A IMPORTÂNCIA DA CRIAÇÃO DE UM SISTEMA DE COOPERAÇÃO INTERNACIONAL EFICAZ NO COMBATE AOS CRIMES CIBERNÉTICOS

THE IMPORTANCE OF CREATING AN EFFECTIVE INTERNATIONAL COOPERATION SYSTEM IN THE FIGHT AGAINST CYBERCRIME

Diego Bini, Fatec Ministro Ralph Biasi - Americana,
diego.bini@fatec.sp.gov.br
Henri Alves de Godoy, Fatec Ministro Ralph Biasi - Americana,
henri.godoy@fatec.sp.gov.br

Resumo

A informação transformou-se, atualmente, em um ativo de elevadíssimo valor e a segurança da informação possui o árduo mister de garantir que as informações permaneçam imunes às mais variadas espécies de ataques e violações. No entanto, esses ataques ocorrem diuturnamente e, muitas vezes, adentram à esfera criminal, devido à extrema gravidade dessas condutas e muitos são os artifícios utilizados para o cometimento dos denominados crimes cibernéticos, bem como para a ocultação da identidade dos criminosos e impunidade desses crimes. A transnacionalidade do crime cibernético é um dos subterfúgios mais utilizados pelos cibercriminosos para se manterem na clandestinidade por haver muitos empecilhos legais que atrapalham a investigação desses crimes quando perpassam por mais de um país, sendo que um dos maiores entraves é, justamente, a falta de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos. A metodologia utilizada neste trabalho foi a revisão bibliográfica. O objetivo deste trabalho é demonstrar que a criação desse sistema que funcione eficazmente pode contribuir sobremaneira para o esclarecimento dos crimes cibernéticos que assolam o Brasil e o mundo.

Palavras-chave: Segurança da Informação, Crimes Cibernéticos, Sistema de Cooperação Internacional Eficaz.

Abstract

Information has now become an asset of very high value and information security has the arduous task of ensuring that information remains immune to the most varied types of attacks and breaches. However, these attacks occur daily and often enter the criminal sphere, due to the extreme gravity of these conducts and many are the devices used to commit the so-called cybercrimes, as well as to conceal the identity of the criminals and impunity of these crimes. The transnationality of cybercrime is one of the subterfuges most used by cybercriminals to remain underground, because there are many legal obstacles that hinder the investigation of these crimes when they pass through more than one country, and one of the biggest obstacles is, precisely, the lack of an effective international cooperation system in the fight against cybercrime. The methodology used in this study was the literature review. The objective of this work is to demonstrate that the creation of this system that works effectively can contribute greatly to the clarification of cyber crimes that plague Brazil and the world.

Keywords*: Information Security, Cybercrimes, Effective International Cooperation System.*

1. Introdução

A preocupação com a Segurança da Informação vem crescendo bastante nos últimos anos, pois a informação constitui atualmente um dos ativos mais valiosos e, como tudo que possui valor, a informação passou a ser alvo de ataques, com as mais variadas finalidades. Existem várias formas de realizar ataques às informações – engenharia social, *ransomwares*, por exemplo, sendo que como consequência, a Segurança da Informação tem que se valer de todos os artifícios disponíveis para garantir ou tentar garantir que as informações não sejam violadas.

Em alguns casos, de maior gravidade, as violações das informações podem constituir crimes, os denominados crimes cibernéticos, os quais podem ser executados das mais diferentes formas, tendo em vista os inúmeros artifícios digitais que existem para tanto e, aliado à falta de conhecimento de muitas vítimas e, não raro, até mesmo das autoridades incumbidas da repressão dos mencionados crimes, muitas vezes eles permanecem impunes. Neste trabalho foram analisadas algumas modalidades de ataques e crimes cibernéticos, bem como alguns aspectos da investigação de tais crimes e uma das maiores dificuldades constatadas durante a investigação dos crimes cibernéticos, precipuamente os mais graves, como, por exemplo, os crimes de abuso e exploração sexual infantil, tráfico de drogas e tráfico de armas, que é a falta de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos, haja vista que muitas vezes a morosidade ou até mesmo a falta desse mecanismo conduz ao insucesso das investigações e à impunidade do cibercriminoso.

O objetivo desse trabalho, portanto, é demonstrar a necessidade da criação de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos, haja vista que

em abril do corrente ano o Brasil se tornou signatário da Convenção de Budapeste, que trata dos crimes cibernéticos e temas correlatos. Com a criação e o funcionamento, de forma eficaz, esse sistema de cooperação internacional de combate aos crimes cibernéticos, certamente, auxiliará grandemente no esclarecimento de vários crimes cibernéticos ocorridos no Brasil e pelo mundo.

2. Referencial Teórico

Será desenvolvida nesta oportunidade a base teórica do presente trabalho, com fulcro num estudo de revisão bibliográfica de fontes diversas, visando conduzir o leitor ao conhecimento de quais são as bases da segurança da informação, quais as características e espécies de crimes cibernéticos, alguns aspectos da investigação dos crimes cibernéticos, bem como a demonstração da necessidade da criação de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos para que a repressão aos mais graves crimes dessa espécie não permaneça prejudicada.

2.1. Segurança da Informação

A informação sempre foi de grande importância no que tange aos grandes feitos da humanidade. Isto fica evidente quando um inventor necessita registrar a patente de uma invenção, uma montadora de automóveis mantém em segredo um modelo novo de veículo ainda a ser lançado, nas grandes organizações que movimentam a economia mundial, assim como num momento beligerante onde as nações envolvidas escondem e dissimulam suas táticas de guerra para confundir o inimigo. Como afirma Sun Tzu (2019, p.47): “Conhece-te a ti e ao teu inimigo, e em cem batalhas que sejam, nunca correrás perigo”. Analisando mais detidamente os dizeres de Sun Tzu, o que seria conhecer a ti e ao teu inimigo, senão obter informações assertivas acerca de ambos.

Atualmente, a importância da informação alcançou um patamar elevadíssimo, tendo em vista os avanços tecnológicos e o, consequente, tráfego massivo das mais variadas espécies de informações verificado, diuturnamente, por meio da Internet. Consequentemente, a Segurança da Informação também adquiriu grande relevância hodiernamente e conforme escrevem Baars, Hintzbergen, Smulders e Hintzbergen (2018, p. 37-41) a Segurança da Informação possui três pilares, também chamados de princípios fundamentais, quais sejam: a confidencialidade, a integridade e a disponibilidade. A confidencialidade se refere à propriedade na qual a informação não deverá ser disponibilizada ou divulgada para quem não estiver autorizado, ou

seja, as informações somente devem ser visualizadas por pessoas, entidades ou processos autorizados. A integridade garante a proteção, a exatidão e a integridade das informações, isto é, as informações não serão indevidamente alteradas. A disponibilidade garante que as informações possam ser acessadas e utilizadas a qualquer momento, ou seja, mesmo diante das diversas intempéries a que estão sujeitas, as informações deverão estar disponíveis sempre que precisarem ser acessadas.

Destarte, esses pilares devem estar sempre protegidos de forma que a informação mantenha seu valor. Todavia, existem ainda, outras propriedades da segurança da informação que, apesar de não serem consideradas, pilares possuem grande importância no concernente à segurança da informação, e precisam estar presentes para a informação manter seu valor, são elas a autenticidade, é a capacidade de uma entidade ser o que afirma que é, a responsabilidade, vista como a atribuição de ações e decisões a uma entidade ou pessoa, o não repúdio, considerada a habilidade de provar a ocorrência de um evento ou ação e sua origem, e a confiabilidade, vista como propriedade de consistência dos comportamentos e resultados desejados.

Conforme se observa acima, a segurança da informação precisa garantir que as informações se mantenham em conformidade com os vários pilares ou princípios e propriedades acima mencionados, dentre outros, sendo que essa tarefa não é fácil, pois muitos são os artifícios utilizados no intuito de violar os pilares e propriedades da segurança da informação com as mais variadas finalidades. Importante diploma legal que passou a balizar o tratamento de dados, é a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual prescreve em seu primeiro artigo (BRASIL, 2018):

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Importante neste momento fazer, de maneira breve, uma análise do surgimento e do avanço da Internet, no contexto da globalização, e seus impactos na segurança da informação e nos crimes cibernéticos.

Conforme escrevem Barreto, Kufa e Silva (2022, p. 36): “A globalização consiste em um complexo processo de estreitamento das relações sociais, culturais, políticas e, especialmente, econômicas no mundo”.

Explanam, ainda, Barreto Kufa e Silva (2022, p. 36-37) que não existe consenso acerca de qual é o marco inicial da globalização, havendo aqueles que enxergam esse início no ano de 1914, com o surgimento de novas tecnologias como trens, ferrovias e telégrafo. Alguns autores apontam como marco inicial da globalização o final da Segunda Guerra Mundial.

Em que pese tais opiniões divergentes acerca do marco inicial da globalização, um fato irrefutável é que a rede mundial de computadores, conhecida como Internet, proporcionou um avanço extremo para todo o mundo, haja vista a possibilidade de comunicação sem fronteiras criada pela famigerada rede mundial de computadores e acelerou, sobremaneira, o fenômeno da globalização.

A Internet, consoante escrevem Wendt e Jorge (2021, p. 27-30), surgiu em decorrência da evolução da rede de comunicações denominada ARPANET, a qual foi acionada no ano de 1969, a qual, inicialmente interligava a Universidade da Califórnia, a Universidade de Stanford e a Universidade de Utah e, com o decorrer dos anos a mesma cresceu e na década de 80 a ARPANET se disseminou pelos Estados Unidos interligando universidades, órgãos militares e governo, até que no ano de 1986 a ARPANET começou a ser chamada de Internet que, posteriormente, com a criação da rede "Word Wide Web" foi possível a expansão e a utilização comercial da Internet. No Brasil não foi diferente, a Internet chegou e sua evoluiu rapidamente, sendo que no ano de 1992 foi implementada a primeira rede conectada à Internet, ligando as principais universidades brasileiras que, através da famigerada rede, apenas conseguiam trocar e-mails. Entretanto, no ano de 1995 iniciou-se o uso comercial da Internet no Brasil.

Importante salientar a importância da Internet atualmente, haja vista que por meio da rede mundial de computadores as pessoas enviam e recebem mensagens, se ocupam com entretenimento, efetuam transações financeiras dentre tantas outras atividades e todos esses dados trafegam pela Internet livremente contendo informações da quase totalidade dos cidadãos brasileiros, pois segundo pesquisa realizada pelo (IBGE, 2022), a Internet já é acessível em 90,0% dos domicílios do país em 2021.

A Internet, como explicitado acima, foi um avanço muito grande para a humanidade, porquanto eliminou barreiras geográficas, facilitou diversas ações e a cada dia se aprimora mais, no entanto, juntamente com todo esse avanço também se verifica a crescente utilização dessa tecnologia para condutas desviadas e muitas vezes criminosas, o que fez com que se desenvolvesse todo um arcabouço na área da Segurança da Informação, bem como na esfera

criminal, por meio das leis penais, com vistas a proteção das informações dos usuários da rede mundial de computadores.

2.2. Dos Crimes Cibernéticos

Para iniciar o estudo dos crimes cibernéticos, mostra-se necessário conceituar o que é crime. Segundo Jesus (2003, p. 150): "Materialmente, tem-se o crime sob o ângulo ontológico, visando a razão que levou o legislador a determinar como criminosa uma conduta humana, a sua natureza danosa e suas consequências".

No tocante aos crimes cibernéticos, várias são as nomenclaturas utilizadas para designar os mesmos, tais como crimes virtuais, crimes de alta tecnologia, crimes de informática, crimes tecnológicos, dentre outros. No entanto, nesse trabalho adotaremos a nomenclatura crimes cibernéticos, haja vista ser a que melhor se amolda ao tema em comento. Outro ponto importante a ser esclarecido, de início, é a diferenciação entre as categorias de crimes cibernéticos. Em que pese as variadas classificações existentes, a que melhor engloba os crimes cibernéticos, é a apresentada por Wendt e Jorge (2021, p. 40), a qual prevê as denominadas "ações prejudiciais atípicas", os "crimes cibernéticos abertos" e os "crimes exclusivamente cibernéticos":

> As "ações prejudiciais atípicas" são aquelas condutas, praticadas por intermédio de dispositivos informáticos, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade.

E mais adiante, Wendt e Jorge (2021, p. 40) escrevem sobre os denominados "crimes cibernéticos abertos" e os "crimes exclusivamente cibernéticos", conforme se observa adiante:

> Conforme anteriormente mencionado, os "crimes cibernéticos" se dividem em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Com relação aos crimes cibernéticos "abertos", são aqueles que podem ser praticados da forma tradicional ou por intermédio de dispositivos informáticos, ou seja, o dispositivo é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Dentre os tipos penais abarcados nesta modalidade estão, por exemplo, crimes contra a honra, ameaça, furto mediante fraude, estelionato, falsificação documental, falsa identidade, extorsão, tráfico de drogas etc. Já os crimes "exclusivamente cibernéticos" são diferentes, pois eles somente podem ser praticados com a utilização de dispositivos informáticos. Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate-papo na Internet, previsto no art. 244-B, § 1º, do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990).

Conforme supracitado, existem os "crimes exclusivamente cibernéticos", como o previsto no artigo 244-B, § 1º, do Estatuto da Criança e do Adolescente (BRASIL, 1990):

> Art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com

> ele praticando infração penal ou induzindo-o a praticá-la:
> Pena - reclusão, de 1 (um) a 4 (quatro) anos.
> § 1º Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet.

Percebe-se pela leitura do tipo penal que a "utilização de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet" é elementar do crime, isto é, o mencionado crime somente se verificará se utilizar algum meio eletrônico.

Outro exemplo de "crime exclusivamente cibernético" é o crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal (BRASIL, 1940), o qual prescreve:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

Os crimes cibernéticos, entretanto, podem ser perpetrados de várias maneiras, sendo que a gama de crimes que podem ser cometidos com a utilização de recursos informáticos é enorme, porquanto, conforme a classificação dos "crimes cibernéticos abertos", este é verificado quando um crime que pode ser cometido de forma tradicional o é por meio de recursos informáticos, como, por exemplo, os crimes de estelionato e extorsão, os quais podem ser perpetrados na forma tradicional, porém, diuturnamente, são cometidos pelos meios cibernéticos. Outro exemplo é o crime de tráfico de entorpecentes, de extrema gravidade. O meio tradicional de se praticar o crime de tráfico de entorpecentes é por meio do ponto de venda das drogas, local ao qual o usuário se dirige e efetua a compra dos entorpecentes. Todavia, antes disso houve uma transação maior, na qual uma quantidade muito maior de entorpecentes foi negociada e transacionada. É totalmente possível que essa transação, na qual uma grande quantidade de entorpecentes é negociada, seja efetuada pelos meios informáticos, com vistas a dificultar a identificação dos envolvidos. Esse mesmo procedimento pode ser utilizado, exemplificativamente, por traficantes de armas, outro crime de extrema gravidade. Ou seja, a mesma tecnologia que auxilia e facilita tantos afazeres diários, também é utilizada com interesses escusos por criminosos para o cometimento de crimes. Frise-se, ainda, que houve um crescimento exponencial no cometimento de crimes cibernéticos, especialmente após o ano de 2019, pós-pandemia.

Cumpre salientar, ainda, que existem inúmeras formas para que o criminoso possa cometer o crime e quando ele encontra ferramentas no âmbito informático que podem auxiliar no

cometimento do crime ou na ocultação de sua autoria, esse passa a ser um método muito interessante a ser explorado pelo cibercriminoso. Destarte, analisar-se-ão adiante algumas ferramentas utilizadas por esses criminosos para perpetrar os crimes cibernéticos, contudo, tais ferramentas não serão exaustivamente tratadas, tendo em vista não ser este o objetivo do presente trabalho, sendo que somente algumas das principais serão abordadas adiante.

2.2.1. Engenharia Social

Engenharia Social é uma ferramenta, pela qual uma pessoa com interesses escusos tem em vista conseguir informações que não poderiam ser acessadas por ela. Consoante dizeres de Wendt e Jorge (2021, p. 41), Engenharia Social "é a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo".

É por meio da Engenharia Social que o elo mais vulnerável da Segurança da Informação é atacado, qual seja o fator humano. Interessante as palavras de Mitnick e Simon (2003) sobre o tema:

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia.

A Federação Brasileira de Bancos (FEBRABAN) elenca oito sentimentos humanos explorados pelos ataques do Engenheiro Social, sendo eles (FEBRABAN, 2017): curiosidade, preguiça, vaidade, solidariedade, ingenuidade, confiança, ganância e medo. E, ainda, lista os que são considerados os métodos mais utilizados para a prática de golpes, quais sejam: a) Sites Falsos, como, por exemplo, "www.rnercadolivre.com.br", ou seja, a letra "m" do site verdadeiro é substituída pelas letras "rn" no site fraudulento, induzindo o usuário ao erro; b) E-mail (SPAM), os quais podem oferecer alguma vantagem ou prêmio, por exemplo; c) Redes Sociais, por meio da qual os golpistas abordam suas vítimas; d) Aplicativos de comunicação instantânea, por meio dos quais os criminosos passam a conversar diretamente com as vítimas tentando enganá-las; e) Telefone e SMS, abordagem por ligações ou mensagens e; f) Presencialmente, meio utilizado para se aproveitar da ingenuidade ou descuido em determinado ambiente, como a abordagem de clientes em agências bancárias.

Diante de todo o acima explicitado, fica evidente que a Engenharia Social é uma das facetas exploradas em grande escala pelos cibercriminosos.

2.2.2. Ransomware

O *ransomware* é, conforme dizeres de Wendt e Jorge (2021, p. 70-71) um código malicioso muito utilizado pelos cibercriminosos que faz com que os dados armazenados em um equipamento se tornem inacessíveis, geralmente usando criptografia, e que exige um pagamento como forma de resgate para que se restabeleça o acesso ao usuário. O *ransomware* tem sido um desafio para as polícias brasileiras e internacionais, bem como para as agências de *cybersecurity*, haja vista que a lógica da criptografia aliada ao pagamento com moeda virtual dificulta grandemente a identificação dos autores.

Atualmente, é comum observar casos de ataques a empresas que tem seus dados e informações tornados inacessíveis, objeto desse tipo de código malicioso, gerando grandes prejuízos para as vítimas.

2.3. Investigação dos Crimes Cibernéticos

Diante de todo o supracitado, resta cristalino que os crimes cibernéticos podem ser executados das mais variadas formas, haja vista que existem os crimes classificados como "crimes exclusivamente cibernéticos", porém existem, também, os "crimes cibernéticos abertos", os quais englobam praticamente todas as modalidades delitivas, caso haja a utilização do aspecto informático para a sua perpetração. Em relação às ferramentas utilizadas para o cometimento dos crimes cibernéticos observou-se acima algumas das mais conhecidas, no entanto, existem várias outras e a dinamicidade da tecnologia da informação faz com que novas técnicas sejam desenvolvidas muito rapidamente e, todos esses aspectos contribuem para que a investigação dessa modalidade criminosa seja considerada muito complexa, por diversos motivos, conforme se demonstrará doravante.

Não existe um manual de investigação para se aplicar aos crimes cibernéticos, assim como não há um manual padrão de investigação para os crimes em geral. A investigação criminal persegue os fatos ocorridos e, a partir disso, inicia-se a coleta de evidências que podem se transformar em indícios e, posteriormente, em provas. O mesmo ocorre no caso dos crimes cibernéticos, porquanto, como explicitado acima, a variedade de condutas que podem ser executadas e de ferramentas que podem ser utilizadas para a prática de um crime cibernético é demasiadamente vasta. Portanto, neste trabalho serão analisados alguns métodos de investigação utilizados na investigação dos crimes cibernéticos que resultaram na identificação do criminoso e, por conseguinte, na apuração da autoria criminosa, bem como alguns casos nos quais a autoria não foi elucidada, mesmo havendo, em tese, meios para tal. E, por fim,

demonstrar-se-á a necessidade da criação de um sistema mais simples e eficiente de colaboração internacional para que a repressão dos crimes cibernéticos seja mais efetiva, objetivo principal do estudo desenvolvido neste trabalho.

2.3.1. Investigação criminal em fontes abertas

Consoante explicado acima, a investigação criminal cibernética pode se embasar em qualquer meio que seja amparado pela legalidade, sendo que as fontes abertas oferecem uma gama enorme de informações que podem ser úteis para o esclarecimento do crime.

O conceito de fontes abertas fornecido por Barreto e Wendt (2020, p. 15) é o seguinte:

> A fonte aberta é considerada fonte de inteligência graças às evoluções tecnológicas e, principalmente, à Internet.
> São as informações disponíveis ao público e que não exigem nenhuma espécie de restrição ao seu acesso. São também conhecidas como *open source intelligence* (Inteligência de Fontes Abertas), ou seja, uma forma de coletar, selecionar e adquirir informações que possam ser úteis à produção do conhecimento. Podem ser obtidas através da leitura de jornais, periódicos, pesquisas de cunho acadêmico, livros, revistas e principalmente através da Internet.

Pelo conceito acima exposto se observa que as fontes abertas podem ser todos aqueles meios que estiverem disponíveis e sem nenhuma espécie de restrição para serem acessados, os quais, não raro, são coletados e podem se transformar em provas no decorrer da investigação criminal.

Em alguns países já houve a criação e de agências com base em fontes abertas, como a Austrália, país no qual foi criada, no ano de 2001, a NOSIC (*National Open Source Intelligente Centre*), uma agência que monitora, pesquisa e analisa informações disponíveis em fontes abertas. No Brasil, o tema ainda precisa amadurecer, pois ainda é muito baixo o nível de utilização de informações de fontes abertas no âmbito da investigação criminal.

Uma fonte aberta com uma infinidade de informações disponíveis são as denominadas "redes sociais", o que pode auxiliar em vários casos, como, por exemplo, identificação de testemunhas e autores de crimes, coleta de evidências digitais, localização de foragidos, dentre outros. Um exemplo interessante é colocado por Barreto e Wendt (2020, p. 36-37):

> Polícia mineira e localização de suspeito de homicídio: a prisão de um investigado por homicídio ocorreu na cidade de Mathias Lobato-MG. A fotografia postada pelo foragido com um conjunto de montanhas ao fundo forneceu dados relevantes na localização e detenção do foragido.

Sendo assim, fica claro que as fontes abertas podem auxiliar grandemente as investigações criminais, especialmente quando o agente incumbido da mesma tiver o conhecimento necessário para perscrutar no universo digital, sendo que muitas vezes é,

justamente, na esfera digital que estarão disponíveis as evidências que podem levar ao esclarecimento de crimes graves.

2.3.2. Investigação criminal cibernética: Outros meios

Dentre as variadas técnicas de investigação criminal cibernéticas utilizadas no cotidiano elencar-se-ão algumas a seguir com o escopo de ilustrar como ocorre na prática tais procedimentos.

Consoante palavras de Wendt e Jorge (2021, p. 34) é notório que a Internet tem se transformado num ambiente utilizado para comunicação, informação e interação social pela maior parte das pessoas, tanto no âmbito pessoal como no profissional, assim como também tem se verificado nas grandes corporações.

No âmbito criminal não é diferente, a Internet se transformou numa ferramenta muito utilizada como subterfúgio para o cometimento de crimes. Quando nos deparamos com o termo fraude, logo vem em mente o crime de Estelionato, previsto no artigo 171, caput, do Código Penal, no qual o sujeito ativo pratica o crime mediante artifício, ardil, ou qualquer outro meio fraudulento. O criminoso busca sempre uma forma de aperfeiçoar a forma de praticar o crime com vistas a obter uma vantagem maior e um risco menor de ser descoberto, sendo que durante a pandemia, verificada no ano de 2019, o número de crimes cometidos por meio de fraudes aumentou absurdamente, em especial as fraudes utilizando meios informáticos, ao ponto de ser criado, no ano de 2021, um tipo penal específico, denominado Fraude ou Estelionato Eletrônico, previsto no artigo 171, §2º-A, do Código Penal (BRASIL, 1940), que prevê:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
>
> ...
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Em caso de ocorrência de crime de fraude por meio eletrônico, os passos da investigação, conforme ensinamento de Wendt e Jorge (2021, p. 104-105), serão os seguintes: a) registro das informações sobre o site; b) cópia das conversações mantidas com o criminoso (e-mail, *whatsapp*, telegrama etc.); c) verificação do registro do domínio; d) verificação quanto à responsabilidade pela hospedagem do site; e) pesquisa dos dados informados no registro de

domínio. Em se tratando de fraude eletrônica no sistema bancário, pode-se dizer o mesmo, contudo com algumas outras especificidades como, por exemplo, a busca, junto ao banco do qual a vítima é cliente, com o objetivo de obter os dados referentes a IP, data, hora e como ocorreu a transação fraudulenta.

Saliente-se que os passos acima descritos não se trata de um rol taxativo, é dizer, não afastam quaisquer outros tipos de providência que se mostrem necessárias ao caso concreto.

Outras condutas criminosas que são muito praticadas na Internet são os crimes de *cyberstalking* e *cyberbulling*, os quais, segundo dizeres de Wendt e Jorge (2021, p. 125-129) cresceram muito nos meios eletrônicos. O *cyberstalking* ocorre quando o criminoso passa a perseguir a vítima por meios eletrônicos ao ponto de causar danos à paz da mesma, seja por meio de mensagens insistentes, tentativas de contatos indevidas, condutas que ultrapassam os limites da privacidade da vítima. O *cyberbulling* pode ficar caracterizado mediante a ocorrência de variados crimes previstos no Código Penal, como, por exemplo, os crimes contra a honra – calúnia, difamação e injúria, o crime de ameaça ou o crime de falsa identidade, dentre outros. Os crimes contra a honra ocorrem quando a vítima tem sua honra, objetiva ou subjetiva, atingida por publicações em redes sociais ou outros meios informáticos. O crime de ameaça é outra espécie delituosa que frequentemente ocorre pelos meios eletrônicos, via *whatsapp*, por exemplo. Já o crime de falsa identidade é outra modalidade muito recorrente nos meios eletrônicos, pois muitos criminosos utilizam a tecnologia para tentar homiziar sua identidade e cometer os crimes procurando garantir sua impunidade, o que muitas vezes acontece.

Todavia, conforme bem lembra Wendt e Jorge (2021, p. 131):

> A prática deste tipo de crime pela Internet não é sinônimo de impunidade, muito pelo contrário. A Polícia Civil e a Polícia Federal possuem instrumentos adequados e profissionais capacitados para que, por intermédio da investigação criminal, a autoria e a materialidade sejam comprovadas.

Cumpre lembrar que como meios de prova nos crimes acima analisados mostram-se muito importantes o registro das conversas, bem como a cópia delas, entretanto, muitas vezes as vítimas apresentam somente a captura de tela, chamadas de prints – das conversas o que não possuem um alto valor probatório, devido ao fato de poder ser manipulados facilmente. Destarte, é mais recomendável lavrar uma ata notarial com as informações que podem servir como provas para que possuam valor probatório durante a investigação e o processo criminal.

2.3.3. Investigação criminal cibernética na Deep Web

O termo *deep web*, conforme escrevem Barreto e Santos (2019, p. 6-7) foi utilizado pela

primeira vez no ano de 2001, Michael K. Bergman, sendo que atualmente a doutrina ainda diverge ao estudar os conceitos de *deep web*. Parte defende a presença de quatro requisitos (descentralização, segurança, anonimidade e codificação aberta) concomitantemente presentes, enquanto outra parte apregoa a necessidade de um ou outro requisito, principalmente a descentralização e o anonimato.

Barreto e Santos (2019, p. 7) fornecem o seguinte conceito de deep web:

> A *deep web* é, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é "visível" pelas ferramentas de busca convencionais. A arquitetura de redes predominante é a ponto a ponto (P2P), ou seja, dispensa um servidor central, cenário no qual todos os componentes (pontos ou nós) funcionam ora como cliente, ora como servidor. O exemplo mais clássico de rede tipicamente dentro dos conceitos de *deep web* é a Tor. Nessa rede estão presentes as quatro características básicas listadas anteriormente e por isso ela é, muitas vezes, associada erroneamente ao próprio conceito de *deep web*.

Muito se fala sobre o conteúdo da *deep web*, alguns imaginam que lá estão conteúdos totalmente fora da normalidade, no entanto, observar-se-á adiante, que na realidade esse conteúdo pode ser variado e geralmente é algo reprovável ou ilícito e, devido a isso, o que se busca, verdadeiramente, com a utilização da *deep web* são os requisitos acima mencionados, dentre eles o anonimato, que se tenta garantir com forte criptografia e outros artifícios disponíveis. No que tange aos cibercriminosos, esses objetivam manter a autoria dos crimes cometidos desconhecida e, consequentemente, o crime impune.

Como advertem Barreto e Santos (2019, p. 11):

> O acesso ao conteúdo pode ser considerado mais ou menos difícil, não pelo fato de estar presente em um nível mais profundo, mas em razão de os programadores, ou até mesmo o usuário que disponibilizou o acesso, terem definido regras distintas: criptografia, senha, distribuição do endereço para comunidades fechadas, mudança constante de formas de acesso, dentre outras.

Diante das condições favoráveis que a *deep web* oferece para os cibercriminosos, variadas modalidades criminosas são ali verificadas, sendo que crimes graves são cometidos por esse meio, tais como tráfico de entorpecentes, tráfico de armas e abuso e exploração sexual infantil.

A gravidade e o quão pernicioso é o crime de tráfico de drogas para a sociedade são notórios, por ser um crime que além de movimentar cifras elevadas ano após ano, deixa marcas profundas nas famílias atingidas e na sociedade como um todo. A utilização da *deep web* é um ótimo negócio para os cibercriminosos que atuam nesse ramo, porquanto, com a utilização da *deep web*, o anonimato está quase garantido e é utilizado para manter a sensação de impunidade.

Na *deep web*, conforme escrevem Barreto e Santos (2019, p. 84-86) são encontrados inúmeros sites, especialmente na rede Tor, os chamados mercados negros, onde vários vendedores estão reunidos com uma grande variedade de drogas e outros produtos ilegais. No concernente ao tráfico de drogas, a comercialização de ecstasy é um dos carros-chefes desse mercado negro, pois são pequenos comprimidos fáceis de esconder e com grande consumo entre jovens de classe média e alta.

Ocorreu um caso interessante, citado como exemplo por Barreto e Santos (2019, p. 90), em que a investigação da Polícia Civil da cidade de Araçatuba, no interior do Estado de São Paulo, obteve êxito em identificar cibercriminosos que praticavam tráfico de entorpecentes:

> No *notebook* de um autuado em flagrante foram encontradas capturas de telas (imagens) de um *site* denominado *Dream Market*. O endereço desse *site* estava hospedado na rede Tor, através do domínio *onion*.
> A identificação da origem da droga sintética apreendida foi obtida através de um número de rastreio dos correios encontrado em uma anotação no aparelho celular do autuado. Em consulta de fontes abertas realizadas no *site* dos correios, os investigadores lograram êxito na elucidação da origem e do destino final da entrega das drogas sintéticas, assim como foram mapeadas mais de vinte pessoas que comercializam as drogas sintéticas em festas *rave* da região.
> Parte do produto adquirido via *deep web* do fornecedor dos Estados Unidos foi apreendida em uma ação do Grupo de Operações Especiais de Araçatuba, no início de novembro de 2018.

Em se tratando do crime de tráfico de armas os mesmos preceitos vistos em relação ao tráfico de drogas são verificados, pois o mesmo modo de execução que é utilizado para um pode ser implementado para o outro e o mesmo se pode dizer em relação à gravidade dos crimes, haja vista que as armas, ilegalmente comercializadas, por meio da *deep web* são utilizadas, em sua grande maioria, por organizações do crime organizado para o cometimento dos mais variados e repugnantes crimes.

O crime de abuso ou exploração sexual infantil é extremamente reprovável e repugnante e sabendo disso os cibercriminosos se valem de todos os recursos possíveis para não serem identificados. Por conseguinte, é uma das modalidades criminosas mais verificadas na *deep web*, conforme corroboram Barreto e Santos (2019, p. 92): “Um dos crimes mais praticados nas redes *deep web* é o abuso e a exploração sexual de crianças e adolescentes”.

A reprovabilidade que recai sobre os crimes cibernéticos sexuais contra crianças e adolescentes em todo o mundo, de tal forma que foram estabelecidos parâmetros aceitos em qualquer parte do mundo, onde foram criados critérios de classificação dos arquivos que circulam na internet envolvendo crianças e adolescentes, de acordo com três características, conforme dizeres de Barreto e Santos (2019, p. 93): a) Visualmente, deve ser possível a

identificação de crianças em fotos ou vídeos; b) O foco da fotografia ou filmagem é direcionado para o genital da criança; c) Nas imagens há crianças em ato explícito de sexo com outra criança ou com adulto.

Diante de todo o estudo acima exposto, resta cristalino que são demasiadamente variadas as formas pelas quais os crimes cibernéticos podem ser perpetrados, bem como novas e mais avançadas técnicas surgem com bastante rapidez e são utilizadas para o cometimento das mais variadas fraudes e crimes no ambiente informático. Existem grandes empecilhos durante as investigações dos crimes cibernéticos, tais como a falta de conhecimento daqueles que atuam na persecução penal, desde a investigação policial até o processo criminal em juízo. Todavia, os crimes mais graves e de maior vulto encontram um outro obstáculo, maior e que causa maior entrave, qual seja, a falta de um sistema de cooperação internacional mais eficaz para a repressão dos crimes cibernéticos, conforme se demonstrará adiante.

3. Metodologia

O método de pesquisa utilizado nesse trabalho foi a pesquisa bibliográfica, utilizando informações oriundas de, livros e artigos, em sua maioria publicados entre os anos de 2018 e 2023, publicações eletrônicas com notícias em fontes como, *site* do governo federal, entre os anos de 2022 e 2023 e legislações que se relacionam com o tema em estudo, com o intuito de aprofundar os conhecimentos referente ao assunto, fundamentar a pesquisa sobre o tema, proporcionando uma base mais sólida acerca dos temas como, segurança da informação, crimes cibernéticos, investigação de crimes cibernéticos e os sistemas de cooperação internacional no combate aos crimes cibernéticos. Foram considerados os textos que apresentaram relevância com o tema tratado, sendo excluídos os que não apresentavam relação com o tema, bem como foram priorizados os textos mais recentes, preferencialmente a partir do ano de 2018, o que formou a base de dados para o desenvolvimento deste trabalho por meio dos livros, pesquisas em *sites* da Internet que forneceram informações relevantes ao enriquecimento do trabalho.

4. Resultados e Discussões

Doravante serão apresentados, objetivamente, os resultados da pesquisa acima efetuada, sendo que para tal finalidade será feita a análise da importância da criação de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos, haja vista que muitos crimes cometidos no ambiente cibernético restam sem esclarecimento devido às estratégias

evasivas utilizadas pelos cibercriminosos para se manterem anônimos perante as autoridades e não responderem pelos crimes cometidos, principalmente a transnacionalidade do delito cometido.

4.1. A importância da criação de um sistema de cooperação internacional eficaz no combate aos crimes cibernéticos

É cediço que a tecnologia evolui de forma muito rápida e dinâmica, a ponto de algumas tecnologias que eram consideradas novas anos atrás, hodiernamente, já se mostram obsoletas. Em relação aos crimes cibernéticos, o mesmo fenômeno se verifica, pois muitos são os artifícios utilizados pelos cibercriminosos e muitas são as novas técnicas que surgem em curto espaço de tempo. Sendo assim, as técnicas utilizadas na repressão dos crimes cibernéticos também devem possuir essas características, rapidez e dinamicidade, sob pena de não conseguirem conduzir ao esclarecimento dos crimes cibernéticos. Segundo publicação da InfoMoney (2023), *site* especializado em mercados, investimentos e negócios no Brasil, no ano de 2022 o Brasil – com 103,1 bilhões de tentativas, foi segundo colocado no ranking de ataques cibernéticos da América Latina e Caribe, ficando atrás somente do México.

No Brasil, assim como a maioria dos outros países, percebeu-se um crescimento muito rápido dos crimes cibernéticos, precipuamente após a pandemia de 2019, onde as pessoas ao redor do mundo precisaram se adaptar às novas tecnologias para trabalharem em casa, bem como para realizarem muitas outras tarefas rotineiras, haja vista o momento vivenciado naquele período. Consequentemente, houve também o crescimento na criminalidade utilizando os meios tecnológicos, bem como o avanço das técnicas criminosas neste meio e, muitas vezes, crimes extremamente graves não são punidos porque a autoria permanece desconhecida, tendo em vista que seus autores se valem de subterfúgios como a utilização de servidores em variados países – ou seja, o crime toca os territórios de várias nacionalidades, para dificultar o rastreamento de suas atividades criminosas e permanecerem impunes. O que, infelizmente, não raro acontece, pois a comunicação realizada entre os países para cooperação no combate aos crimes cibernéticos, muitas vezes, não possui um meio padronizado, eficaz e rápido suficiente para a identificação dos envolvidos e, por conseguinte, verificam-se vários casos em que seria possível a identificação e punição do criminoso, que permanecem na impunidade. Jesus e Milagre (2016, p. 194) corroboram o supracitado, nos seguintes termos:

> Em termos judiciais, em verdade, para que uma autoridade brasileira consiga dados relativos a usuários que usaram de serviços no exterior, o meio mais usual é a morosa

> "carta rogatória", considerando que não se deve produzir prova ilícita, como o lançamento de "iscas" ou "trojans forenses". Também existe o chamado "auxílio direto", sendo que cada país adota uma forma de cooperação.

Saliente-se que, de nada adianta a criação de instrumentos de colaboração que não sejam efetivos, conforme escreve Santos (2018, p. 168):

> Como mais de 50% dos crimes cometidos na internet têm algum aspecto transnacional, as investigações desses crimes envolvem diferentes jurisdições, o que demanda – quer por meio de tratados multilaterais ou bilaterais, quer pelas leis internas dos países – uma cooperação mútua dinâmica, que não seja emperrada pela falta de instrumentos jurídicos que viabilizem essa cooperação.

É essencial a implementação de alternativas viáveis em sede de legislação nacional e em termos de uma eficaz cooperação internacional, com ferramentas automatizadas que permitam a localização dos proprietários dos arquivos e a persecução penal desses criminosos que os armazenam ou distribuem. (CAIADO, CAIADO, 2018, p. 18)

Em relação às técnicas de investigação dos crimes cibernéticos, oportuno mencionar as palavras de Barreto e Santos (2019, p. 108-109) a *Network Investigative Technique* (NIT), também conhecida como Técnica de Investigação de Redes – a qual é utilizada, mediante autorização judicial, para instalar um software em dispositivo de terceiro, com o objetivo de coletar provas digitais e outras informações necessárias à atribuição da autoria e materialidade delitiva. Referida técnica vem sendo aplicada pelo *Federal Bureau of Investigation* (FBI), há mais de 25 anos em casos graves como abuso e exploração sexual infantojuvenil e terrorismo, dentre outros. Durante uma operação do FBI, no combate ao abuso e exploração sexual infantojuvenil, a utilização da Técnica de Investigação de Redes, foram coletadas informações de milhares de usuários do *site* criminoso em diversos estados e até mesmo em países de outros continentes.

O crime cibernético, devido a suas características intrínsecas já é considerado de difícil elucidação e, ao se verificar um crime cibernético que toca o território de mais de um país, a situação apresenta uma dificuldade infinitamente maior, pois se faz necessário, nesses casos, da utilização concomitante de legislações de nacionalidades diversas, as quais muitas vezes podem ser conflitantes em determinados pontos, sendo que esse subterfúgio muitas vezes é utilizado pelos cibercriminosos, tendo em vista que não é incomum a prática do delito por meio de sistemas hospedados no exterior e nesses casos, a investigação, realizada no Brasil, precisa da cooperação de provedores de fora do país e parte desses provedores costumam alegar que não estão sujeitos às ordens da jurisdição brasileira. Todavia, conforme escrevem Jesus e Milagre

(2016, p. 194-195) a praxe é a utilização de uma forma de cooperação denominada *Mutual Legal Assistance Treaty* (MLAT), conhecido como Assitência Jurídica em Matéria Penal, todavia tal procedimento é demasiadamente moroso, o que pode levar a perda das provas do crime.

As palavras de Domingos e Röder (2018, p. 34-35) corroboram a morosidade, muitas vezes verificada, na utilização da MLAT, pois segundo os dizeres delas 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 técnologias.

No ano de 2001 foi realizada a Convenção de Budapeste, na Hungria. Esse tratado internacional foi elaborado com o intuito de padronizar a cooperação internacional para a obtenção de provas digitais, nas searas penal e processual penal, e foi homologado por 52 países. Por se tratar do primeiro tratado internacional a discorrer sobre crimes cibernéticos, tornou-se o padrão a ser seguido por legislações de vários países.

A quase totalidade dos países europeus aderiram a Convenção de Budapeste, todavia a Rússia não assinou tal convenção, conforme escreve Jesus e Milagre (2016, p. 76):

> Importa dizer que a Rússia, por fim, não assinou a Convenção de Budapeste, que trata do combate ao cibercrime e a padronização das legislações dos Estados-membros. O país categoricamente não adota a Convenção de Budapeste, especialmente em relação ao art. 32, que trata do chamado "acesso transfronteiriço", que permite que as agências de inteligência de alguns países acessem as redes de computadores de outros países para realizar operações, sem o conhecimento das autoridades nacionais.

O Brasil demorou, porém, mesmo que tardiamente, tornou-se signatário da Convenção de Budapeste e publicou tal ato, por meio do Decreto nº 11.491 de 12 de abril de 2023, conforme se observa no site do Ministério da Justiça e Segurança Pública (BRASIL, 2023):

> Por meio da denominada Convenção de Budapeste, firmada em 23 de 2001, as autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos, assim como de outras infrações penais, que demandem a obtenção de provas eletrônicas/digitais armazenadas em outros países. Prevê-se uma cooperação "mais intensa, rápida e eficaz".
>
> …
>
> Além do aperfeiçoamento da cooperação internacional na instrução e elucidação dos delitos praticados no ambiente virtual, a Convenção também impulsiona o Brasil a dar continuidade ao desenvolvimento de seu ordenamento jurídico e de sua política diante do avanço da criminalidade no ambiente cibernético, assim o fazendo com o devido equilíbrio entre a intensificação da persecução penal e a proteção de dados pessoais.

Saliente-se que se mostra de grande importância a adesão à Convenção de Budapeste por parte do Brasil, entretanto, de maior e extrema necessidade se faz a criação de um organismo

centralizado e, muito bem organizado para a consecução dos objetivos constantes na referida Convenção, porquanto de nenhuma valia terá sido essa adesão se a cooperação entre os países envolvidos não possuírem os requisitos da rapidez e eficácia na comunicação entre os eles, haja vista que a morosidade na comunicação é um dos maiores trunfos dos cibercriminosos para permanecerem impunes, porquanto, conforme escreve Barreto, Kufa e Silva (2022, p. 107): "Para uma melhor persecução da macrocriminalidade, a dinamização e a desburocratização da cooperação jurídica são imprescindíveis".

5. Considerações finais

Após a análise de todo o estudo realizado durante este trabalho, conclui-se que a ocorrência de crimes cibernéticos cresceu demasiadamente nos últimos anos, principalmente após a pandemia verificada no ano de 2019, haja vista que a tecnologia, que já apresenta avanços de forma dinâmica, necessitou mostrar soluções ainda mais rápidas neste período. Como consequência, houve muitas evoluções tecnológicas e, concomitantemente, cresceu exponencialmente a ocorrência de crimes cibernéticos, os quais estão sendo praticados com técnicas cada vez mais sofisticadas.

Os meios utilizados e os crimes cibernéticos praticados, como explicado no trabalho, são variados, porém, o criminoso cibernético possui uma característica intrínseca a todos àqueles que cometem qualquer tipo de delito, manter-se desconhecido, evitando assim sua identificação e, consequente, punição. Em que pese haver os criminosos mais descuidados na área cibernética, a maioria dos crimes, especialmente os mais graves, como, por exemplo, as grandes redes de exploração sexual infantil e o tráfico de entorpecentes e armas, se utilizam de recursos mais abrangentes, como utilização de territórios de países diferentes para o tráfego das informações criminosas, sabendo que isso dificultará grandemente as investigações, devido à falta de uma comunicação rápida e eficaz entre os órgãos incumbidos pela repressão dos citados crimes, mormente em se tratando de crimes que tocam o território de um ou mais países.

A criação de um mecanismo de cooperação internacional mostra-se uma necessidade premente para que esses graves crimes cibernéticos não continuem impunes e cada vez mais crescendo no Brasil e em todo o mundo, pois essa falta de punição reflete diretamente no crescimento dos referidos crimes. Recentemente, o Brasil deu um passo enorme neste caminho, ao se tornar signatário da Convenção de Budapeste. Todavia, o passo mais importante é o passo porvindouro, qual seja, a operacionalização dessa cooperação internacional, padronizando e

simplificando o acesso às autoridades brasileiras envolvidas na repressão dos crimes cibernéticos e estabelecendo meios de comunicações eficazes entre as autoridades nacionais e internacionais, pois de nada adianta possuir o arcabouço legal disponível se ele não se mostrar eficaz.

Referências

BAARS, Hans. et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Traduzido por Alan de Sá. 3. ed. Rio de Janeiro: Brasport, 2018.

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 3. ed. São Paulo: Juspodivm, 2022.

BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. **Deep Web: investigação no submundo da internet**. Rio de Janeiro: Brasport, 2019.

BARRETO, Alessandro Gonçalves; WENDT, Emerson. **Inteligência e investigação criminal em fontes abertas**. 3. ed. Rio de Janeiro: Brasport, 2020.

BRASIL**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal**. Planalto, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 set. 2023.

BRASIL**. Lei nº 8.069, de 13 de julho de 1990**. Planalto, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 set. 2023.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Planalto, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 set. 2023.

BRASIL, Ministério da Justiça e Segurança Pública. **Convenção de Budapeste é promulgada no Brasil: Autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 12 set. 2023.

CAIADO, Felipe B.; CAIADO, Marcelo. **Crimes cibernéticos: coletânea de artigos vol. 3 - MPF: Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse**. Brasília: MPF, 2018.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. **Crimes cibernéticos: coletânea de artigos vol. 3 - MPF: Obtenção de provas digitais e jurisdição na Internet**. Brasília: MPF, 2018.

FEBRABAN. **Engenharia Social: saiba como evitar possíveis armadilhas e se proteger de golpes**. São Paulo: Febraban, 2017.

IBGE. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. IBGE, 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 05 set. 2023.

INFOMONEY. **Brasil aparece em 2º em ranking de ataques cibernéticos; como se proteger**. InfoMoney, 2023. Disponível em: https://www.infomoney.com.br/negocios/brasil-aparece-em-2o-em-ranking-de-ataques-ciberneticos-como-se-proteger/amp/. Acesso em: 20 set. 2023.

JESUS, Damásio E. de. **Direito penal: parte geral**. 26. ed. São Paulo: Saraiva, 2003.

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

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação**. Traduzido por Kátia Aparecida Roque. São Paulo: Pearson Education, 2003.

SANTOS, Paulo Ernani Bergamo dos. **Crimes cibernéticos: coletânea de artigos vol. 3 - MPF: Direito internacional e o combate à cibercriminalidade contra crianças**. Brasília: MPF, 2018.

TZU, Sun. **A arte da guerra**. Traduzido por Pedro Manoel Soares. 3. ed. Jandira/SP: Ciranda Cultural, 2019.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 3. ed. Rio de Janeiro: Brasport, 2021.