



CENTRO UNIVERSITÁRIO REDENTOR – AFYA
CURSO DE GRADUAÇÃO EM DIREITO

KISSIANE VIEIRA LIMA

OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS NO BRASIL

Itaperuna, RJ

2021

KISSIANE VIEIRA LIMA

OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS NO BRASIL

Trabalho de Conclusão de Curso
apresentado como requisito
parcial para a obtenção do título
de Bacharel em Direito ao Centro
Universitário Redentor.

Orientadora: Daniela Garcia Botelho

Itaperuna,RJ
2021

FOLHA DE APROVAÇÃO

Autora: KISSIANE VIEIRA LIMA

Título: OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS NO BRASIL

Natureza: Trabalho de Conclusão de Curso

Objetivo: Título de Bacharel em Direito

Instituição: Centro Universitário Redentor

Área de Concentração: Direito Penal

Aprovada em: ____/____/____

Banca Examinadora:

Profª Daniela Garcia Botelho
Especialista (Orientadora)
Instituição: Centro Universitário Redentor

Profª Renata Alfradique Carpi Paiva
Especialista
Instituição: Centro Universitário Redentor

Profª Maria Luiza Lacerda Carvalhido
Mestra
Instituição: Centro Universitário Redentor

AGRADECIMENTOS

Agradeço a Deus, em primeiro lugar por terabençoadado e iluminado meu caminho até aqui.

A minha família, por todo o apoio e suporte durante esse período, foram cruciais para concretização do meu sonho e minha base nos momentos mais difíceis.

Aos meus amigos por todo o incentivo, fizeram com que a caminhada até aqui fosse imensamente mais leve.

A minha orientadora pelo auxílio, apoio e ensinamentosao longo do meu projeto final, foram essenciais para que eu conseguisse concluir o presente trabalho.

Agradeço, ainda, aqueles que de certa forma me incentivam a continuar e concluir minha trajetória acadêmica.

“Decifrar o mundo se baseia em fazer as melhores perguntas.”

Leandro Karnal

RESUMO

Com o processo de evolução tecnológica houve também uma sofisticação na prática de crimes por meio da *internet*, diante disso, o presente trabalho tem como objeto a realização de um estudo acerca dos crimes cibernéticos no Brasil, em que serão abordadas as principais legislações que tratam dessas espécies de delito no país, sendo feito um breve relato da evolução histórico-legislativa, demonstrando que a legislação vigente por si só não é suficiente no enfrentamento dos crimes virtuais, uma vez que não abarca todas as modalidades dos crimes que podem ser praticados no meio virtual, dessa forma, o presente estudo tem como justificativa a necessidade de uma adaptação do Estado brasileiro face os crimes informáticos. Ademais, através de uma pesquisa bibliográfica de abordagem qualitativa e caráter exploratório foi possível identificar dificuldades na fase da persecução penal, ocasionadas em razão do caráter transnacional desses delitos, juntamente com o avanço tecnológico, que gera embaraço na identificação da autoria dos crimes virtuais e na busca de vestígios visando à comprovação da materialidade dos tipos, tendo em vista que os indícios dos *ciber Crimes* desaparecem com uma maior rapidez que os crimes comuns, diante disso, a cooperação judiciária internacional pode ser uma alternativa no enfrentamento dos crimes cibernéticos, principalmente no que se refere à ratificação pelo Brasil à Convenção de Budapeste de 2001, a primeira convenção a tratar do crime cibernético no mundo, dispondo acerca de mecanismos fundamentais visando o combate aos *ciber Crimes*.

Palavras-Chave: Crimes cibernéticos, crimes virtuais, cooperação judiciária internacional, Convenção de Budapeste.

ABSTRACT

With the process of technological evolution there was a sophistication in the practice of crimes through the internet, therefore, the present work aims to carry out a study about cyber crimes in Brazil, in which the main legislations that deal with these categories will be addressed of crime in the country, with a brief report on the historical-legislative evolution, showing that the current legislation by itself is not enough in the confrontation of virtual crimes, since it does not cover all the modalities of crimes that can be committed in the virtual world. Furthermore, difficulties are encountered in the criminal prosecution phase, caused by the transnational nature of these crimes, together with technological advances, which generate embarrassment in identifying the authorship of virtual crimes and in the search for traces in order to prove the materiality of the crimes, having considering that the evidence of cybercrime disappears faster than common crimes, in view of this, international judicial cooperation can be an alternative in tackling cybercrime, especially with regard to Brazil's ratification of the 2001 Budapest Convention, the first convention to deal with cybercrime in the world, providing for fundamental mechanisms aimed at combating cybercrime.

Key words: Cyber crimes, international judicial cooperation, Budapest Convention.

SUMÁRIO

RESUMO.....	6
ABSTRACT.....	7
1 INTRODUÇÃO	8
2 BREVE RELATO DA EVOLUÇÃO HISTÓRICO-LEGISLATIVA	10
2.1 Lei Carolina Dieckmann Lei de nº 12.737/2012 e as alterações trazidas pela Lei de nº 14.155/2021:	10
2.2 Lei do Marco Civil da Internet, Lei nº 12.965/2014, e as alterações trazidas pela Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018:	14
3 DOS CRIMES CIBERNÉTICOS.....	18
3.1 Das características dos Crimes Cibernéticos.....	19
3.2 Competência para processar e julgar os crimes cibernéticos:.....	21
4 DAS DIFICULDADES ENFRENTADAS PELO BRASIL NO COMBATE AOS CRIMES CIBERNÉTICOS	24
4.1 Os desafios na fase da persecução penal	24
4.2 Dados sobre os crimes cibernéticos	27
5 DOS POSSÍVEIS MEIOS DE COMBATE AOS CRIMES CIBERNÉTICOS	29
5.1 Da Cooperação Jurídica Internacional	29
5.2 Um estudo sobre a ratificação do Brasil à Convenção de Budapeste como uma possível solução ao combate aos crimes cibernéticos.....	31
6 CONCLUSÃO	35
REFERÊNCIAS.....	37

1 INTRODUÇÃO

Com o advento da globalização houve também uma evolução nos meios de comunicação, o que facilitou o convívio em sociedade, e este período é conhecido pelos estudiosos como era da informação. Entretanto, apesar dos grandes avanços e pontos positivos, essas inovações tecnológicas trouxeram também novos artifícios para o cometimento de crimes no meio virtual, sendo este fato decorrente do crescente processo de informatização da sociedade (DELGADO, 2007, *online*).

Diante da sofisticação das condutas criminosas na prática de delitos por meio da *internet*, surge a necessidade da adoção de novos mecanismos que visem a suprimir tais condutas, uma vez que nem todos os atos são abarcados pelo ordenamento jurídico brasileiro atual.

O presente trabalho de conclusão de curso tem como pilar principal realizar um estudo acerca da eficiência dos meios de enfrentamento presentes na legislação atual brasileira no combate aos crimes cibernéticos no país, analisando quais são os principais problemas no enfrentamento dessas espécies de crimes, e buscar responder a nível nacional e internacional quais as medidas o Brasil deverá adotar para que adquira êxito na elucidação destes delitos dada a sua transnacionalidade.

O presente estudo possui como objetivos específicos construir o percurso histórico das legislações que tratam do crime no meio virtual no Brasil, bem como realizar uma análise das características dos cibercrimes, em que será abordado o conceito, a classificação e a competência.

Ainda no que tange aos objetivos específicos, será realizada uma avaliação acerca da atual situação do Brasil no que se refere o combate aos crimes cibernéticos, assim como, elaborar uma análise dos meios de combate aos crimes praticados por meio da *internet*, sob o prisma da cooperação jurídica internacional.

Diante do crescimento e evolução das tecnologias houve também uma maior complexidade e sofisticação na prática de crimes por meio da *internet*, dessa forma, o presente estudo tem como justificativa a necessidade de uma adaptação do Estado brasileiro face os crimes informáticos.

A metodologia utilizada no presente trabalho consiste em uma pesquisa bibliográfica de abordagem qualitativa e caráter exploratório.

O presente trabalho busca responder se os meios de enfrentamento utilizados pelo nosso ordenamento jurídico estão sendo eficientes para combater os crimes cibernéticos no Brasil, bem como identificar os principais desafios encontrados na legislação brasileira no que tange a elucidação dos crimes praticados no meio virtual e como a cooperação Jurídica Internacional pode auxiliar no combate a essas espécies de delitos.

O primeiro capítulo é a presente introdução, que busca realizar uma breve exposição acerca do tema que será abordado ao longo do capítulo, bem como detalhar outros critérios de ordem técnica que se fizeram presentes da confecção do presente trabalho.

No segundo capítulo será realizada uma demonstração do percurso histórico das leis que tratam dos crimes praticados pelo meio virtual no Brasil, com abordagem especial quanto a uma das primeiras leis a dispor sobre o tema, qual seja, a Lei nº 12.737/2012, mais conhecida como “Lei Carolina Dieckmann”, bem como as alterações trazidas pela Lei de nº 14.155/2021, promulgada em maio de 2021. Também será abordada a Lei de nº 12.965/2014, conhecida como “Lei do Marco Civil na Internet”, que estabelece direitos e garantias acerca do uso da *internet* no Brasil.

Em seguida, no terceiro capítulo, será feito um estudo específico acerca dos crimes cibernéticos, em que serão trazidos o conceito, as características, e a competência referente a essas espécies de delitos.

Posteriormente, no quarto capítulo será examinada a situação atual do Brasil no que tange o combate aos crimes cibernéticos, principalmente a questão da investigação, os desafios encontrados na fase da persecução penal, bem como a ausência de uma legislação clara e específica que proteja os bens jurídicos que hoje são afetados por cibercriminosos.

No capítulo posterior será realizado um estudo acerca da cooperação jurídica internacional, bem como será analisada a possibilidade de ratificação pelo Brasil à Convenção de Budapeste de 2001, e os benefícios que essa ratificação pode trazer para o enfrentamento dos crimes cibernéticos.

Derradeiramente, no sexto e último capítulo, será apresentada uma conclusão acerca do entendimento a que se pode chegar com o estudo dos pontos descritos anteriormente.

2 BREVE RELATO DA EVOLUÇÃO HISTÓRICO-LEGISLATIVA

O Brasil sofria uma enorme cobrança quanto à coerção dos crimes virtuais, por não haver uma legislação penal específica dispondo do tema, o que acabava gerando a impunidade de alguns atos. Em verdade, não havia até mesmo leis que tratassem acerca do uso da *internet* de forma geral no país.

Atualmente, as principais leis que tratam do assunto é a Lei de nº 12.737/2012, a Lei nº 14.155/2021, bem como a Lei do Marco Civil da Internet, Lei nº 12.965/2014 e a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, que serão estudadas neste capítulo.

Neste contexto, cumpre ressaltar que o objetivo do presente trabalho não é exaurir o estudo das referidas normas, mas sim levantar as questões pertinentes aos crimes virtuais.

2.1 Lei Carolina Dieckmann Lei de nº 12.737/2012 e as alterações trazidas pela Lei de nº 14.155/2021:

A Lei de nº 12.737/12 foi uma das precursoras a tratar dos crimes no meio virtual no Brasil, incluindo no Código Penal o art. 154-A, que trata do tipo penal de “invasão de dispositivo informático” (BRASIL, 2012, *online*):

Art. 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

A referida lei originou-se do Projeto de Lei de nº 2.793/2011, sendo impulsionado pelo fato de fotos íntimas da atriz Carolina Dieckmann serem expostas na *internet*, após terem sido supostamente copiadas de seu computador, motivo pelo qual a lei em questão foi apelidada pelo nome da atriz (JESUS; MILAGRE, 2016, p. 89).

Antes do advento da Lei nº 12.737/12, não havia na legislação brasileira um tipo penal que tratasse de forma específica acerca da cópia não autorizada de dados ou informações, dessa forma, quando se deparavam a casos semelhantes, os

membros do Ministério Público acabavam por oferecer a denúncia embasados no art. 155 do Código Penal, mas muitos doutrinadores sustentavam ser impossível a aplicação do tipo penal de furto a esses casos, haja vista que *“a coisa ‘dados’ não saía da esfera de disponibilidade da vítima, mas tão somente era ‘copiada’. Um ‘ctrl+c’ não poderia ser considerado furto”* (JESUS; MILAGRE, 2016, p. 89).

No que tange ao art. 154-A incluído no Código Penal, a doutrina classifica este tipo penal como sendo de um delito de perigo abstrato, uma vez que não se espera o acontecimento do resultado (JESUS; MILAGRE, 2016, p. 88), bastando que ocorra a invasão do dispositivo da vítima com a intenção de se alcançar os objetivos ilegais.

Nesse contexto, na sociedade atual, denominada como sendo a sociedade da informação, é objetivada a proteção de direitos supraindividuais, de forma preventiva, conforme acentuam Damásio de Jesus e Antonio Milagre (2016, p.88):

(...) na sociedade da informação, cada vez mais buscam-se proteger direitos supraindividuais, em um modelo preventivo do Estado contra os riscos e não contra ameaças concretas de lesão ao bem jurídico protegido.

Ocorre que a promulgação da Lei nº 12.737/2012 pôs fim ao problema da falta de tipificação, mas não teve capacidade de por si só abarcar os diversos modos de cometimento do crime, como

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

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

A lei supramencionada realizou a majoração da pena do tipo de “invasão de dispositivo informático”, pois antes a pena para quem praticasse este delito era de detenção de três meses a um ano e multa, e agora passou a ter como medida punitiva a pena de reclusão, podendo ser aplicada de um a quatro anos, além da pena de multa.

Em ambos os casos o bem jurídico tutelado é a privacidade, bem como a liberdade individual, o direito à intimidade e segurança informática, conforme dispõe Damásio de Jesus (2020, p. 410): “O legislador inseriu o tipo penal entre os crimes contra a inviolabilidade dos segredos, revelando parte do bem jurídico protegido. Tutelam-se, além deste, a intimidade e a segurança informática”.

Tal proteção corrobora a proteção de direitos resguardados constitucionalmente, especialmente no que refere o direito à intimidade e à vida privada, prevista no art. 5, inciso X, da Constituição de 1988 (BRASIL, 1988, *online*):

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação

A nova lei fez outras alterações no dispositivo legal, abrangendo a área de proteção do referido artigo, além disso, deixou evidente que para ser enquadrado no tipo penal, não é necessário que a vítima seja a proprietária do dispositivo violado.

Ademais, a lei em questão retirou a exigência de “violação de mecanismo de segurança” exigida pela Lei nº 12.737/2012, agora basta a invasão do dispositivo informático, com o objetivo “de obter, adulterar ou destruir dados” sem autorização do usuário para configurar a prática do crime.

Rogério Sanches Cunha (2021, *online*) acentua que a retirada da exigência de invasão do dispositivo de segurança viabilizou o enquadramento no tipo apenas

com a invasão não autorizada, uma vez que a falta daquele obstava a configuração do delito:

(...) O tipo penal foi alterado para possibilitar a punição do simples ato de invadir o dispositivo informático com o fim de obter, adulterar ou destruir dados ou informações ou de instalar vulnerabilidades para obter vantagem ilícita.

Para Antonio Milagre (2021, *online*) a invasão se caracteriza da seguinte forma:

Invadir é penetrar hostilmente. O agente que invade, praticando o tipo penal, assim o faz em circunstâncias aqui claramente definidas: a) rompe, acessa fraudulentamente, penetra à força determinado dispositivo; b) ainda que não tenha violado o ativo, que não mais precisa de um “mecanismo de segurança” para estar protegido, o retira da disponibilidade da vítima, ocupa de forma abusiva, toma, tira da vítima, usurpa, remove a vítima da administração ou tenta obter informações fraudulentamente ou que serão usadas (serão próprias) para fraude.

Nessa linha, o sujeito ativo do tipo “invasão de dispositivo informático” pode ser qualquer pessoa, por se tratar de um crime comum. O sujeito passivo, no entanto, pode ser o proprietário do dispositivo invadido, ou apenas o usuário do mesmo, conforme mencionado anteriormente, foi retirada a necessidade de a vítima ser titular do dispositivo para a configuração do crime.

A lei 14.155/2021 trouxe, ainda, uma figura equiparada, disposta no parágrafo primeiro mesmo artigo (BRASIL, 2021, *online*):

Art. 154-A (...)

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

A nova norma fez alterações nos tipos penais de furto e estelionato, incluindo no art. 155, do Código Penal, o parágrafo 4-B, que se trata de uma qualificadora do furto mediante fraude quando o crime for realizado através de dispositivo informático e eletrônico (BRASIL, 2021, *online*):

Art. 155 (...)

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

No que tange ao crime de estelionato, previsto no art. 171 do Código Penal, a lei em comento inseriu o parágrafo 2º-A, criando a qualificadora da fraude eletrônica (BRASIL, 2021, *online*):

Art. 171 (...)

§ 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.

2.2 Lei do Marco Civil da Internet, Lei nº 12.965/2014, e as alterações trazidas pela Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018:

A Lei do Marco Civil na Internet, Lei de nº 12.965/2014, foi editada com o objetivo de estabelecer princípios, garantias, direitos e deveres acerca do uso da *internet* no Brasil, sendo conhecido perante a doutrina como sendo a “Constituição da Internet” (JESUS; MILAGRE, 2016, p. 182).

Antes da promulgação da lei em análise não havia no ordenamento brasileiro uma lei que tratasse do uso da *internet*, principalmente uma que regulasse acerca da manutenção dos dados pelos provedores de *internet*, o que dificultava o trabalho da Polícia Judiciária na fase de investigação.

Nesse contexto, Damásio de Jesus e Antonio Milagre (2016, p. 183) acentuam que:

(...) existia apenas “recomendação” do Comitê Gestor Internet do Brasil, para que os provedores (de acesso) passassem a manter, por prazo mínimo de 3 (três) anos, dados de conexão e de comunicação realizadas por seus equipamentos (identificação do endereço IP, data e hora de início e término da conexão e origem da chamada), o que refletia também o posicionamento do Superior Tribunal de Justiça.

A necessidade de uma legislação que disponha acerca do tema surge em razão da necessidade de cooperação entre terceiros a fim de auxiliar na investigação, principalmente no que tange os crimes informáticos, em que sujeito passivo, “não é administradora do ativo informático utilizado para a prática do crime ou do ativo atacado”(JESUS; MILAGRE, 2016, p. 183).

O art. 3º da referida Lei dispõe acerca dos direitos referentes ao uso da *internet*, quais sejam (BRASIL, 2014, *online*):

Art. 3º (...)

- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;
- IV - preservação e garantia da neutralidade de rede;
- V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- VII - preservação da natureza participativa da rede;
- VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Nessa linha, cabe ressaltar que a Lei nº 12.965/2014, além de dispor acerca dos direitos e garantias quanto ao uso da *internet* no Brasil, também possui aplicabilidade no âmbito Penal e Processual Penal, tendo em vista que a referida norma “estabelece conceitos fundamentais, bem como disciplina formas de obtenção de provas quanto à materialidade e à identificação da autoria delitiva” (BARRETO; BRASIL, 2016, p. 38).

A norma em questão também serve de base na investigação criminal dos *ciber Crimes*, uma vez que trata dos registros de conexão, bem como do acesso de dados pelas autoridades administrativas, conforme acentuam Damásio de Jesus e Antonio Milagre (2016, p. 205):

(...) Lei do Marco Civil da Internet (n. 12.965/2014), trazendo este a obrigatoriedade da guarda de registros de conexão ou acesso a aplicações, regulamentando também o acesso, por autoridades administrativas, aos dados cadastrais de um indiciado ou investigado.

Já a Lei Geral de Proteção de Dados (LGPD), Lei de nº 13.709/2018, fez algumas alterações na Lei do Marco Civil da Internet, com o objetivo de garantir uma maior segurança e transparência no que tange ao tratamento dos dados pessoais dos usuários, sendo um reflexo do regulamento europeu, o *GDPR – General Data Protection Regulation*, que entrou em vigor em 25 de maio de 2018 (MACIEL, 2019, p. 14):

Em 2016, o *General Data Protection Regulation* (GDPR) foi aprovado e em 2018 ele entrou em vigor. Com sua entrada em vigor, em 25 de maio de 2018, os legisladores brasileiros viram-se pressionados a agilizar a votação de um projeto de lei de dados pessoais, caso contrário as empresas brasileiras teriam enorme dificuldade em realizar negócios com europeus, porquanto o país seria considerado não adequado para tratar dados de cidadãos que estiverem localizados na Europa.

A LGPD foi aprovada em agosto de 2018, com *vacatio legis* de 24 (vinte e quatro) meses após sua publicação, entrando em vigor na sua integralidade em agosto de 2020. A referida lei tem como finalidade criar um cenário de segurança jurídica, versando sobre os tratamentos de dados pessoais por pessoa natural, pessoa jurídica de direito público ou privado, buscando garantir a proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive por meio digital” (MACIEL, 2019, p. 17).

Cumprir destacar que a Lei Geral de Proteção de Dados (LGPD) possui âmbito de atuação a todas as operações de tratamento realizadas no Brasil, aplicando-se a todas pessoas que estejam no território brasileiro, sejam elas nacionais ou não, conforme previsão no art. 3º da referida norma (MACIEL, 2019, p.18).

A LGPD define como sendo dados pessoais as informações que identifiquem de forma direta ou indireta um indivíduo, como documento de identidade, CPF, telefone, endereços, fotografias, informações financeiras, dentre outras informações (SERPRO, 2020, *online*).

Um dos pontos mais marcantes do advento da norma aqui estudada é a necessidade do consentimento do titular, a fim de autorizar que seus dados sejam manuseados por empresas ou órgãos públicos (SERPRO, 2020, *online*).

Nessa linha, a LGPD dispõe, ainda, acerca da possibilidade de acesso, retificação de dados, e até mesmo revogação do consentimento antes oferecido pelo usuário.

A nova lei é de grande importância na prevenção dos crimes virtuais, uma vez que dificulta o acesso aos dados pessoais dos indivíduos a potenciais criminosos, o que diminui gradativamente o risco de serem vítimas de *cibercrimes*.

3 DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos recebem pela doutrina diversas nomenclaturas, não existindo um consenso entre os juristas, podendo ser conhecidos como crimes cibernéticos, crimes virtuais, crimes informáticos e até mesmo como crimes tecnológicos por alguns doutrinadores, todos correspondem “de certa forma a todas as condutas tipificadas cometidas com o uso de tecnologia” (NASCIMENTO, 2018, *online*).

Nos crimes cibernéticos o bem jurídico tutelado pelo direito penal é a informática, assim como a integridade dos dados informáticos e a privacidade, conforme acentuam Damásio de Jesus e Antônio Milagre (2016, p. 48):

Elevaram-se, pois, os dados informáticos e os dispositivos ao status de valores jurídicos fundamentais das relações sociais de uma sociedade dependente da tecnologia da informação, protegendo-os. Assim, ao tratarmos de “crime informático”, usamos tal nomenclatura justamente para demonstrar qual o bem jurídico protegido pelo Direito Penal, a informática, ou a privacidade e a integridade dos dados informáticos.

No que tange à conceituação dos crimes virtuais, estes eram considerados como sendo crimes-meios no qual se utilizava a *internet* ou o meio informático para a prática de “crimes comuns”, conforme aduzido por Patrícia Peck Pinheiro (*apud*, JESUS; MILAGRE, 2016, p. 40):

Não é crime-fim por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros.

Atualmente, o *cibercrime* é conceituado por alguns doutrinadores como sendo toda atividade que tem por instrumento a rede computadores, ou “base de ataque como meio de crime” (CASSANTI, 2014, p. 24).

Já Alessandro Barreto (2016, p. 16) define os crimes virtuais como uma subespécie dos crimes tecnológicos, os quais se valem do uso de tecnologias para sua prática, sendo o primeiro aqueles praticados através da *internet*, e apesar de se materializarem no meio virtual, seus efeitos alcançam o mundo real.

Antonio Milagre e Damásio de Jesus (2016, p. 49) entendem de modo diverso, para os juristas crime virtual é um “fato típico e ilícito, cometido através da informática de forma geral, face um sistema, dispositivo informático ou rede de computadores”.

A Convenção de Budapeste de 2001 (*COUNCIL OF EUROPE*, 2001, *online*) define o *cibercrime* como sendo atos praticados face os sistemas informáticos ou a uso fraudulento dos mesmos:

Atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados (...)

Visto isso, pode-se concluir que para haver a configuração de um crime virtual, seja ele um crime-meio ou crime-fim, se faz necessária a utilização de tecnologias, mais precisamente a *internet* para a prática da atividade criminosa.

3.1 Das características dos Crimes Cibernéticos

Em relação ao modo de execução dos crimes cibernéticos, eles são classificados de duas formas pela doutrina, podendo ser crimes virtuais próprios ou puros e também crimes virtuais impróprios ou impuros.

No caso dos crimes virtuais próprios o bem jurídico tutelado é o sistema de informação, o crime se dirige ao sistema informático, banco de dados, arquivos, dentre outros (BARRETO, 2016, p. 17).

São exemplos de crimes informáticos próprios no Código Penal o tipo de “invasão de dispositivo informático” previsto no art.154-A, o crime de dano do art. 163, quando este se destinar a destruição ou deterioração de dados armazenados, bem como os artigos 266 e 313-A, que tratam do tipo de “interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” e o tipo de “inserção de dados falsos em sistema de informações” (BRASIL, 1940, *online*).

Já o crime virtual impróprio pode ser considerado também como um crime-meio, uma vez que o sistema informático é utilizado como instrumento para a prática de determinado tipo, conforme demonstrado por Alexandre Barreto (2016, p. 18):

São aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução ou o seu resultado. Aqui, apenas o veículo em de o crime é praticado é que envolve tecnologia, sendo perfeitamente adequadas diversas figuras típicas previstas no Código Penal Brasileiro ou em leis penais especiais.

Neste contexto, podem ser enquadrados nessa conceituação aqueles crimes previstos na legislação brasileira e para a sua configuração é utilizada a *internet* ou qualquer outro objeto informático, como por exemplo o tipo “induzimento, instigação ou auxílio a suicídio ou a automutilação” prevista no art. 122 do CP, os crimes contra a honra, sendo eles a calúnia, injúria e difamação, previstos nos artigos 138, 139 e 140 do CP, dentre outros tipos (BRASIL, 1940, *online*).

Damásio de Jesus (2016, p. 54) aduz quando diante dos crimes virtuais impróprios as condutas estão abarcadas pelo ordenamento jurídico vigente, tendo em vista que há correlação entre os atos praticados e os tipos penais existentes.

Antonio Milagre e Damásio de Jesus (2016, p. 54) acentuam a existência de outras duas classificações de crimes cibernéticos, os crimes informáticos mistos, em que há a tutela de bens jurídicos distintos, e o crime informático mediato ou indireto:

(...) trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto).

Quanto ao *modus operandi* dos cibercriminosos, Mário Furlaneto Neto e José Augusto Chaves Guimarães (*apud*, DELGADO, 2007, *online*) exemplificam algumas condutas ilícitas, como o *spamming*, *cookies*, *spywares*, *hoaxes*, *sniffer* e cavalo de tróia:

(...) o *spamming*, que é utilizado como forma de envio de e-mails indesejados por meio do correio eletrônico para os usuários; *cookies*, que são pequenos arquivos de textos que são armazenados no computador do internauta para a obtenção de informações relativas ao consumidor, como, por exemplo, a frequência com que o mesmo costuma visitar o site, entre outros; *spywares*, que são programas espiões que expedem informações do internauta à desconhecidos; *hoaxes* são e-mails que possuem conteúdo falso onde, usualmente, os criminosos colocam, como remetente, empresas de grande

renome ou órgãos governamentais, podendo ainda estar vinculado a vírus; *sniffer*, que também são programas espiões, mas que são implantados no disco rígido, visando rastrear e reconhecer e-mails que estão na rede, com a finalidade de os controlar e os ler; cavalo de troia, que, quando instalado, abre a possibilidade do roubo de informações, dados, senhas, arquivos, entre outros, sendo esta a espécie mais perigosa e destrutiva referente aos crimes cibernéticos.

No tocante ao sujeito ativo dos crimes cibernéticos próprios, estão os *hackers* e *crackers*, sendo aqueles os mais conhecidos. Cassanti (2014, p. 22) afirma que embora ambos sejam grandes conhecedores do mundo virtual principalmente no que se refere aos sistemas e programações, há diferença entre eles. Os *hackers* não objetivam causar danos ou o cometimento de crimes:

O termo hacker, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é aplicada pela própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas.

O que se difere dos *crackers* que empregam seus conhecimentos para a prática de crimes (CASSANTI, 2014, p. 22):

Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos.

Além dos *hackers* e *crackers*, existem os conhecidos como *carders* e *phreakers*, os primeiros praticam estelionatos por meio de fraudes com cartões, já os *Phreakers* se refere aos criminosos que praticam suas ações por meio da telefonia, como por exemplo, com a realização de interceptações (JESUS; MILAGRE, 2016, p. 60).

3.2 Competência para processar e julgar os crimes cibernéticos:

A territorialidade referente aos crimes virtuais é motivo de certa controvérsia na doutrina, mesmo com previsão no Código Penal e Processo Penal brasileiro.

A regra geral referente a fixação da competência para o processamento e julgamento dos crimes virtuais está prevista no art. 69 do Código de Processo Penal,

já o art. 6 do Código Penal, dispõe acerca do princípio da ubiquidade (BRASIL, 1940, *online*):

Art. 6. Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Acerca do referido princípio o jurista Rogério Greco (2017, p. 46) dispõe que o mesmo resolve alguns problemas referente ao possível conflito de jurisdição entre países:

A adoção da teoria da ubiquidade resolve problemas de Direito Penal Internacional. Ela não se destina à definição de competência interna, mas, sim, à determinação da competência da justiça brasileira. Embora competente a justiça brasileira, pode acontecer que, em virtude de convenções, tratados e regras de Direito Internacional, o Brasil deixe de aplicar a sua lei penal aos crimes cometidos no território nacional.

Todavia, o Superior Tribunal de Justiça (STJ, 2015, *online*) entendeu no Conflito de Competência de nº 136.700 / SP que o local do crime será o local da hospedagem do *site* utilizado para a prática do mesmo:

(...) Então, o *punctum saliens* está em saber se a competência se firma pelo local onde fica a sede de quem hospeda determinado domínio ou pelo local do titular do próprio domínio e que criou a home page em que se abastecerá seu conteúdo. Em uma palavra: o local do provedor não se confunde com o local da home page que veicula determinada informação, o que não significa dizer que eles possam ser coincidentes quando, por exemplo, o próprio provedor tenha e hospede sua home page, v.g., "Uol empresas".

A partir disso, surge o questionamento quanto à competência dos crimes praticados pelo meio virtual através de sites hospedados no exterior (ROCHA; CERQUEIRA, 2013, p. 16), neste ponto estamos diante de uma clara omissão legislativa.

Ainda no que se refere à competência, Vladimir Delgado (2007, *online*) aduz acerca da Soberania dos Estados, que definem sua fixação a partir de critérios estabelecidos pela sua legislação interna:

A competência dos Estados é determinada pelos critérios estabelecidos em suas respectivas leis internas, que podem adotar, além do princípio geral da territorialidade da lei penal, também outros critérios de extraterritorialidade, conforme previsão legal interna.

Outro problema encontrado referente a competência é quando a vítima do crime está situada no Brasil, mas o agente criminoso está situado no exterior ou utiliza artifícios a fim de ocultar a origem da conexão (JESUS; MILAGRE, 2016, p. 62):

Logicamente que a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que este agente adentre no território nacional. Logo, crimes cometidos por meio de proxies, vpns, entre outros recursos para mascarar a origem da conexão, onde o agente está no Brasil e só se vale de uma conexão do exterior, podem ser processados aqui, desde que, claro, identificado o criminoso. E aí reside mais um problema, pois provedores estrangeiros muitas vezes se recusam a fornecer dados de acesso a aplicações feitas por brasileiros, mas armazenados no exterior.

Cabe ressaltar que será de competência da Justiça Federal os crimes virtuais praticados face interesses, bens e serviços da União, conforme previsão no art. 109, IV da Constituição da República (BRASIL, 1988, *online*).

Mesmo não existindo na legislação um critério de fixação de competência próprio para os crimes cibernéticos, o art. 70 do Código de Processo Penal (BRASIL, 1941, *online*), dispõe que será competente o lugar em que se consumar a infração, ou em caso de tentativa o local da prática do último ato, e no parágrafo segundo do mesmo artigo, o juiz competente será o do local onde o crime se consumou ou deveria produzir o resultado, no caso de a ação ter se iniciado no exterior.

Visto isso, além da necessidade de uma harmonia legislativa internacional quanto os *ciber Crimes*, se faz necessária uma cooperação entre os Estados visando a repressão dos crimes virtuais, o que será abordado de forma mais aprofundada posteriormente.

4 DAS DIFICULDADES ENFRENTADAS PELO BRASIL NO COMBATE AOS CRIMES CIBERNÉTICOS

Conforme citado anteriormente o processo de informatização e globalização da sociedade oriunda da evolução das tecnologias acabou ocasionando uma sofisticação na prática de crimes, conforme dispõe Guilherme Nucci (2019, p. 882):

A globalização da economia, dos meios de comunicação, do mercado financeiro, dos transportes, do turismo, entre outros fatores, trouxe também a globalização do crime tipo de delito por meio de um direito penal eficiente, sem perder de vista as conquistas trazidas pelos direitos humanos fundamentais.

São encontrados alguns obstáculos na fase de investigação da prática dos referidos crimes, tendo em vista que os procedimentos a serem adotados pelas autoridades são diferentes dos procedimentos dos crimes comuns.

O presente capítulo abordará alguns dos muitos empecilhos encontrados na fase da persecução penal concernente a esses crimes, além de expor dados atualizados acerca dos crimes cibernéticos no Brasil.

4.1 Os desafios na fase da persecução penal

A fase investigativa objetivada na busca de indícios de autoria e materialidade para indiciar e punir os autores dos crimes cibernéticos é um desafio para as autoridades brasileiras, principalmente para a polícia judiciária, uma vez que são encontrados diversos fatores que dificultam a coleta das provas necessárias para se iniciar a ação penal (ROCHA; CERQUEIRA, 2013, p. 8).

A ausência da tecnologia necessária é considerada para Claudionor Rocha e Sílvia Castro Cerqueira (2013, p. 8) como sendo um dos problemas técnicos encontrado pela polícia na fase investigatória:

Existem tipos penais específicos que incluem o uso de recursos de alta tecnologia no núcleo das condutas como elementar do tipo, isto é, só cabem quando é usado o recurso de alta tecnologia, ou o recepcionam diretamente como meio propiciador da conduta.

Além disso, Claudionor Rocha (2013, p. 15) aduz, ainda, acerca da necessidade de uma maior capacitação dos profissionais para estes possam se tornar mais aptos e adquirirem êxito na fase investigatória:

Não obstante, para assegurar o sucesso das investigações soluções incrementais são essenciais, como as novas legislações, treinamento para agências policiais e a cooperação policial e jurídica internacional.

Normalmente para que haja a coleta de vestígios do crime virtual as autoridades se valem da interceptação telemática como meio de obtenção de prova, que consiste na captação de dados dos serviços informáticos de comunicação (ROCHA; CERQUEIRA, 2013, p. 15):

No caso da interceptação telemática, a obtenção do trânsito de dados de internet do investigado pode ser buscada no local de trabalho, residência, instituição de ensino, no smartphone ou outro meio. Entretanto, apenas mediante técnicas de intrusão se poderia reproduzir todo o movimento de navegação.

Todavia, para que haja a interceptação telemática é necessária prévia autorização judicial, conforme dispõe o art. 1º da Lei de nº 9.296/96 (BRASIL, 1996, *online*):

Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática

Não pode ocorrer a interceptação caso não haja indícios razoáveis de autoria e materialidade, a possibilidade de obter essa prova por outro meio, e não sendo possível também na hipótese de o crime investigado ser punido apenas com a pena de detenção, nos termos do art. 2ª da lei supramencionada.

Damásio de Jesus e Antônio Milagre (2016, p. 185) demonstram que os usuários tem direito à inviolabilidade e ao sigilo de suas comunicações na *Internet*, ressalvado em caso de autorização judicial, para fins de investigação criminal, nos

termos do disposto no art. 7º, inciso I da Lei do Marco Civil da Internet – Lei nº 12.965/2014.

Cumprido destacar que a não observância das hipóteses previstas na legislação importa na ilicitude da prova, que não poderá ser utilizada para incriminar o acusado, sendo inadmissível, conforme disposto no art. 5º, inciso LVI da Constituição Federal (BRASIL, 1988, *online*), ratificada pelo art. 157 do Código de Processo Penal (BRASIL, 1941, *online*):

Art. 5, LVI, CR: são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

Art. 157, CPP: São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

Outro problema enfrentado pela polícia judiciária é descobrir o IP (*Internet Protocol*), o número que identifica a origem da conexão, uma vez que os cibercriminosos conseguem mascarar-lo (ROCHA; CERQUEIRA, 2013, p. 16):

Uma das maiores dificuldades na investigação de crimes cibernéticos é descobrir o IP da origem de uma conexão, que pode ser burlado com o uso de recursos técnicos de mascaramento, de proxies (que facilitam a navegação em redes privadas), de hotspots (pontos de acesso à internet) como redes wifi abertas (aeroportos, por exemplo), cyber cafés e lanhouses. Dificuldades adicionais ocorrem com a inserção de dados falsos no cadastro da conta do usuário, além do uso de documento falso nesse cadastro.

Nesse sentido, Damásio de Jesus (2016, p. 185) aduz de acordo com a Lei do Marco Civil da Internet – Lei nº 12.965/2014 que os provedores de *internet* somente serão obrigados a fornecerem informações que auxiliem na identificação dos usuários por meio de ordem judicial.

Claudionor Rocha e Sílvia Castro Cerqueira (2013, p. 22) expõem, ainda, no caso de crimes praticados por meio de serviços de correio eletrônico com sede em outros países, os procedimentos regulados pela lei denotam uma certa demora, e em razão da rapidez com que os vestígios desaparecem no meio virtual, essa demora acaba gerando a impunidade alguns crimes.

Como atualmente este procedimento apresenta acentuada demora, o recebimento da resposta não apresentaria nenhum valor prático para

a persecução penal, pois a volatilidade da prova eletrônica faria desaparecer os indícios ainda existentes no território nacional, que somente poderiam ser encontrados com as informações oriundas do estrangeiro, redundando em impunidade ao autor do crime e irreparável prejuízo às vítimas e à sociedade, que se vê desde há muito, desamparada.

Sob este prisma deve ser observado o disposto no art. 386, incisos IV e V, do Código de Processo Penal (BRASIL, 1941, *online*), no caso de não haver provas suficientes para demonstrar que o réu concorreu para a ação penal o juiz deve absolvê-lo em consonância com o princípio do *in dubio pro reo*.

Com o estudo dos desafios citados anteriormente resta evidente que é necessário por parte do Estado brasileiro uma adaptação face as novas modalidades de crimes, principalmente no que se refere a preparação dos profissionais responsáveis pela investigação dos delitos, bem como o fornecimento de tecnologias necessárias a fim de auxiliar nas investigações (ROCHA; CERQUEIRA, 2013, p. 18).

4.2 Dados sobre os crimes cibernéticos

De acordo com uma pesquisa feita pela ONG *Safernet* Brasil (*SAFERNET*, 2020, *online*) em parceria com o Ministério Público Federal, foram realizadas no ano de 2020, 156.692 denúncias anônimas a respeito de crimes praticados no meio virtual.

Cumprе destacar que os dados são referentes aos crimes virtuais impróprios, em que a *internet* foi utilizada apenas como um instrumento para a prática dos crimes.

Dentre os dados, 98.244 denúncias são referentes a crimes relacionados à pornografia infantil, 12.698 são sobre violência ou discriminação contra as mulheres e 11.852 são sobre apologia e incitação à prática de crimes contra a vida (*DATASAFER*, 2020, *online*).

Segundo o *Norton Cyber Security Insights Report de 2017* (*NORTON*, 2018, *online*) o Brasil perdeu cerca de 22,5 bilhões de dólares em razão dos crimes cibernéticos, sendo o segundo da lista.

Dos dados, 20% (vinte por cento) das vítimas utilizavam a mesma senha para várias outras contas *online* e 58% (cinquenta e oito por cento) das mesmas compartilhavam suas contas e senhas com outras pessoas (NORTON, 2018, *online*).

Algumas pesquisas mostraram que em decorrência da pandemia do COVID-19 houve uma maior demanda do uso da internet por parte da população, o que acabou gerando também um aumento de golpes através da *internet*, conforme uma pesquisa realizada pela FEBRABAN (Federação Brasileira de Bancos), que demonstra um aumento de 340% da prática “do golpe da falsa central telefônica e do falso funcionário” nos meses de janeiro e fevereiro de 2021 em comparação com o ano de 2020 (FEBRABRAN, 2021, *online*).

Além disso, os golpes conhecidos como *phishing*, que consiste geralmente no envio de mensagens ou e-mails falsos objetivando a obtenção de dados das vítimas, dobrou em relação ao ano de 2020 (FEBRABRAN, 2021, *online*).

Esses dados demonstram a necessidade de uma adaptação do Estado brasileiro no que se refere ao enfrentamento dos crimes virtuais, que vem crescendo e se sofisticando gradativamente a cada ano (BONONI, 2021, *online*).

5 DOS POSSÍVEIS MEIOS DE COMBATE AOS CRIMES CIBERNÉTICOS

A coleta de provas nos crimes virtuais pode vir a ser um problema para os Estados, tendo em vista seu caráter transnacional, o que faz com que seja necessário o auxílio de outros Estados para a obtenção de meios que identifiquem e indiciem os criminosos (DELGADO, 2007, *online*).

Um mecanismo utilizado é a cooperação jurídica internacional, dessa forma, o presente capítulo irá aduzir alguns possíveis meios a serem utilizados pelo Estado a fim auxiliar na coleta de provas dos crimes que extrapolem os limites da jurisdição do Brasil.

Além de tratar de aspectos importantes da Convenção de Budapeste (COUNCIL OF EUROPE, 2001) no combate aos cibercrimes.

5.1 Da Cooperação Jurídica Internacional

Conforme exposto anteriormente o *modus operandi* dos criminosos referentes aos crimes virtuais são diferentes à prática dos crimes considerados comuns, podendo o primeiro possuir um caráter transnacional, dessa forma, surge a necessidade de adoção de meios que visem suprimir tais condutas sem ferir o princípio da territorialidade da lei penal (DELGADO, 2007, *online*).

Vladimir Delgado (2007, *online*) aduz que a cooperação jurídica internacional pode ser uma solução para este empecilho:

O caráter transnacional das redes informáticas oferece novas possibilidades tanto para a prática de crimes informáticos, como de crimes tradicionais. A natureza transnacional destas infrações, como por exemplo, quando cometidas através da Internet, opõe obstáculos à persecução penal, em virtude do princípio da territorialidade da lei nacional. Diante desse quadro, a cooperação internacional em matéria penal constitui elemento fundamental para que se proteja a sociedade do moderno fenômeno da “criminalidade informática”.

Neste contexto, Ilana Muller (2013, p. 25) entende que “os tratados internacionais, bilaterais ou multilaterais, relativos à cooperação jurídica internacional conferem maior segurança aos Estados e aos jurisdicionados”.

Lessa (2009, p. 49) apregoa, ainda, a possibilidade de utilização da cooperação jurídica internacional pelas autoridades brasileiras não só nos crimes de

natureza transnacional, mas também sempre que tal mecanismo for eficiente para supressão de alguns delitos:

Não só a persecução local de delitos transnacionais é a regra, como, também, a persecução local dos delitos previstos pelo Direito Internacional é vista como a melhor opção sob qualquer aspecto que se observe a questão. Além disso, outros princípios, concorrem para incentivar os Estados a trabalhar em conjunto na repressão à criminalidade.

A cooperação jurídica internacional é conceituada como sendo um instrumento formal por meio do qual um Estado, com a finalidade de auxílio em algum procedimento, solicita a outro Estado medidas, tanto administrativas quanto judiciais que detenham caráter judicial em um Estado visando a elucidação acerca de alguma questão (BRASIL, 2014, *online*).

Nádia de Araújo (2016, *online*) entende que a cooperação jurídica consiste como sendo um “intercâmbio internacional para o cumprimento extraterritorial de medidas processuais provenientes do Judiciário de um Estado estrangeiro”.

Vladimir Delgado (2007, *online*), diferente do conceito acatado por Nádia de Araújo, abrange a concepção de cooperação jurídica internacional a fim de incluir também as medidas e atividades administrativas:

(...)tratar-se-á de cooperação internacional em matéria penal quando o aparato administrativo ou judicial de um Estado recorrer à colaboração que lhe podem prestar outros Estados, por meio de suas atividades jurisdicionais ou administrativas, em matéria de natureza criminal.

O mesmo autor aduz que não há pela doutrina um direito e um dever de cooperação entre os Estados, resultante de um princípio geral do direito, a obrigação é decorrente de acordos realizados entre os mesmos (DELGADO, 2007, *online*):

O direito e o dever de cooperação penal internacional resultam apenas de convênios expressos firmados entre os Estados. Assim, a prestação de cooperação internacional em matéria penal apenas adquire o caráter de uma obrigação juridicamente vinculatória entre os Estados, mediante a prévia formulação de um convênio expresso, em que se estipulem as regras da cooperação.

No Brasil a autoridade responsável pela execução de atividades referentes à cooperação jurídica internacional, denominada como "autoridade central", é o Ministério da Justiça, por meio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) e do Departamento de Estrangeiros (DEEST), conforme disposto no Decreto nº 6.061/2007 (BRASIL, 2014, *online*).

Os mecanismos mais comuns utilizados pelo Brasil concernente à cooperação jurídica entre os países é a Carta Rogatória e o Auxílio Direto (BRASIL, 2014, *online*).

Milton Fornazari (2016, p. 27) demonstra que o primeiro instrumento, a carta rogatória, é um dos meios tradicionais que os países recorrem a fim de requerer a produção de determinados atos em outro país, podendo ser utilizada para intimações, citações etc:

A carta rogatória é meio tradicional utilizado por um Estado soberano, por sua Jurisdição, para solicitar que se produza atos processuais em outro território soberano, visando a produção e coleta de provas ou de qualquer outro ato de instrução processual. A solicitação é sempre expedida por uma autoridade judicial à outra equivalente de outro país. Destina-se (sic) à citação de réu ou investigado domiciliado no exterior (com endereço certo), oitivas, intimações, etc.

Já o auxílio direto é semelhante à carta rogatória, mas é um mecanismo mais célere, uma vez que não passa pelos mesmos procedimentos da segunda, não sendo necessário o *exequatur* ou homologação do ato jurisdicional estrangeiro (BRASIL, 2014, *online*).

Uma vez demonstrado o instituto da cooperação jurídica internacional pode-se chegar ao entendimento que o referido instituto é um grande aliado no combate aos crimes cibernéticos, tendo em vista que por meio do mesmo é garantido aos Estados a possibilidade de obtenção de provas visando a demonstração de autoria e materialidade dos delitos (DELGADO, 2007, *online*)

5.2 Um estudo sobre a ratificação do Brasil à Convenção de Budapeste como uma possível solução ao combate aos crimes cibernéticos

A Convenção sobre Cibercrimes ou Convenção de Budapeste, foi criada pelo Conselho da Europa em 2001, com o objetivo de combater os crimes praticados por

meio da *internet* com foco no auxílio mútuo entre os Estados (*COUNCIL OF EUROPE*, 2001, *online*).

A referida Convenção (*COUNCIL OF EUROPE*, 2001) é composta por quatro capítulos: I- “Terminologia”; II- “Medidas a tomar em nível nacional”, III- “Cooperação internacional” e IV- “Disposições finais”.

O primeiro capítulo traz algumas definições acerca do significado de sistema informáticos, dados informáticos, fornecedor de serviços e dados de tráfego (*COUNCIL OF EUROPE*, 2001, *online*):

Artigo 1º - Definições Para os fins da presente Convenção:

- a) “Sistema informático” significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
- b) “Dados informáticos” significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;
- c) “Fornecedor de serviço” significa: (i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e (ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.
- d) “Dados de tráfego” significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Um fato interessante do referido tratado é o texto do capítulo segundo, que dispõe acerca de condutas a serem tipificadas no âmbito interno dos países signatários, para que haja uma harmonização legislativa entre os mesmos (*DELGADO*, 2007, *online*).

Já o capítulo terceiro dispõe acerca da cooperação internacional, tratando da extradição e do auxílio mútuo em matéria penal. O referido Capítulo encontra-se subdividido em duas Seções (*DELGADO*, 2007, *online*).

A convenção citada foi aderida por 60 (sessenta) países, estando aguardando os trâmites de votação na câmara dos deputados, após será encaminhada ao Senado Federal para a ratificação pelo Brasil (*ANPR*, 2021, *online*).

Alguns órgãos demonstraram apoio à ratificação da referida norma, em razão do gradativo aumento da criminalidade cibernética, conforme exposto pela Associação Nacional dos Procuradores da República –ANPR (ANPR, 2021, *online*):

Nos 15 anos de atividade dos grupos, verificou-se aumento exponencial na quantidade e sofisticação no cometimento dos delitos cibernéticos, com a migração de delitos comuns como fraudes, estelionatos, ameaças e extorsões para o meio digital que não têm encontrado nem capacitação para o seu combate, nem ferramentas jurídicas aptas a permitir a persecução penal efetiva, aumentando a insegurança da vida diária e dificultando a prevenção.

Nesse cenário, a Convenção do Cibercrime (2001) conta com mais de 60 países aderentes, apresenta-se como um instrumento eficaz de cooperação internacional para a obtenção de provas digitais, além de inserir o Brasil no mapa do combate ao crime cibernético.

Diante da necessidade de uma legislação que trate da tipificação dos delitos informáticos e garanta meios de enfrentamento dos crimes cibernéticos, a ANPR fez um pedido em nota técnica à Câmara de Deputados, assinada pelas Coordenadoras do Grupo de Apoio sobre Criminalidade Cibernética da 2ª CCR, Neide Cardoso de Oliveira e Fernanda Teixeira Domingos, para que o Brasil ratifique a convenção supramencionada (ANPR, 2021, *online*).

Além da ANPR, o Ministério Público Federal- MPF (BRASIL, 2021, *online*), também demonstrou apoio à adesão do tratado pelo Brasil:

Para o Ministério Público Federal, a Convenção do Cibercrime é útil não somente para a persecução de crimes cibernéticos, mas principalmente para a obtenção das 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 se pereçam ou sejam omitidas. A nota técnica aponta a convenção como instrumento eficaz para a aquisição de tais provas, em razão da existência da Rede 24/7 em todos os países que aderiram a Convenção.

Em outubro do ano de 2021, a câmara de deputados aprovou a adesão do Brasil à Convenção de Cibercrime, PDL 255/2021, sendo favorável ao voto do relator deputado Victor Hugo, no sentido de que a referida norma supriria eventuais omissões existentes no ordenamento vigente (BRASIL, 2021, *online*):

A demanda pela adesão do Brasil vem somar-se à Lei 12.965/2014 – o Marco Civil da Internet, visando suprir a carência por um marco equivalente na seara criminal que delimitasse parâmetros para a persecução penal de tais crimes que, por sua própria natureza, transcendem as fronteiras geográficas.

Como foi aprovada na referida Câmara a Convenção foi encaminhada ao Senado Federal para prosseguimento dos trâmites legislativos.

A Convenção de Budapeste se mostra um meio eficaz no combate aos crimes cibernéticos, tendo em vista que além de dispor acerca de uma homogeneização legislativa referente aos crimes virtuais entre os países, trata também de técnicas de cooperação entre os mesmos (BRASIL, 2021, *online*).

Nessa linha, Tais Vasconcelos Cidrão, Antônio Walber Muniz e Ana Abigail Costa Vasconcelos Alves (2018, *online*) dispõem que o tratado em análise é considerado como o único meio jurídico com caráter internacional eficiente no combate aos crimes virtuais.

6 CONCLUSÃO

Conforme demonstrado no decorrer do presente estudo, nos últimos anos houve um aumento exponencial acerca do uso da *internet* no Brasil e no mundo, decorrente da globalização, o que favoreceu a evolução da prática de crimes nesse meio.

Sob este prisma foi observado que o Estado brasileiro, a fim de se adequar e suprimir tais delitos, criou algumas leis tratando do uso da internet no Brasil, dados pessoais e tipos penais criminalizando algumas condutas.

Uma das primeiras normas a tratar dos crimes cibernéticos no Brasil foi a Lei nº 12.737/2012, que deu origem ao tipo penal de “invasão de dispositivo informático”, sendo de grande importância. Todavia, mesmo com o advento da lei em comento, ficaram algumas lacunas em aberto, o que acabava gerando a impunidade de algumas condutas, em razão da condutado agente criminoso não se enquadrar totalmente no tipo do art. 154-A do Código Penal.

A lei nº 14.155/2021 foi promulgada com o objetivo de pôr fim a essas lacunas, garantindo uma maior proteção à privacidade, bem jurídico tutelado pelo tipo penal supramencionado.

Além de retirar a necessidade do dispositivo de segurança para a configuração do tipo de “invasão de dispositivo informático”, a referida norma, ainda, abrangeu a proteção do sujeito passivo do tipo para usuário do dispositivo, não sendo necessário que a vítima seja o titular do dispositivo violado.

A criação da Lei do Marco Civil na Internet também foi de igual importância para o ordenamento jurídico brasileiro, uma vez que foram estabelecidas normas acerca do uso da *internet* no Brasil, tratando também da responsabilidade dos provedores de *internet* no país.

Quanto aos crimes cibernéticos, que podem ser classificados como próprios ou impróprios, foi observado que algumas condutas do segundo encontram correspondência com tipos penais já existentes no ordenamento jurídico brasileiro.

Contudo, são encontrados alguns empecilhos no que se refere a investigação e competência dos crimes virtuais, o primeiro está relacionado a ausência de preparo das autoridades policiais que não possuem o treinamento adequado e equipamentos eficientes para auxiliar nas investigações.

Dessa forma, foi verificada a dissonância existente entre os cibercriminosos que estão em constante evolução no cometimento de crimes e as autoridades brasileiras, que por não possuírem os equipamentos adequados cominado com fato de que os vestígios dos crimes virtuais desaparecem com uma maior rapidez que a dos crimes comuns, acaba gerando a impunidade de alguns crimes.

Além disso, os crimes cibernéticos possuem natureza transnacional, o que facilita a ocorrência de conflitos de competência envolvendo Estados soberanos.

Por isso, a cooperação jurídica internacional entre os países é de suma importância no combate aos crimes cibernéticos. Todavia, ela por si só também não é suficiente no enfrentamento dos referidos crimes, haja vista que os procedimentos adotados atualmente nessas hipóteses são morosos o que favorece o desaparecimento dos vestígios dos crimes virtuais.

Sendo assim, a ratificação pelo Brasil à Convenção de Budapeste (2001) se mostra de grande evolução no enfrentamento dos crimes cibernéticos, tendo em vista que a referida convenção além de propor uma harmonia legislativa entre os Estados no que se refere aos crimes cibernéticos, dispõe, ainda, acerca de meios de cooperação a serem utilizados pelos Estados na repressão desses delitos, mostrando-se mais eficiente que procedimentos adotados atualmente no Brasil.

REFERÊNCIAS

ANPR, **ANPR pede que comissão da Câmara ratifique convenção sobre crime cibernético**. Disponível em: <<https://www.anpr.org.br/imprensa/noticias/25025-anpr-pede-que-comissao-da-camara-ratifique-convencao-sobre-crime-cibernetico>> Acesso em 16 out. 2021.

_____. **Câmara aprova adesão do Brasil à convenção de crimes cibernéticos**. Disponível em: <<https://www.anpr.org.br/imprensa/noticias/25776-camara-aprova-adesao-do-brasil-a-convencao-de-crimes-ciberneticos>> Acesso em 16 out. 2021.

ARAUJO, Nádia de. **Direito Internacional Privado: Teoria e Prática Brasileira**. 1. ed. Porto Alegre: Revolução e-Book, 2016.

BRASIL. **Câmara dos Deputados. PDL 255/2021. Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais**. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513>>. Acesso em 16 out. 2021.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Texto constitucional promulgado em 5 de outubro de 1988. Disponível: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 04 nov. 2021.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. (1940). **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 08 out. 2021.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. (1941). **Código de Processo Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 15 out. 2021.

_____. **Lei Nº 9.296, de 24 de julho de 1996**. (1996). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 10 de out. 2021.

_____. **Lei Nº 12.727, de 30 de novembro de 2012**. (2012). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 26 de fev. 2021.

_____. **Lei Nº 12.965, de 23 de abril de 2014**. (2014). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 de fev. 2021.

_____. **Lei Nº 13.709, de 14 de agosto de 2018**. (2018). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 de out. 2021.

_____. **Lei Nº 14.155, de 27 de maio de 2021.** (2021). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 17 de out. 2021

_____. Ministério da Justiça. **Cartilha Cooperação Jurídica Internacional em matéria Penal.** Brasília, DF, 2012. Disponível em: <<https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/cartilha-penal-09-10-14-1.pdf>>. Acesso em: 12 out. 2021.

_____. Ministério Público Federal. **MPF defende adesão do Brasil à convenção internacional para combate a crimes cibernéticos.** Disponível em: <<https://mpf.jusbrasil.com.br/noticias/623847312/mpf-defende-adesao-do-brasil-a-convencao-internacional-para-combate-a-crimes-ciberneticos>>. Acesso em 13 out. 2021.

_____. Superior Tribunal de Justiça. Conflito de Competência nº 136.700 / SP– São Paulo. Relator: Ministro Rogerio Schietti Cruz. **Pesquisa de Jurisprudência,** Acórdãos, 01 de outubro de 2015. Disponível em: <<https://scon.stj.jus.br/SCON/pesquisar.jsp>>. Acesso em: 12 out. 2021.

BARRETO, Alessandro Gonçalves e BRASIL, Beatriz Silveira, **Manual de investigação cibernética: à luz do marco civil da internet.** 1ª ed. Rio de Janeiro; Brasport; 2016.

BONONI, Fernando, **Crimes Cibernéticos- Avanço Legislativo no Brasil.** Disponível em: <<https://www.migalhas.com.br/depeso/347513/crimes-ciberneticos--avanco-legislativo-no-brasil>> Acesso em 09 dez. 2021.

CASSANTI, Moisés de Oliveira, **Crimes Virtuais- vítimas reais.** 1ª ed. Rio de Janeiro: Brasport, 2014.

CERQUEIRA, Sílvia Castro e ROCHA, Claudionor. **Crimes cibernéticos: desafios da investigação.** *In:* Cadernos As legis. Brasília, n.49, p. 131-136, mai/ago 2013. Disponível em: <<http://bd.câmara.gov.br/bd/handle/bdcamara/27420>>. Acesso em 18 set. 2021.

CIDRÃO, Tais Vasconcelos; MUNIZ, Antônio Walber e ALVES, Ana Abigail Costa Vasconcelos. **A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira.** Disponível em: <<https://revistas.marilia.unesp.br/index.php/bjir/article/view/7069>> Acesso em 05 de nov. 2021.

COUNCIL OF EUROPE. **Convention on Cybercrime. Budapest, 23. XI. 2001.** Disponível em: <<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>> Acesso em: 16 out. 2021.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP.** Disponível em:

<<https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/>>. Acesso em 01 nov. 2021.

DATASAFER, **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, 2020**. Disponível em: <<https://indicadores.safernet.org.br/>>. Acesso em 25 set. 2021.

DELGADO, Vladimir Chaves, **Cooperação Internacional em Matéria Penal na Convenção sobre Cibercrime**. Dissertação (Mestrado em Direito das Relações Internacionais) - Centro Universitário de Brasília, Brasília, 2007.

FEBRABAM. **Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet**. Disponível em: <<https://febraban.org.br/noticia/3631/pt-br/>>. Acesso em: 25 set. 2021.

FORNAZARI JUNIOR, Milton. **Cooperação Jurídica Internacional: Auxílio direto penal**. 2 ed. Rio de Janeiro: Editora Lumen Juris, 2016.

GOV.BR. **Serpro e LGPD: segurança e inovação**. Gov.br. Disponível em: <https://www.serpro.gov.br/lgpd>. Acesso em: 30 ago. 2021.

GRECO, Rogério. **Código Penal: comentado**. 11. ed. – Niterói, RJ: Impetus, 2017.

JESUS, Damásio de; atualização ESTEFAM, André. **Direito penal parte geral vol. 1**, 37. ed. São Paulo: Saraiva Educação, 2020.

_____. Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. 1 ed. São Paulo: Saraiva, 2016.

LESSA, Luis Fernando Voss Chagas. **A assistência direta e a persecução penal internacional transnacional pelo Ministério Público brasileiro**. Tese (Doutorado) – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2009.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. 1ª Ed. Goiânia – GO. Ed. RM Digital Education; 2019.

MILAGRE, José Antonio. **Lei de crimes informáticos (14.155/2021): Aspectos técnicos controvertidos e critérios para caracterização do crime de “invasão de dispositivo informático”**. Disponível em: <<https://direitodigital.adv.br/artigos/lei-de-crimes-informaticos-14-155-2021-aspectos-tecnicos-controvertidos-e-criterios-para-caracterizacao-do-crime-de-invasao-de-dispositivo-informatico/>>. Acesso em 02 nov. 2021.

MULLER, Ilana. **Cooperação jurídica internacional em matéria penal e seus reflexos no direito à prova no processo penal brasileiro**. Tese (Doutorado) - Universidade de São Paulo, São Paulo, 2013.

NASCIMENTO, Talles Leando Ramos. **Crimes Cibernéticos**. Disponível em: <<https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>>. Acesso em 09 dez. 2021.

NORTON, 2017 ***Norton Cyber Security Insights Report, 2018***. Disponível em <<https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/>>. Acesso em 25 set. 2021.

NUCCI, Guilherme de Souza, **Curso de Direito Penal: parte geral: arts. 1º a 120 do Código Penal**. 3. ed. Rio de Janeiro: Ed. Forense, 2019.