PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

A ATUAÇÃO DO MINISTÉRIO PÚBLICO NO COMBATE AOS CRIMES CIBERNÉTICOS

ORIENTANDO: VICTOR SHIN ITI MONTEIRO TAKAHASHI
ORIENTADOR: PROF. DR. FAUSTO MENDANHA GONZAGA

GOIÂNIA-GO
2022

VICTOR SHIN ITI MONTEIRO TAKAHASHI

A ATUAÇÃO DO MINISTÉRIO PÚBLICO NO COMBATE AOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás
Prof. Orientador: Dr. Fausto Mendanha Gonzaga.

O aluno orientando (autor do presente trabalho) declara para os devidos fins que procedeu à revisão do presente artigo para fins de detecção de plágio, assumindo, de forma exclusiva, a responsabilidade por incorporação de textos de terceiros, sem a devida citação ou indicação de autoria.

GOIÂNIA-GO

2022

VICTOR SHIN ITI MONTEIRO TAKAHASHI

A ATUAÇÃO DO MINISTÉRIO PÚBLICO NO COMBATE AOS CRIMES CIBERNÉTICOS

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): FAUSTO MENDANHA GONZAGA Nota:

_____

Examinador Convidado: Prof.: Nota:

SUMÁRIO

A ATUAÇÃO DO MINISTÉRIO PÚBLICO NO COMBATE AOS CRIMES CIBERNÉTICOS

VICTOR SHIN ITI MONTEIRO TAKAHASHI

O presente trabalho tem por objetivo analisar a cibercriminalidade no contexto brasileiro mostrando de que forma o Ministério Público atua nesses tipos de crimes. Para abordar essa problemática foi necessário trazer os principais tipos de crimes virtuais no Brasil e suas características. Além disso, elencar a legislação penal brasileira mostrando de que forma ela opera na tipificação dos cibercrimes e as mudanças na lei já ocorridas para se adaptar à diversificação desses crimes. O estudo tem como foco central analisar a temática do Ministério Público como órgão investigativo e fiscalizador. De que forma ele atua na esfera jurídica combatendo a criminalidade no ambiente digital e criando políticas de controle utilizando outros órgãos para atingir seu objetivo.

Palavras-chave: Cibercrimes. Ministério Público. Investigação.

INTRODUÇÃO

O crescimento exponencial da rede mundial de computadores revelou-se como um fator de mudança no espaço, modificando a realidade do ser humano. Cabe salientar que a informática favoreceu de forma quase que indiscutível a comunicação entre as pessoas por se tratar de uma tecnologia que permite de forma bastante simples essa interação entre as pessoas em toda parte do mundo.

Com o desenvolvimento dos sistemas informáticos e da Internet como ferramentas primárias para a transferência de dados e informações, a interatividade entre os usuários se diversificou. Desta forma, podem conviver no mesmo espaço pessoas de diferentes culturas, nacionalidades, personalidades e interesses, fazendo com que a interação e a conexão entre essas pessoas se torne inevitável.

Por isto, na medida em que a internet concentra, processa e transfere qualquer tipo de informação e dados, também se transformou em um meio eficaz para a realização de crimes ou certas condutas que agridem bens relevantes do homem. Podemos dizer que houve o uso desta tecnologia de maneira prejudicial tendo o Estado teve que intervir e reprimir esses tipos de crimes praticados de forma virtual.

Diferentemente do crime convencional, o cibercrime assume um aspecto de constante evolução e conta com a participação das mudanças tecnológicas para o seu aprimoramento. É cada vez mais comum nos dias atuais surgirem novas formas desse tipo de criminalidade já que os meios informáticos se tornaram cada vez mais modernos e diversificados.

Com o aumento da acessibilidade dos meios digitais, a internet tornou-se também um ambiente perigoso, suscetível a prática de infrações penais, o que vem se tornando cada vez mais recorrente, apresentando inclusive um cenário preocupante no Brasil atualmente, tendo em vista as dificuldades enfrentadas na investigação criminal e no âmbito do judiciário brasileiro com relação a esses delitos.

Nesse sentido, a internet se mostra como um instrumento facilitador para a consecução de crimes, pois, em muitos casos, o agente delituoso não precisa utilizar de nenhum instrumento físico que seja ou violento, ou ameaçador

para realização daqueles, bastando apenas o computador e o conhecimento técnico, ou não, para concretizar as condutas delitivas.

Escorreito analisar que as práticas criminosas, as quais são exercidas com o suporte da internet ou por meio de um computador, em sua grande maioria, carecem de uma tipificação específica, o que dificulta demasiadamente uma medida punitiva dos agentes envolvidos. Além desse entrave, atualmente muitos dos crimes praticados ainda não são divulgados, seja por conta da falta de disseminação de informações ou pela falta de denúncias. Em muitos casos, evita-se demonstrar a fragilidade quanto à segurança das empresas, e por conta da carente punibilidade dos transgressores, a lei ainda padece de meios para coibi-los.

Dada as dificuldades encontradas diariamente no combate aos crimes no “mundo” cibernético, deu-se a necessidade de uma atuação mais efetiva do Estado, no entanto, de forma geral, essa atuação não tem acompanhado as evoluções constantes daqueles que a utilizam com finalidade de obter vantagem em face de outrem. Desse modo, o Estado não consegue oferecer uma segurança jurídica quanto aos crimes cibernéticos, haja vista que os níveis dos delitos na internet são elevados e rápidos, e através de ações ágeis os criminosos conseguem invadir redes e provocar uma série de condutas ilícitas.

Para reprimir delitos cibernéticos, o reconhecimento legal de tais condutas é imprescindível, observando o princípio da legalidade e também o princípio da taxatividade do direito penal, o qual compele que a norma penal incriminadora seja exata, e caso não observe tal determinação, corre o risco de perder a eficácia.

O Ministério Público, como órgão de defesa dos direitos individuais e sociais indisponíveis, da ordem jurídica e do regime democrático de direito, possui um papel fundamental no combate aos crimes cibernéticos no Brasil.

Como órgão essencial à função jurisdicional do Estado, segundo a própria Constituição Federal de 1988, ele atua em prol dos interesses da coletividade e é o responsável por promover a ação penal pública, além de exercer diligências ao longo do procedimento investigatório. No âmbito federal, o Ministério Público Federal atua nos crimes que a Constituição determina como crimes de competência federal, incluindo os crimes virtuais praticados na rede mundial de computadores, desde que tenha o requisito da transnacionalidade.

Como órgão auxiliar da justiça, o Ministério Público atua na investigação dos crimes virtuais através de um sistema complexo de análise de dados, contando com a participação de profissionais da área de tecnologia que localizam os criminosos digitais por meio de um amplo aparato tecnológico.

Recentemente o Ministério Público Federal traçou um panorama sobre o combate aos crimes cibernéticos, o que tem sido um importante combatente, capacitando cada vez mais seus agentes para lograr a identificação dos transgressores.

A luta contra o cibercrime por meio do órgão ocorre em duas etapas e serão abordadas posteriormente. Primeiro, quando comprometida a confidencialidade dos dados telemáticos, tentando identificar o utilizador e a máquina onde o crime foi cometido. Este é o endereço IP (número de protocolo único de acordo com o tempo de conexão), data e hora de acesso. Assim, o combate aos crimes cibernéticos empreende-se a partir da comprovação da autoria e da materialidade, através de busca e apreensão do objeto utilizado, oitiva do assinante da conexão, fotos do local, do laudo pericial, entre outros meios de investigação.

Procedeu-se uma pesquisa para apresentar quais foram os principais mecanismos utilizados pelo Ministério Público para atingir o objetivo de providenciar segurança ao ambiente virtual, os desafios enfrentados inicialmente e os avanços alcançados com a sua atuação. Além disso, buscou-se apresentar os principais métodos, aliados à informática, para investigação no âmbito da criminalidade cibernética, quais foram as principais inovações tecnológicas propiciadas, os principais desafios a serem encarados e como o ordenamento jurídico brasileiro tem buscado sanar as falhas nesse sistema.

1. DOS CRIMES CIBERNÉTICOS

1.1 CONCEITUAÇÃO E CARACTERÍSTICAS

Pode-se conceituar os crimes cibernéticos, como aqueles cometidos na internet, seja por meio de uma rede de utilização pública, privada ou doméstica. Eles podem atingir uma única pessoa ou várias pessoas ao mesmo

tempo, e têm finalidades diversas. Convém salientar, inclusive, que um mesmo crime pode ser praticado em vários lugares ao mesmo tempo, por meio do uso de um ou de vários computadores diferentes.

Para Spencer Toth (2009) a criminalidade que se realiza no meio real é mais fácil de ser combatida devido a algumas características como o ofensor e a vítima precisarem estar no mesmo espaço e ao mesmo tempo, sendo assim, caso não ocorra a prisão em flagrante, ainda é mais fácil identificar o criminoso, por meio do reconhecimento feito pelo ofendido, depoimento de testemunhas, identificação de impressões digitais, dentre outras formas de provas, o que, normalmente, não é possível quando se trata de crimes virtuais.

Com a análise de conceitos ligados aos crimes cibernéticos, entende-se que são infrações virtuais aquelas condutas dolosas ou culposas que acabam por causar prejuízo (seja no ambiente virtual ou fora dele), ao bem jurídico da inviolabilidade de dados, acarretando danos na esfera da integridade moral, econômica, ou em qualquer âmbito da vida dos usuários (FERREIRA, 2000).

Pode-se conceituar também os crimes virtuais como crimes digitais, crimes eletrônicos, cibercrimes, crimes cibernéticos, entre outras nomenclaturas. São os nomes dados à atividade onde um computador ou rede destes é utilizado como base para cometimento de crimes ou facilitação para estes.

Nas palavras de Roque (2007, p. 13), os crimes cibernéticos são: “toda conduta, definida em lei como crime, em que o computador tenha sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. Por sua vez, pode-se dizer, de uma forma simplificada, que "os crimes cibernéticos são praticados através da internet, e o meio usualmente utilizado é o computador”. (Castro, 2003).

Vale lembrar que existem diversas nomenclaturas adotadas para titular esses delitos: crimes virtuais, crimes informáticos, crimes eletrônicos, delitos computacionais, dentre outros, mas todos se referem a condutas típicas, antijurídicas e culpáveis, praticadas contra ou com a utilização dos sistemas informáticos, sendo próprios quando as ações são praticadas com a intenção de atingir um sistema informático, e impróprios quando são praticadas com o objetivo de atingir outro bem jurídico, tendo a internet apenas como meio para fazê-lo (GRECO, 2000).

Outro conceito importante associado ao crime virtual é o de ciberespaço, se caracterizando como um novo tipo de sociedade em que novas formas de relações sociais estão surgindo. A partir daí, partimos do mundo real, onde os territórios não têm fronteiras e não há subjetividade suficiente para simular o crime. Uma projeção do mundo real que lhe dá a sensação de estar em um determinado local atual quando você executa uma tarefa na frente de um computador.

Para Pierre Lévy (1997), um dos grandes estudiosos sobre esta temática, o ciberespaço é um espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores, amplia o ambiente. Estes novos meios de comunicação que coletam, manipulam, estocam, simulam, transmitem os materiais da informação e criam uma nova camada. Desta forma, como a tecnologia nunca é neutra, este ciberespaço pode ser um espaço de democracia, de expansão da informação ou de controle, e até de crimes virtuais.

Acerca dos crimes cibernéticos, existe no mundo virtual, a figura principal dos criminosos, que é o sujeito ativo que utiliza dos conhecimentos da informática e da internet para praticar o crime causando prejuízo à vítima, podendo atentar contra sua vida, liberdade, honra e privacidade. Já o sujeito passivo é o titular do bem jurídico lesado ou ameaçado pela conduta criminosa. Nos crimes de informática, o sujeito passivo é aquele que comete qualquer tipo de prejuízo proveniente de sistemas informatizados, podendo ser física ou jurídica". (BRASIL, 2008, p. 125).

Os autores desses delitos são comumente chamados de hackers que, segundo o Dicionário Aurélio, são aqueles que possuem habilidade para burlar os sistemas de segurança dos dispositivos informáticos e gerar conexões desautorizadas (SPERANDIO, 2009). Porém nessa conceituação, há divergências pois os hackers também podem ser aqueles que atuam na proteção de computadores e impedem a invasão de sistemas informáticos.

Outra definição importante são os "crackers". Esta definição é menos popular e serve para indicar aqueles que se utilizam da rede informática para praticarem crimes, adquirindo uma conotação mais negativa já que atuam de maneira maliciosa. De forma mais específica são aqueles hackers que buscam atacar computadores com o objetivo de danificá-los e/ou furtar informações

(SPERANDIO, 2009). Em um período muito curto de tempo, o cracker pode acessar uma conta bancária, manipular dados dessas contas bancárias do computador de outra pessoa e identificar senhas e dados bancários. Este especialista em TI tem habilidade e conhecimento específico para roubar o valor contido em contas bancárias. Isso cria novos meios para realizar crimes já arraigados no sistema estatal.

Assim, depreende-se que o perfil do criminoso é consideravelmente ímpar, necessitando ter uma inteligência em demasia, todavia infelizmente é utilizada para a prática inadequada. Outro ponto importante é a sensação dos criminosos de serem inatingíveis por acreditarem que não estão agindo de forma ilegal, o quê de certa forma está correta, vez que muitas condutas que eles praticam não estão estatuídas em lei, ou seja, não estão agindo em desconformidade com o ordenamento jurídico para serem punidos.

Os criminosos na maioria das vezes vivenciam a total tranquilidade de não serem identificados, visto que estão escondidos atrás de um computador ou um celular ou por outro meio que lhes cause essa noção, e o fato de se sentirem assim é um fator que deixa o usuário criminoso sentindo-se seguro para a prática dos delitos cibernéticos.

Para uma melhor compreensão dos termos utilizados para definir esses criminosos, surge um conceito relevante, os chamados “Preaker”, sendo definidos como “aqueles que fraudam os meios de comunicação telefônica, para proveito próprio sem o pagamento devido, instalando escutas a fim de facilitar o acesso externo, visando o ataque a sistemas” (WENDTH JORGE,2012).

Além deste, outro conceito estudado por especialistas no assunto, são os “Lammers”. Esses são definidos como “aqueles que possuem algum conhecimento e querem se tornar um hacker, e dessa maneira invadem e perturbam sites, para os praticantes, podem ser denominados de iniciantes” (WENDTH JORGE, 2012).

Da mesma forma, as vítimas dos crimes cibernéticos são pessoas que são atingidas de forma direta ou indiretamente pelo uso da tecnologia, haja vista que, os bandidos se apoderam de dados, imagens, áudios, senhas, entre outros recursos pessoais para prejudicar o usuário qualquer tipo de medo às infrações que podem se caracterizar. Assim, qualquer pessoa pode ser vítima desses

delitos, sendo que na grande maioria das vezes, se manifestam devido a anseios financeiros ou pelo simples objetivo de prejudicar alguém.

1.2 CLASSIFICAÇÃO DOS CIBERCRIMES

Quanto à classificação dos crimes cibernéticos também há diversos entendimentos doutrinários que podem levar em consideração os bens jurídicos violados, os procedimentos adotados para cometimento da infração ou o objetivo final da conduta praticada (FERREIRA, 2000).

Os crimes cibernéticos são classificados pela doutrina brasileira dominante como delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico. Ademais, e com muita propriedade em torno do tema, o jurista Vicente de Paula Rodrigues Maggio (2013), assim classificou os crimes cibernéticos:

> "Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: "invadir", "instalar") e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada (somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se prolonga no tempo), monossubjetivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima)."

A classificação mais ampla e mais acolhida pelos doutrinadores é aquela pautada na forma de cometimento, nas quais divide os crimes em próprios, que são aqueles praticados através dos dispositivos informáticos e com o objetivo final de lesar os bens jurídicos que nasceram das relações digitais, e impróprios, como sendo aqueles que utilizam a ferramenta digital como um meio, repercutindo seus efeitos na esfera real (FERREIRA, 2000).

Dentro dessa forma de classificação, percebe-se que, enquanto os impróprios abrangem todos os crimes já praticados anteriormente à popularização dos dispositivos informáticos, da Internet e que utilizam a tecnologia apenas como facilitador ou meio de atuação; os próprios possuem como alvo o próprio sistema informático. Ambos, em geral, são crimes que utilizam a engenharia social aliada à fragilidade e despreparo da vítima para alcance de objetivos delitivos.

Em regra, cita-se como crimes cibernéticos impróprios os crimes patrimoniais, os crimes contra a honra, pedofilia, racismo, ameaças, dentre outros já tipificados na legislação penal em vigor. Já os crimes cibernéticos próprios ocorrem quando há a invasão não autorizada ou desprotegida a dispositivos informáticos, como por exemplo, o acesso indevido a banco de dados, os ataques de negação de serviço contra sites, o sequestro de informações, a apropriação indevida de dados, dentre outros.

No tocante a essas duas categorias, Marcelo Xavier de Freitas Crespo ressalta que: Temos que para se cometer delitos classificados como impróprios não se verificam grandes diferenças quanto ao modus operandi. Em outras palavras, embora mude o modo pelo qual se pratica a ação delitiva, não se vislumbra a necessidade de conhecimentos técnicos. Já quanto aos ilícitos classificados como próprios, estes sim, dependem de conhecimentos específicos de computação.

Para efeitos de análise, quanto à tipificação da conduta delituosa informática, cabe observar que, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos.

Outra classificação agrupa os crimes “virtuais” em três grupos: o crime virtual puro, o crime virtual misto e o crime virtual comum. O crime virtual puro corresponderia à conduta ilícita voltada para o sistema do computador, para a violação do equipamento e de seus componentes, inclusive dados e sistemas (software, hardware e meios de armazenamentos).

Já os crimes virtuais mistos, são aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático (transferência ilícita de valores

ou “salemislacing” – retiradas diárias de pequenas quantias de milhares de contas bancárias). Há também a categoria dos crimes virtuais comuns que correspondem àqueles em que a internet é utilizada como instrumento de realização do delito que já tipificado na lei penal, como os crimes contra a honra e a veiculação de pornografia infantil (FIORILLO, 2012).

2. A LEGISLAÇÃO NO COMBATE AOS CIBERCRIMES

Em verdade, o que acontece no campo do Direito Penal é que, enquanto um determinado bem não adquire a necessidade de proteção pelo ordenamento, este não causa lesão ou ameaça relevante para devida repreensão pelo Estado, configurando-se como uma realidade jurídica diversa e notadamente coaduna ao universo tecnológico e até mesmo de um novo ramo jurídico denominado Direito Informático.

De tal sorte que os delitos praticados por meio do espaço cibernético podem ter implicações no campo constitucional, civil e/ou penal. Até o ano de 2012 a legislação pátria era omissa quanto à tipificação dos delitos que ocorriam por utilização do meio internet. Em obediência ao previsto no artigo 5º, XXXIX, Constituição Federal de 1988, o princípio da legalidade, os delitos assim cometidos não poderiam ser repreendidos, se não devidamente tipificados em Lei. Em razão da imprevisão de regramentos específicos, a disseminação de tais condutos foi rápida e diversificada.

A lacuna deixada pelo rastro da internet instalou discussões acerca da necessidade de o ordenamento jurídico atentar às novas condutas realizadas pelos meios informáticos. Tal debate se intensificou quando da repercussão de episódios ocorridos com figuras públicas, em que estas tiveram vazadas por meio de invasão do seu computador fotos de sua intimidade.

2.1 LEGISLAÇÃO INTERNACIONAL

Os crimes cibernéticos têm se tornado cada vez mais frequentes em todo o mundo, com impactos significativos na segurança dos indivíduos, empresas e governos. Diante dessa realidade, os países têm implementado medidas para combater essa ameaça, incluindo a criação de leis e regulamentos específicos para crimes cibernéticos.

Nesse sentido, torna-se fundamental analisar a evolução da legislação internacional no combate aos crimes cibernéticos, destacando as principais leis e acordos internacionais que surgiram ao longo dos anos para lidar com essa questão. Com isso, serão discutidos os desafios enfrentados no âmbito internacional para a aplicação da lei no ambiente digital. Sendo assim, serão analisados brevemente alguns instrumentos jurídicos, especificamente dos Estados Unidos e da Europa.

2.1.1 ESTADOS UNIDOS

Em 1986, o Congresso dos Estados Unidos aprovou a Lei de Fraude e Abuso de Computadores (Computer Fraud and Abuse Act - CFAA). Esta lei foi a primeira tentativa significativa de combater o cibercrime, estabelecendo penas para hackers que invadissem sistemas de computadores do governo ou de empresas. Desde então, a CFAA foi atualizada várias vezes para se adaptar às mudanças tecnológicas e às novas formas de ataques cibernéticos.

Em 1996, foi aprovada a Lei de Comunicações Eletrônicas de Privacidade (Electronic Communications Privacy Act - ECPA), que estabeleceu a privacidade eletrônica e restringiu o acesso não autorizado a comunicações eletrônicas, como e-mails e mensagens de texto. Embora a lei tenha sido bem recebida na época, hoje em dia é criticada por ser antiquada e não ter acompanhado o avanço tecnológico, permitindo que o governo tenha amplo acesso a dados pessoais sem a necessidade de um mandado judicial.

Em 2001, os Estados Unidos aderiram à Convenção de Budapeste sobre Cibercrime, um tratado internacional que estabelece normas globais para

a prevenção e o combate ao crime cibernético. A Convenção de Budapeste define uma série de atividades criminosas cibernéticas, incluindo a invasão de sistemas informáticos, a interceptação de comunicações e a produção de malware. Além disso, estabelece a obrigatoriedade da cooperação internacional na investigação e punição desses crimes.

Em 2014, a Lei de Proteção de Dados do Consumidor (Consumer Data Protection Act - CDPA) foi introduzida para melhorar a proteção dos dados pessoais dos consumidores. A CDPA estabeleceu requisitos rigorosos para empresas que coletam, armazenam e compartilham dados pessoais, incluindo penalidades por violações de segurança de dados.

Em 2015, o presidente Barack Obama assinou a Lei de Informação sobre Ameaças de Cibersegurança (Cybersecurity Information Sharing Act - CISA), que autoriza empresas privadas a compartilharem informações de segurança cibernética com o governo. A lei foi projetada para facilitar a troca de informações de segurança entre empresas e o governo, a fim de melhorar a resposta a ameaças cibernéticas.

Em 2018, a Lei Geral de Proteção de Dados da Califórnia (California Consumer Privacy Act - CCPA) foi aprovada para estabelecer requisitos de privacidade de dados para empresas que atendem a residentes da Califórnia. A CCPA estabeleceu direitos para os consumidores em relação à privacidade de dados e penalidades para empresas que não cumprem suas obrigações.

2.1.2 EUROPA

A União Europeia tem buscado desenvolver uma legislação abrangente para combater os crimes cibernéticos desde a Diretiva de 2005, que estabeleceu medidas mínimas para o combate a ataques contra sistemas de informação. Desde então, várias iniciativas legislativas foram adotadas, culminando no Regulamento Geral de Proteção de Dados (RGPD) de 2018, que estabelece regras mais rigorosas para a proteção dos dados pessoais na UE.

A Diretiva de 2005 foi adotada pelo Parlamento Europeu e pelo Conselho para estabelecer medidas mínimas de combate a ataques contra sistemas de informação e punição adequada aos responsáveis. A diretiva definiu crimes cibernéticos, incluindo ataques contra sistemas de informação, programas de computador maliciosos e invasões de redes, e estabeleceu sanções criminais mínimas para esses crimes.

Posteriormente, a Diretiva de 2013, também conhecida como Diretiva de Cibercrime, estabeleceu regras mais abrangentes para combater os crimes cibernéticos. A diretiva incluiu novos tipos de crimes, como a intrusão em dispositivos, a distribuição de vírus e a utilização de ferramentas de hacking. Além disso, a diretiva prevê a obrigação de os Estados-membros tomarem medidas adequadas para prevenir, investigar e processar os crimes cibernéticos, bem como a cooperação entre as autoridades dos Estados-membros para combater esses crimes.

O Regulamento Geral de Proteção de Dados (RGPD) de 2018 representa uma grande evolução na legislação europeia no combate aos crimes cibernéticos, uma vez que estabelece regras mais rigorosas para a proteção dos dados pessoais na UE. O RGPD impõe a obrigação de os controladores de dados protegerem os dados pessoais e notificarem as autoridades em caso de violação, além de estabelecer multas significativas para as violações.

Além disso, há de se destacar que o continente europeu deu origem a um singular instrumento legislativo para abordar a temática dessas contravenções: a Convenção de Budapeste. Adotada em 2001 pelo Conselho da Europa, foi o primeiro tratado internacional a tratar especificamente do cibercrime. Desde então, a Convenção tem sido ratificada por vários países, incluindo Estados Unidos, Japão, Canadá, Brasil e a maioria dos países da União Europeia.

Entre os objetivos da referida Convenção, pode-se citar a criminalização de um conjunto de delitos contra e através de computadores no direito doméstico e a harmonização dos elementos normativos relativos às infrações. Além deste, a definição dos poderes necessários às autoridades

competentes, de acordo com o código de processo penal pátrio, para proteger as provas digitais de qualquer crime, e ainda, limitar tais poderes, a fim de evitar abuso de poder e proteger os princípios fundamentais dos Estados.

Após a análise supra, torna-se crível aferir que, após a sua adoção, a Convenção de Budapeste continua sendo um tratado internacional mais eficaz em matéria de crimes cibernéticos e do Estado de Direito no Ciberespaço. Tendo em consideração sua importância, visto que nos últimos anos, ela teve um impacto global que resultou numa legislação mais abrangente e harmonizada no domínio da cibercriminalidade, numa colaboração internacional mais efetiva na investigação e instauração de processos penais dos cibercrimes a nível mundial.

2.2 EVOLUÇÃO NA LEGISLAÇÃO BRASILEIRA

A internet “chegou” ao Brasil em 1988 e foi ganhando espaço, até chegar em todos os Estados, e desde sua concepção tiveram algumas leis como a Constituição Federal de 1988 que trata a respeito das proteções dos dados e ainda anterior a constituição federal, como forma de prevenção a lei 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências. Fora estas leis protecionistas, até o ano de 2012 a respeito da internet não havia nenhuma outra lei. E mesmo na falta de lei os crimes praticados através da rede, eram punidos com base no efeito da ação.

Nos últimos anos, tem havido um aumento significativo nos crimes cibernéticos no Brasil, com os hackers utilizando técnicas sofisticadas para violar sistemas e roubar informações pessoais e financeiras. Para combater esses crimes, o Brasil tem implementado leis e regulamentos cada vez mais rigorosos, a fim de garantir a proteção dos cidadãos e das empresas.

A legislação brasileira relacionada aos crimes cibernéticos começou a ser criada em 1996, com a Lei de Propriedade Intelectual. No entanto, a primeira lei específica para crimes cibernéticos só foi criada em 2012, com a Lei 12.737, conhecida como Lei Carolina Dieckmann, em referência à atriz que teve fotos íntimas divulgadas na internet sem seu consentimento.

A Lei Carolina Dieckmann foi um marco na legislação brasileira de crimes cibernéticos, pois estabeleceu penas mais severas para crimes virtuais, como invasão de computadores e a divulgação de informações privadas. Além disso, a lei tornou ilegal a venda de softwares ou ferramentas utilizadas para a prática de crimes cibernéticos.

A lei supracitada surgiu como alternativa à Lei Azeredo, a qual foi alvo de várias críticas em razão do temor de supressão da liberdade virtual, e, ao ser promulgada, somente previu a obrigatoriedade dos órgãos da polícia judiciária se estruturarem, para buscarem o combate de ações delituosas no meio virtual.

A lei de crimes informáticos (leis 12.735/12 e 12.737/12) entrou em vigor na data de 02 de Abril de 2013, elas alteram o Código Penal para tratar dos crimes cibernéticos. Esta lei, a 12.735/12, transitou no congresso desde 1999 (PL 84/99, na câmara). Em seu texto original ele era bem extenso e bastante polêmico no sentido da responsabilidade dos provedores de internet, mas apesar disso, durante sua tramitação foi reduzido a quatro artigos, sendo reduzida a dois por veto na sanção, pela presidente Dilma Rousseff.

Além destes, cita-se o Decreto Federal nº 7.962/13, ele entrou em vigor na data de 14 de maio de 2013, seu objetivo era preencher as lacunas no Código de Defesa do Consumidor acerca do comércio em lojas virtuais, ou como é chamado o comércio eletrônico, visto que inexiste legislação específica sobre o processo de compra e venda na internet.

Posteriormente, em 2014, foi criada a Lei 12.965, conhecida como Marco Civil da Internet, que estabeleceu os princípios, garantias, direitos e deveres para o uso da internet no Brasil. O Marco Civil da Internet estabelece regras para a coleta e uso de informações pessoais, bem como para a responsabilidade de provedores de serviços de internet em relação ao conteúdo postado por seus usuários.

Em 2018, foi aprovada a Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais no Brasil. A LGPD estabelece regras para a coleta, armazenamento, processamento e compartilhamento de informações pessoais, com o objetivo de proteger a privacidade e os direitos dos indivíduos.

Além disso, em 2021, foi aprovada a Lei 14.155, que aumenta as penas para crimes cibernéticos, como invasão de dispositivos eletrônicos, roubo de dados e extorsão. A lei também estabelece penas mais severas para crimes cometidos contra autoridades, servidores públicos e seus familiares.

Essa evolução da legislação brasileira no combate aos crimes cibernéticos mostra a preocupação do governo em proteger os cidadãos e empresas contra as ameaças virtuais. No entanto, ainda há muito a ser feito, especialmente em relação à conscientização da população sobre os perigos da internet e à importância da proteção de dados pessoais.

3. O PAPEL DO MINISTÉRIO PÚBLICO

O Ministério Público é responsável por defender a ordem jurídica, os interesses sociais e individuais indisponíveis, atuando em diversas áreas, incluindo a área de cibercrimes. Na área criminal, o órgão pode atuar divulgando diretamente infrações penais, cabendo-lhe, ainda, o relevante papel de exercer o controle externo da atividade policial, na forma da lei complementar de cada Estado.

O Promotor de Justiça do Ministério Público do Estado de São Paulo, Luiz Sales do Nascimento, em seu artigo ‘Ministério Público: aspectos gerais’ (2017), aponta que tal órgão, devido à sua autonomia perante os três poderes, executivo, legislativo e judiciário, possui a incumbência de ser fiscalizador destes, além de possuir também a função de acusador, já que a função de julgador é privativa do Estado.

Nesse sentido, a CONAMP, Associação Nacional dos Membros do Ministério Público, esclarece que é dever institucional do Órgão, atuar em atividades de interesse social, defesa e garantia dos direitos dos cidadãos, e relativas à educação, fiscalizando a qualidade dos serviços escolares e ainda promovendo iniciativas de colaboração com os mesmos.

Dessa forma, sendo as políticas públicas ferramentas utilizadas pelo Estado para garantir a efetividade dos direitos sociais dos indivíduos, e os crimes cibernéticos atos infracionais que lesam direitos de usuários da internet, cabe ao

Ministério Público, tanto Federal quanto Estadual, estar à frente das atividades de prevenção e combate, cumprindo seu dever de tutela dos interesses da população.

O Ministério Público, exercendo seu papel de controle da Administração Pública, tem a obrigação de fiscalizar a implementação de políticas públicas, além de atuar também na realização de atividades pertinentes ao programa, e na adequação dele para melhor alcançar os fins traçados como objetivos.

A Instituição dispõe de papel essencial no monitoramento das políticas sociais, indo além da fiscalização, atuando também na concretização destas na sociedade, por meio da realização de projetos e atividades, além ainda do dever de, ante à inércia do Estado frente à alguma política, cobrar tal atuação por vias judiciais ou extrajudiciais.

Além do Ministério Público, existem outros atores de participação fundamental no processo das políticas sociais implementadas em atenção aos crimes virtuais, tais como ONG's, empresas privadas e delegacias especializadas, dotadas de maior capacidade técnica para investigação dos atos delituosos.

Nos casos de cibercrime, o Ministério Público atua em conjunto com outras autoridades competentes, como a Polícia Federal, a Polícia Civil, a Receita Federal, entre outras. O papel do Ministério Público é de investigar, processar e punir os crimes cometidos no ambiente virtual, como fraudes eletrônicas, invasão de sistemas, pornografia infantil, cyberbullying, entre outros.

Nesse sentido, o Ministério Público pode requisitar a quebra de sigilo de dados telemáticos, como e-mails, registros de conexão e acesso, informações de transações financeiras, para investigar e comprovar a autoria de um crime cibernético. Além disso, pode propor ações penais, civis e de improbidade administrativa, buscando a responsabilização dos criminosos e a reparação dos danos causados às vítimas.

O Ministério Público também atua na prevenção de cibercrimes, realizando campanhas educativas e orientando a população sobre medidas de segurança digital para evitar a ocorrência desses crimes.

3.1 DA INVESTIGAÇÃO DOS CRIMES VIRTUAIS

A adequada investigação dos crimes cibernéticos é parte importante no processo de repressão dessas condutas, e para que isso seja possível, é imprescindível que existam órgãos que disponham de recursos e profissionais capacitados para uma averiguação eficiente dos atos ilícitos a eles reportados.

A investigação de crimes ocorridos no ambiente digital, ou através dele, exige profissionais com conhecimento mais especializado e técnico na área, além de exigir também ferramentas mais específicas para possibilitar a apuração dos fatos, e as delegacias comuns não vinham atendendo de maneira eficaz esses requisitos, fazendo com que surgisse assim, a necessidade de delegacias especializadas.

De uma forma geral a persecução penal pode ser dividida em duas fases, a Investigação Criminal e o Processo Penal. A primeira fase delimita-se à colheita de provas, apuração de indícios de autoria e materialidade da ação criminosa, enquanto que a segunda fase tem por escopo a função de processar e julgar.

De certo é que quando da investigação policial as diligências tomadas em sede de inquérito policial são importantes e determinarão a efetividade na apuração dos delitos. Especialmente, a apuração de crimes cibernéticos traz especificidades para a investigação policial, de forma que a necessidade de utilização de recursos adequados é evidente, e torna-se, por vezes, um entrave à elucidação desses crimes.

O Ministério Público (MP) atua na investigação de crimes virtuais de várias maneiras, dependendo da natureza e da gravidade do crime em questão. Entre as formas de atuação do Ministério Público está a Investigação Preliminar que consiste em poder conduzir uma investigação para determinar se há provas suficientes para justificar a abertura de um processo criminal.

Além disso, o Ministério Público pode solicitar a requisição de informações de empresas de tecnologia, provedores de serviços de internet e outras fontes para ajudar na investigação de crimes virtuais. Outra forma de atuação é a colaboração com outras agências. Dessa maneira, o órgão pode trabalhar em conjunto com outras agências governamentais, como a polícia, para coletar provas e conduzir investigações.

A principal forma de atuação é por meio da ação judicial para obter informações ou documentos relevantes para a investigação. Ao entrar com a ação, o MP pode conseguir provas relevantes perante as autoridades judiciárias e assim, conseguir um aparato investigativo suficiente para identificar os delitos e punir os responsáveis.

Por último, e igualmente importante está a atuação na denúncia e na acusação. Dessa maneira, se houver evidências suficientes, o MP pode apresentar uma denúncia e acusar os suspeitos de crimes virtuais.

Vale destacar que, em casos de crimes cibernéticos, a investigação pode ser mais complexa, já que muitas vezes as informações são armazenadas em servidores em outros países, exigindo a cooperação internacional entre as autoridades. Além disso, a identificação do autor do crime pode ser mais difícil, já que ele pode se esconder atrás de múltiplos endereços de IP ou de dispositivos de anonimato. Por isso, as autoridades precisam contar com peritos e especialistas em tecnologia para auxiliar nas investigações e comprovar a autoria do crime.

3.1.1 FASES DA INVESTIGAÇÃO

De acordo com Wendt (2013) durante a investigação de crimes cibernéticos há uma fase inicial, técnica, e uma fase consequencial, de investigação propriamente dita.

O objetivo principal da fase técnica consiste em localizar o computador ou dispositivo que foi utilizado para a prática da conduta criminosa. Durante essa etapa, são realizados alguns procedimentos iniciais, dentre eles, a compreensão do fato ocorrido na internet, orientações à vítima que buscam a preservação do material comprobatório do crime e a sua proteção virtual, iniciação da coleta de provas em ambiente virtual, formalização da conduta criminosa através do registro do boletim de ocorrência, e a instauração do procedimento, possíveis autores, origem e-mails, registros e hospedagens de domínios.

Além disso, atua na formalização das provas coletadas e na apuração preliminar, e também na representação ao Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão ou acesso.

Como assegura Wendt (2013): A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local. Essa diligência deverá ocorrer sempre de maneira discreta, pois poderá haver a necessidade de solicitar uma medida processual penal cautelar, em regra a representação para que o Poder Judiciário conceda o mandado de busca e apreensão. Ela ocorrerá de imediato nos casos de identificar o endereço que corresponda a uma residência e/ou rede não corporativa.

Anteriormente, a regulação pelo ordenamento brasileiro destas condutas tinha como problema a tipificação, aspecto importante, pois evidencia que é de responsabilidade do Estado encontrar formas de prevenção e combate às ilicitudes realizadas no meio virtual (MAUES; DUARTE; CARDOSO, 2018).

Atualmente, as dificuldades que as instituições apresentam perpassam a necessidade de modernização da gestão, e consequente aquisição de um aparato qualificado, especializado, que atenda a demanda desses delitos, que por sua natureza proporcionam um uso de uma carga tecnológica diferenciada.

Além da identificação do autor do crime, um aspecto que permeia a investigação policial nesses casos é a preservação das provas, e a primeira medida a ser observada é a identificação do Protocolo de internet – IP. Protocolos assim podem ser classificados como fixos ou dinâmicos. Tais medidas podem perpassar a preservação de conteúdo através da salvaguarda da Uniform Resource Locator - URL, bem como o horário de acesso (provedor Universal Time Coordinated - UTC).

Para verificar a autoria de um crime praticado no ambiente virtual, deve-se buscar todo o registro de conexão, a fim de verificar para qual usuário aquele IP fora atribuído, no dia e na hora do delito com o fuso horário respectivo. Este conjunto de informações é denominado de registro de conexão, e é de grande valia na investigação policial.

As aplicações de internet que são as redes sociais, sites, contas conectadas, podem fornecer dados importantes relacionados ao crime praticado,

podendo ser solicitado ao provedor de aplicações que preste informações de IP, conta de e-mail, data, hora, fuso horário (BARRETO; BRASIL, 2016).

Uma medida de preservação de conteúdo que pode ser adotada nos casos de identificação de crime virtual, é a elaboração de ata notarial em cartório, de modo a emitir um instrumento público que narre um fato ou situação apresentada por uma parte. Ainda há a possibilidade de utilização da ferramenta de software que possa fazer o download dos dados, evitando-se utilizar printscreen ou screenshot, que tem a validade jurídica questionada. Em consonância, Barreto e Brasil (2016) citam que poderá ser utilizada a certidão elaborada por servidor público dotado de fé pública, a exemplo do escrivão de polícia.

Quanto à preservação do conteúdo estão dois aspectos relevantes e importantes para análise que são a preservação e arquivo de dados. A diferença entre eles pode ser explicada da seguinte forma: na preservação, os dados existem e estão assegurados de alterações ou deteriorações, e no arquivo de dados, há o armazenamento e manutenção dos dados com produção de dados contínua. A preservação implica, portanto, na identificação, coleta e análise da evidência pelo aparelho estatal de forma correta. A preservação pode ser efetuada solicitando-se um mandado de busca ou oficiando junto aos provedores de aplicação de internet solicitando os registros de conexão.

Dados cadastrais podem ser solicitados diretamente aos provedores, sem necessidade de ordem judicial. Em casos como risco de morte ou risco à integridade de crianças e adolescentes, as informações podem ser conseguidas pela autoridade policial, sem necessidade inicial de autorização judicial.

Por outro lado, há a possibilidade de a parte acompanhada pelo seu advogado peticionar diretamente aos provedores, por exemplo, solicitando retirada de conteúdo da rede de computadores através de requerimento de exclusão de conteúdo em Provedor de Aplicação, como medida além das providências a serem tomadas pela polícia. Barreto e Brasil (2016) ressalvam que os advogados só poderão requerer registros nos casos de crimes que forem de ação privada ou quando atuantes enquanto assistentes de acusação.

É salutar que a principal questão quanto à investigação policial, seria em relação ao desenvolvimento tecnológico, que demanda dos profissionais especialização na área, além da consideração de que há um excesso de tutela

penal. Inclusive, a própria Lei nº 12.735/2012 previu no seu artigo 4º que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Portanto, a melhora da prestação do serviço à sociedade vai além da melhora do aparelhamento estatal em termos de infraestrutura: é necessário o investimento em conhecimento especializado na área, inclusive de profissionais na área de informática, conjugando-se as disciplinas na prática, pois não basta o excesso de tutela penal. Anteriormente as tipificações já se tornavam difíceis às investigações, e na atualidade, a dificuldade perfaz-se na expertise que a área requer.

É certo que pela evolução da prática de crimes cibernéticos e o próprio desenvolvimento das investigações tem-se como principal consideração a necessidade de especialização dos profissionais. Ainda, aponta-se que esse envolvimento pode ser alcançado através da cooperação institucional através do intercâmbio de informações de investigação e de soluções de tecnologia da informação (SILVA, 2006).

O provedor de aplicação de internet Facebook disponibiliza uma plataforma denominada Law Enforcement Online utilizada para preservação de perfis online, neste caso, para solicitação de dados dessa plataforma é necessária obrigatoriamente investigação policial em curso. Importante observar que no que se refere aos dados de registro, obrigatoriamente, a autoridade deverá apresentar a ordem judicial, e no caso de acesso aos dados de comunicação deverá ser apresentado um mandado de busca de dados telemáticos (BARRETO; BRASIL, 2016).

3.2 AÇÕES PENAIS CONTRA OS CRIMES CIBERNÉTICOS

Dias (2007) aponta como o raciocínio que a utilização de políticas de informação preventiva e programas de facilitação de denúncias que contem com o auxílio de provedores de internet, contribuíram para aplicação da lei, facilitando também a desburocratização das demandas.

As ações penais contra os crimes cibernéticos seguem os mesmos procedimentos das ações penais em geral, previstas no Código de Processo Penal (CPP). Entretanto, devido às particularidades do ambiente virtual, algumas etapas da investigação e do processo podem demandar mais tempo e recursos.

O processo penal se inicia com o registro da ocorrência na delegacia ou na Polícia Federal, onde é aberto um inquérito policial para a investigação do crime. A partir das provas colhidas durante a investigação, o Ministério Público oferece a denúncia, que é a acusação formal contra o suposto autor do crime.

Caso o juiz aceite a denúncia, o acusado se torna réu e o processo segue para a fase de instrução, em que são ouvidas as testemunhas de acusação e de defesa, bem como realizado o exame de provas. Durante essa fase, o juiz pode determinar a realização de perícia técnica para comprovar a autoria do crime e a materialidade dos fatos. Ao final da instrução, o juiz profere a sentença, que pode ser de absolvição ou de condenação. Caso o réu seja condenado, é possível recorrer da decisão em instâncias superiores.

3.3 ESTRATÉGIAS E MEDIDAS DE PREVENÇÃO

O Ministério Público atua na prevenção dos crimes cibernéticos principalmente por meio de ações educativas, orientando a população sobre medidas de segurança digital e conscientizando sobre os riscos de comportamentos inadequados na internet.

Uma forma bastante importante de atuação é por meio de campanhas de conscientização sobre segurança digital, alertando para os riscos de comportamentos inadequados na internet, tais como o compartilhamento de informações pessoais, a divulgação de senhas e dados bancários, a prática de cyberbullying e o uso de dispositivos sem segurança adequada.

O Ministério Público pode atuar na prevenção realizando palestras e workshops em escolas, empresas e outros locais públicos para orientar sobre segurança digital e boas práticas na internet, além de oferecer orientação jurídica gratuita para vítimas de crimes cibernéticos, fornecendo informações sobre como denunciar e buscar reparação pelos danos sofridos.

Ademais, é importante destacar o seu poder de fiscalizar o cumprimento das leis de proteção de dados pessoais e outras normas

relacionadas à segurança digital, garantindo que as empresas e prestadores de serviços cumpram as regras estabelecidas. Além disso, o órgão pode firmar parcerias com outras instituições, como ONGs, empresas e universidades, para desenvolver projetos de prevenção e combate aos crimes cibernéticos.

Em resumo, o Ministério Público atua na prevenção dos crimes cibernéticos por meio de ações educativas e de conscientização, orientação jurídica, fiscalização, participação em fóruns e comitês, parcerias e outras iniciativas. Porém, mesmo com a regulamentação legal, a recorrência dessas infrações fez com que fossem elaboradas políticas públicas para auxiliar na prevenção e combate a tais práticas, já que, tais políticas são mecanismos usados pelo governo para transformar seus propósitos em programas que apresentarão resultados na vida dos cidadãos.

Dentro do campo das políticas digitais implementadas pelo Ministério Público, há o projeto ‘Ministério Público pela Educação Digital nas Escolas’, que através da atuação do Ministério Público Federal, tem como público-alvo educadores de escolas da rede pública e privada, oferecendo incentivo para a realização de atividades que ensinam crianças e adolescentes sobre o uso seguro e responsável da Internet, evitando assim que sejam vítimas ou pratiquem crimes virtuais (MINISTÉRIO PÚBLICO FEDERAL, 2018).

Instituído em 2015 por meio da Portaria PGR/MPF nº 753, o projeto segue as diretrizes do Marco Civil da Internet (Lei 12965/14), que evidencia o dever do Estado em promover a utilização da internet de forma segura, responsável e consciente. Sob a coordenação da Procuradoria Federal dos Direitos dos Cidadãos, o MPF realiza, em parceria com a ONG SaferNet, a oficina “Segurança, ética e cidadania na Internet: educando para boas escolhas online”, que é promovida em vários estados pelo país (MINISTÉRIO PÚBLICO FEDERAL, 2016).

No Estado da Bahia, o Ministério Público criou um núcleo de investigação especializado, voltado para os delitos virtuais, o NUCCIBER – Núcleo de Combate aos Crimes Cibernéticos -, que tem por objetivo ações de incentivo e cooperação às atividades que visam combater tais crimes (RABELO, VELOSO, 2016).

O Núcleo atua proporcionando capacitação à Promotores de Justiça e outros agentes atuantes na persecução penal, através de treinamentos,

seminários e oficinas. São desenvolvidas ainda, atividades repressivas e preventivas, tais como o auxílio nas investigações criminais, inclusão digital dos cidadãos através de palestras em instituições de ensino, oficinas voltadas para profissionais do Direito e instruções para profissionais que trabalham usando plataformas digitais.

O NUCCIBER utiliza ainda a própria internet, para, através das redes sociais, divulgar dicas e maneiras de prevenção contra os ataques cibernéticos. São 28 publicados cartazes, banners, cartilhas e vídeos acerca do tema nos meios de comunicação digitais e também na televisão e rádio.

Após a análise de algumas dessas políticas públicas adotadas no Brasil, é possível perceber que a Educação Digital é um importante vetor de colaboração na luta contra as infrações virtuais, já que dessa forma os usuários além de conhecer quais são esses delitos, ainda aprendem maneiras de se proteger e quais são as sanções contra quem os comete.

3.4 A ATUAÇÃO DO MINISTÉRIO PÚBLICO FEDERAL

O Ministério Público Federal (MPF) teve atuação decisiva durante a Comissão Parlamentar de Inquérito (CPI) da Pedofilia em 2008, que culminou com a assinatura de Termo de Ajustamento de Conduta com a Google Brasil Internet Ltda., prevendo uma série de medidas para impedir a livre divulgação de imagens de exploração sexual de crianças e adolescentes no serviço ORKUT de rede social, um dos mais populares no país naquela época, bem como medidas que se anteciparam às previstas no Marco Civil da Internet que pudessem assegurar a eficácia da investigação penal desses casos. Da CPI também resultou alteração legislativa do Estatuto da Criança e do Adolescente, criando novos tipos penais e endurecendo as penas de abuso e exploração sexual de crianças e adolescentes.

Desde então, as empresas provedoras de aplicações de internet têm colaborado para limpar a rede dessas imagens e vídeos. A maior parte das empresas brasileiras de aplicações de internet possuem termos de acordo com o MPF para retirar e remeter a esse órgão imagens e vídeos de abuso sexual, bem como conversas online que possam indicar a ocorrência do aliciamento de criança com fins sexuais, o crime do artigo 241-D do ECA, já que a lei brasileira

não tem um comando de busca ativa desse material ilícito e somente responsabiliza os representantes legais dessas empresas por não retirada desse conteúdo ilegal após notificação oficial.

Atualmente, essa circulação de imagens e vídeos ilícitos migrou para a Deep Web, a parte não indexada da internet, onde a navegação depende de conhecer exatamente o endereço que se pretende acessar. Mesmo nesse ambiente onde a identificação do endereços de IP, Internet Protocol, é dificultada pela utilização de proxies, computadores que servem de passagem mascarando a origem das mensagens, os órgãos de persecução penal brasileiros tiveram êxito em investigação pioneira nesse ambiente virtual, tendo sido deflagradas as operações Darknet I e II para investigação e processamento dos crimes de divulgação de imagens e vídeos de abuso e exploração sexual na internet, com o resgate de vítimas reais de abuso durante as operações.

Nesse contexto, o MPF percebeu que, infelizmente, o número desses delitos é enorme, havendo inúmeras dificuldades a serem transpostas para resultar em investigação e condenações exitosas, que venham a servir de desestímulo a prática desses delitos, os quais destroem a infância e juventude de inúmeras crianças e adolescentes, comprometendo a construção de uma sociedade sadia. A prevenção desses delitos é também, portanto, uma das vertentes de atuação do MPF, para que, com educação e conscientização acerca dos riscos que a internet pode apresentar, as crianças e os jovens possam estar melhor preparados para se defender. Uma vez que a internet dá a falsa sensação de segurança, há uma tendência maior à exposição da intimidade nesse ambiente virtual e uma predisposição a confiar em “amigos” virtuais com os quais se constroem relações, que dão a errônea impressão de serem sólidas e reais, propiciando que crianças e adolescentes terminem como vítimas nas mãos de predadores sexuais.

Para tanto, foi firmado um Termo de Cooperação do MPF com a Safernet Brasil, principal hotline brasileiro para a utilização segura da internet e com o Comitê Gestor da Internet (CGI) no Brasil, órgão responsável por gerir a internet no nosso País, com a finalidade de viabilizar o Projeto Ministério Público pela Educação Digital nas Escolas, que consiste em capacitar professores das redes de ensino público e privado no Brasil por meio da Oficina “Segurança, ética e cidadania na Internet: educando para boas escolhas online”, para que abordem

com seus alunos de forma transversal as matérias do currículo como navegar com segurança na internet, não expondo sua intimidade e também não se transformando em agressor, já que o meio virtual elide da percepção do usuário o impacto que suas ações possuem.

CONCLUSÃO

Em conclusão, este artigo científico abordou diversos aspectos dos crimes cibernéticos, incluindo suas características, a legislação brasileira e internacional aplicável, e a atuação do Ministério Público no combate a esses crimes.

Ficou claro que os crimes cibernéticos são uma ameaça cada vez mais presente na sociedade contemporânea, tendo em vista o grande aumento do uso da internet e de tecnologias digitais. Além disso, foi observado que os crimes cibernéticos podem assumir diversas formas, incluindo a invasão de sistemas, o roubo de dados, a extorsão virtual e o ciberbullying.

A legislação brasileira e internacional é considerada ainda insuficiente para lidar com o grande número de casos de crimes cibernéticos que ocorrem atualmente. Embora haja algumas iniciativas para atualizar as leis existentes, ainda há muito a ser feito para garantir a punição adequada aos responsáveis por esses crimes.

O Ministério Público tem desempenhado um papel fundamental no combate aos crimes virtuais. Por meio de sua atuação, o órgão tem buscado garantir a segurança e a proteção da sociedade em relação às ameaças cibernéticas, trabalhando em estreita colaboração com outras agências governamentais e organizações da sociedade civil.

Os promotores públicos têm se dedicado a investigar e processar casos de crimes cibernéticos, buscando a punição dos responsáveis e a recuperação de dados e prejuízos causados. Além disso, têm promovido ações educativas e de conscientização para orientar a população sobre como se proteger e evitar ser vítima desses crimes.

No entanto, ainda há muito a ser feito para enfrentar o crescente número de ameaças cibernéticas. É necessário que o Ministério Público continue a desenvolver suas capacidades e recursos para lidar com os desafios do mundo digital em constante evolução. A colaboração e a coordenação entre diferentes setores e agências, incluindo empresas e organizações da sociedade civil, também serão fundamentais para enfrentar esse problema complexo e em constante mudança.

REFERÊNCIAS

BARROSO, LUÍS ROBERTO. **Estado, Sociedade e Direito: Diagnósticos E Propostas para o Brasil**. In: XXII Conferência Nacional dos Advogados. Rio de Janeiro, 2014.

CÂMARA DOS DEPUTADOS. Deputada Mariana Carvalho; Deputado Esperidião Amin; Deputado Sandro Alex; Deputado Rafael Motta; Deputado Daniel Coelho; E Deputado Rodrigo Martins. **Câmara dos Deputados CPI – Crimes Cibernéticos – Relatório Final.** Brasília; 04 de maio de 2016.

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

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral.** Salvador: Juspodivm, 2014.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 01 mar. 2018.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. **Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet.** Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, p. 7-28, jan./jun. 2016.

GOUVEIA, Sandra Medeiros Proença. **O direito na era digital: Crimes praticados por meio da informática**. Rio de Janeiro: Mauad, 1997. Disponível em:
<http://books.google.com.br/books?id=3vzmW3DtAuQC&pg=PA43&lpg=PA43&dq=o+legislador+come%C3%A7ou+a+se+preocupar+com+o+mau+uso+dos+recursos+da+inform%C3%A1tica&source=bl&ots=TDsESpVdyx&sig=H-FP7BDOai9J5BzdZjtElpc0SU8&hl=pt--BR#v=onepage&q=o%20legislador%20come %C3%A7ou%20a%20se%20

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em:

<http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 20 Nov. 2017.

MIRANDA, Marcelo Baeta Neves. A**bordagem dinâmica aos crimes via internet.** Disponível em: <http://www.charlieoscartango.com.br/cot-diversos-artigobaeta.html>. Acesso em: 22 nov. 2014