e requisição de dados.** In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Pedofilia: repressão aos crimes de violência sexual contra crianças e adolescentes. Rio de Janeiro: Mallet, 2019.

BLATT, Erick Ferreira. **Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federa**l. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BLUM, Renato Opice. **Portas Lógicas de Origem: Identificação e caos jurídico**. Jota, 26 out. 2016. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/direito-digital-portas-logicas-de-origem-dificuldade-de-identificacao-e-o-caos-juridico-26102016> Acesso em:

BRASIL, **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. Agência Senado, 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico> Acesso em:

BRASIL, Coordenação-Geral de Repressão à Corrupção – CGRC, Polícia Federal. **Criptomoedas – Orientações gerais para equipes de busca**, 2019.

BRASIL, Ministério da Economia, Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa Nº 1.888, de 3 de maio de 2019**, Diário Oficial da União, 2019. Disponível em: https://www.in.gov.br/web/dou/-/instru%C3%87%C3%83o-normativa-n%C2%BA-1.888-de-3-de-maio-de-2019-87070039. Acesso em:

BRASIL, Projeto de Lei do Senado n° 76, de 2000, **Define e tipifica os delitos informáticos, e dá outras providências.** Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/43555 > Acesso em

BRASIL. Código Penal Brasileiro**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm. Acesso em:

BRASIL. Decreto nº 3.810, de 2 de maio de 2001**. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997,** corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm> Acesso em:

BRASIL. Lei nº 12.965, de 23 de abril de 2014**. Estabelece Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em:

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2**. Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília, DF: Ministério Público Federal, 2016.

BRASIL. Ministério Público Federal. **Nota técnica do grupo de apoio sobre criminalidade cibernética sobrea convenção do cibercrime** (Convenção de Budapeste). 2018. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf>. Acesso em**:**

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 55.109-PR.** Relator: Ministro Reynaldo Soares da Fonseca. Brasília, DF, 07 de novembro de 2017. Brasília, DF. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201702152566&dt_publicacao=17/11/2017>. Acesso em:

CANÇADO, Hazenclever Lopes. **A pedofilia na era digital e sua tipificaçã**o. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Pedofilia: repressão aos crimes de violência sexual contra crianças e adolescentes. Rio de Janeiro: Mallet, 2019.

CARNEIRO, Márcio Rodrigo de Freitas. **Perícia de informática nos crimes cibernéticos.** In: BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. Investigação e prova nos crimes cibernéticos: Caderno de Estudos. - São Paulo: EMAG, 2017,

CARNEIRO, Tácio Muzzi Carvalho. JUNIOR, Isalino Antonio Giacomet. Ministério da Justiça e Segurança Pública. Departamento de Recuperação de Ativos e Cooperação Jurídica. **Ofício 28725/2017 – DRCI**. Brasília, DF. 20 fev. 2018. Cooperação Jurídica Internacional em Matéria Penal entre Brasil e EUA para fins de de afastamento de sigilo telemático. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379> Acesso em:

CARVALHO, Gabriel Chiovetto. **Crimes Cibernéticos**. Conteúdo Jurídico, Brasília-DF: 12 jun. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. Acesso em:

CASSANTI, Moises de Oliveira Cassanti. **Crimes Virtuais, Vítimas reais**. São Paulo: Brasport. 2014.

CASTRO, Ana Lara Camargo. Crimes cibernéticos e óbices ao cumprimento do acordo de cooperação internacional (MLAT) com base nos standards de causa provável e liberdade de expressão do Direito estadunidense. In: **Revista do Ministério Público do Estado do Rio de Janeiro**, nº 76, p. 19-49, abr./jun, 2020

CERQUEIRA, Silvio Castro; ROCHA, Claudionor. **Crimes cibernéticos: desafios da investigação**. Cadernos Aslegis, 2013. Brasília, DF. Disponível em: <http://bd.camara.gov.br/bd/handle/bdcamara/27420>. Acesso em:

CINTRA, Luciano Henrique. **Criptomoedas: Noções Elementares e Soluções práticas para Investigadores Criminais**. In: Tratado de Investigação Criminal Tecnológica. Higor Vinicius Nogueira Jorge, Salvador: Editora Juspodivm, 2020.

Convenção sobre o Cibercrime. **Convention on Cybercrime**. 23 Novembro de 2001. Disponível em: <https://rm.coe.int/16802fa428> Acesso em:

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

DOMINGOS, Fernanda Teixeira Souza Domingos; RÖDER, Priscila Costa Schreiner. **Obtenção de provas digitais e jurisdição na Internet. In: BRASIL. EMAG. Investigação e prova nos crimes cibernéticos**. Cadernos de Estudos, São Paulo, v. 1, p. 55-84, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em:

FERNANDES, David Augusto. **A internet: como brincar, estudar e navegar com segurança, evitando a ação dos pedófilos nas redes sociais**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Pedofilia: repressão aos crimes de violência sexual contra crianças e adolescentes. Rio de Janeiro: Mallet, 2017.

FERNANDES, Fernanda Santos**. Pedofilia Virtua**l. In: Direito penal e segurança pública / organizadores Andrija Almeida, Antonio Santoro, Regina Berardi. – Rio de Janeiro: Ágora21, 2018.

FERNANDES, Fernando Santos. **"Fake news" e suas consequências**. In: Combate às Fake News / organizador: Clayton da Silva Bezerra / Giovani Celso Agnoletto 1 ed. - São Paulo: Editora Posteridade, 2019

FILHO, Marcelo de Castro Cunha. Bitcoin: uma tentativa de construção da confiança por meio da tecnologia. Revista de Informação Legislativa: RIL, Brasília, DF, v. 56, n. 221, p. 37-60, jan./mar. 2019.

GAMA, Filype Rodrigues. **Sistema financeiro nacional e a regulação das criptomoedas.** Dissertação (mestrado) – Centro Universitário Alves Faria (UNIALFA) - Mestrado em Direito – Goiânia, 2021. Disponível em:

<http://tede.unialfa.com.br/jspui/bitstream/tede/390/2/FILYPE%20RODRIGUES.pdf> Acesso em:

IMAY, Maurício Chouity; GARCIA, Flúvio Cardinelle Oliveira. **A resistência dos provedores de aplicações de Internet no fornecimento de algumas informações relevantes à investigação criminal**. Caderno da Escola Superior de Gestão Pública, Política, Jurídica e Segurança. Curitiba, v. 4, n. 1, p. 5-32, jan./jun. 2021

JESUS, Damásio de. MILAGRE, José Antonio**. Manual de crimes informáticos,** São Paulo: Saraiva, 2016.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica.** Rio de Janeiro: Brasport, 2018.

JUNIOR, Janio Konno. Dados Cadastrais e Dados Pessoais na Investigação Criminal. **Revista Eletrônica Direito & TI**, v. 1, n. 12, p. 7, 13 jun. 2020.

NAVAS JUNIOR, José. **"STALKING**". In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no cyberespaço**. Feira de Santana: Universidade Estadual de Feira de Santana, 2017.

LEITE, Aderson Vieira. **Encaminhamento de Requerimento nº 718/12**, Brasília, DF, 2012. Disponível em: http://www.senado.gov.br/comissoes/documentos/SSCEPI/Vega1358.pdf. Acesso em:

LESSA, Isabella Maria Baldissera; VIEIRA, Tiago Vidal. **Crimes virtuais: análise do processo investigatório e desafios enfrentados**. 5° Simpósio de Sustentabilidade e Contemporaneidade nas Ciências Sociais. 2017, Toledo, p.1-25, 21 a 23 jun. Anais eletrônicos. 2017, Toledo. Disponível em:https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf. Acesso em

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** Monografia (Graduação) - Curso de Direito da Universidade Federal do Ceará, Fortaleza, 2017. Disponível em:

MELO, Inaldo Gomes**. Polícia Federal Internacional: A Polícia Criminal Internacional e a Interpol/Brasil - constituição e objetivo**. Brasília, v. 3, n. 2, p. 15-42, jul./dez. 2010. Disponível em: https://periodicos.pf.gov.br/index.php/RSPC/article/view/99. Acesso em:

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica**, 2012. Disponível em <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-

juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em 20 de abr de 2019.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernético sno Ordenamento Jurídico Brasileiro e a Necessidadede Legislação Específica**. Disponível em <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em

MIRANDA, Sabrina L de Lima. Congresso Brasileiro Sobre Polícia Judiciaria, 2020, Online. **Investigação Policial em Crimes Cibernéticos** [...]. [*S. l.*: *s. n.*], 2020.

NUCCI, Guilherme de Souza, **Manual de processo penal e execução penal**, 4 ed. Rev. Atual. e ampl – São Paulo: Editora Revista dos Tribunais, 2008.

OLIVEIRA, Neide M. C. Cardoso de; MORGADO, Marcia. Projeto "ministério público pela educação digital nas escolas". In: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2**. Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília, DF: Ministério Público Federal, 2016.

PEREIRA, Jeferson Botelho. Lei n.º 12.830/2013: as garantias do delegado de polícia. **Jus Navigandi**, Teresina, ano 18, n. 3648, 27 jun. 2013. Disponível em: https://jus.com.br/artigos/24795/lei-n-12-830-2013-as-garantias-do-delegado-de-policia. Acesso em:

PINHEIRO, Patrícia Peck**. Direito digita**l. 5. ed. São Paulo: Saraiva, 2013.

PIRES, Paulo Sergio da Motta. **Forense computacional:** uma proposta de ensino, 2003. Disponível em: http://www.leca.ufrn.br/~pmotta/ensino-forense.pdf. Acesso em:

ROSSINI, Augusto Eduardo de Souza**. Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004.

SANTOS, Coriolano Aurélio de Almeida Camargo. **Crimes previstos no estatuto da criança e do adolescente.** In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Pedofilia: repressão aos crimes de violência sexual contra crianças e adolescentes. Rio de Janeiro: Mallet, 2019

SANTOS, Rosangela Dos. **Criminalidade digital em tempos de pandemia: principais ocorrências em Sergipe no ano de 2020**. Monografia (Graduação) – Curso de Direito da Universidade Federal De Sergipe, São Cristóvão, 2020.

SHIMABUKURO, Adriana. **As investigações na era das moedas digitais**. In: Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

SIENA, David Pimentel Barbosa de. Lei Carolina Dieckmann e a definição de “crimes virtuais”. **Revista Jus Navigandi,** ISSN 1518-4862, Teresina, ano 18, n. 3652, 1 jul. 2013.

SILVA, Guilherme Brianez da; SILVA, Ricardo da Silveira. **Da investigação criminal no âmbito digital: os limites para se investigar e produzir provas em crimes virtuais no Brasil.** XI EPCC, Anais Eletrônico, 2019. Disponível em: <https://rdu.unicesumar.edu.br/bitstream/123456789/3784/1/Guilherme%20Brianez%20da%20Silva.pdf>. Acesso em:

SILVA, Marcelo Mesquita. BARRETO, Alesandro Gonçalves. KUFA, Karina. **Cibercrimes e Seus Reflexos No Direito Brasileiro.** São Paulo**:** Juspodivm, 2021

SOARES, Valeska Maria Capelasso; ZANIN, Fabrício Carlos. **Marco civil da internet (lei 12.965/2014): a interpretação do endereço IP e suas implicações no ordenamento jurídico penal brasileiro**. Jus Societas, Ji-paraná, n. 13, p.21-30, jan./jun. 2015. Disponível em: <http://www.periodicos.ulbra.br/index.php/jsoc/article/view/2138>. Acesso em:

SOBRAL, Carlos Eduardo Miguel e BEZERRA, Clayton**. Introdução ao estudo do crime cibernético.** In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

SOUZA, Carlos Affonso de Souza. Como as autoridades encaram o acesso a dados na internet para investigações, **Tilt Uol,** 2020. Disponível em: http://tecfront.blogosfera.uol.com.br/2020/02/18/como-as-autoridades-encaram-o-acesso-a-dados-na-internet-para-investigacoes/. Acesso em:

SOUZA, Carolina Yumi de. **Cooperação Bilateral Brasil – EUA em Matéria Penal: Alcançando o Devido Processo**. Tese de Doutorado – Curso de Direito da Universidade de São Paulo, São Paulo, 2015. Disponível em:

SOUZA, Stenio Santos. **Busca e apreensão virtual: evidências digitais em nuvem computacional**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Busca e Apreensão: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo. **Stalking e cyberstalking.** São Paulo: Juspodivm, 2021.

SILVA, Wanessa Rezende. **Cooperação jurídica internacional em matéria penal**. In: Técnicas avançadas de investigação / organizadores: Galtiênio da Cruz Paulino, João Paulo Santos Schoucair, Octahydes Ballan Junior, Tiago Dias Maia. – Brasília: ESMPU, 2021.

TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico, Doutrina, Jurisprudência e prática**. São Paulo. Editora: Saraiva. 2015.

ULRICH, Fernando**. Bitcoin - A Moeda na Era Digital**. 1. ed. São Paulo: Instituto Ludwig Von Mises. Brasil, 2014

VALENTE, Fernanda. Para Moro, cooperação jurídica com EUA para produzir provas é muito demorada. **Revista Consultor Jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-fev-10/cooperacao-juridica-eua-produzir-provas-demorada. Acesso em:

VECCHIA, Evandro Della. **A fronteira entre a investigação e a perícia digital**. Revista Eletrônica Direito & TI, v. 1, n. 1, p. 4, 16 set. 2015. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/17. > Acesso em:

VELLOSO, Jean Pablo Barbosa. **Crimes Informáticos e Criminalidade Contemporânea.** Out. 2015. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=15756>. Acesso em:

VERSIANI, José Augusto Campos. **Cooperação internacional na investigação de crimes cibernéticos**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013

WENDT, Emerson; BARRETO, Alessandro Gonçalves**. Marco Civil da Internet e Acordos de Cooperação Internacional:** Análise da Prevalência pela Aplicação da Legislação Nacional aos Provedores de Conteúdo Internacionais com Usuários no Brasil. **Revista Eletrônica Direito & TI**, v. 1, n. 1, p. 5, 28 out. 2015.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Perícia computacional e investigação de delitos informáticos: importância e desafios.** In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia). 1. ed. Rio de Janeiro: Mallet Editora, 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

ZUMAS, Vytautas Fabiano Silva. **Criptomoedas, criptocrime e criptoinvestigação**. DireitoNet. 08 de maio de 2020. Disponível em:https://www.direitonet.com.br/artigos/exibir/11637/Criptomoedas-criptocrime-e-criptoinvestigacao. Acesso em:

# ANEXOS

**ANEXO A –** Resposta do Whatsapp por e-mail

Prezados,

Obrigado por sua solicitação ao WhatsApp. Recebemos seu pedido para fornecimento de informações.

Com base nas informações fornecidas, acreditamos que a situação não atende aos critérios aplicáveis para divulgação.

Ressalvadas limitadas exceções, o WhatsApp só poderá produzir informações em resposta a ordens judiciais. As limitadas exceções nas quais o WhatsApp pode produzir informações disponíveis sem uma ordem judicial são as seguintes:

Primeiramente, o WhatsApp fornecerá informações básicas de usuário à polícia sem ordem judicial em determinadas circunstâncias, dentre as quais quando o requerimento policial indicar expressamente que a investigação em curso relaciona-se a (i) crime previsto na Lei de Organizações Criminosas (Lei Federal n. 12.850/2013); (ii) crime previsto na Lei de Lavagem de Capitais (Lei Federal n. 9.613/1998); (iii) pornografia infantil; (iv) sequestro ou cárcere privado; (v) redução a condição análoga à de escravo; (vi) tráfico de pessoas; (vii) extorsão mediante sequestro; (viii) extorsão qualificada; (ix) tráfico internacional de criança ou adolescente; ou (x) terrorismo. Por gentileza, note que é necessária uma ordem judicial para disponibilização dos endereços de IP dos usuários.