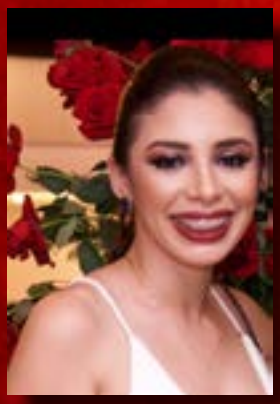
Crimes cibernéticos e investigação policial



Emanuely Silva Costa

Servidora do Ministério Público do Estado do Piauí. Bacharela e Licenciada em Psicologia pela Universidade Estadual do Piauí (UESPI). Atua na área clínica com o público de jovens e adultos, principalmente com transtornos de ansiedade. Bacharela em Direito pelo Instituto Camillo Filho-ICF. Especialista em Direito Constitucional e em Direito Penal e Processual Penal. Discente do Programa de Pós-Graduação em Gestão Pública pela Universidade Federal do Piauí.

Raíla da Cunha Silva

Bacharel em Direito pelo Centro Universitário Santo Agostinho- UNIFSA. Especialista em Direito Penal e Processo Penal pela Faculdade Adelmar Rosado.

Revista Eletrônica do Ministério Público do Estado do Piauí
Ano 01 - Edição 02 - Jul/Dez 2021

CRIMES CIBERNÉTICOS E INVESTIGAÇÃO POLICIAL

RESUMO: O estudo dos crimes cibernéticos é relevante à medida que se considera a utilização da internet como meio hábil e eficaz de comunicação fornecendo ao Direito Penal outros vieses tipológicos. Os crimes cibernéticos apresentam-se como de difícil definição, e conseguintemente, classificá-los não se torna uma tarefa fácil. O objetivo da pesquisa é identificar as condições de investigação policial quando da demanda desses crimes. Para isso utilizou-se a metodologia da pesquisa bibliográfica de caráter exploratório com base no método dedutivo. O propósito do estudo não é o esgotamento do tema, mas sim levantar mais discussões para estudos posteriores. Encontrou-se como principal dado conclusivo a dificuldade de aparelhamento do Estado para subsidiar a investigação policial.
PALAVRAS-CHAVE: Direito e Informática. Crimes Cibernéticos. Investigação Policial.

ABSTRACT: The study of cybercrime is relevant as one considers the use of the Internet as a skillful and effective means of communication, providing the Criminal Law with other typological biases. Cybercrime is difficult to define, and therefore classifying it does not become an easy task. The objective of this work is to identify the conditions of police investigation when the demand for these crimes. The methodology of exploratory bibliographic research was carried out based on the deductive method. The purpose of the present study is not the exhaustion of the theme but raise further discussions further studies. It was found as the main one given the difficulty of equipping the State to subsidize the police investigation.
KEYWORDS: Law and Informatics. Cybercrimes. Police Investigation.

1 INTRODUÇÃO

O presente trabalho versa acerca da conjugação entre crimes cibernéticos e a investigação policial em sua conjectura atual. Partindo do fato de a internet ter crescido muito nos últimos anos, ampliando cada vez mais o número de usuários de vários países do mundo e faixas etárias, nota-se que surge também a questão dos crimes cibernéticos. Sendo algo recente, por vezes é comum pensar que a internet é uma "terra sem lei" e, portanto, alguns crimes começaram a ser reproduzidos também no meio *online*, como invasão de privacidade, espionagem, ataques pessoais como o *bullying,* dentre outros.

Para o estudo é trazido o seguinte problema de pesquisa: "Quais as condições da investigação policial em casos de crimes cibernéticos?". Tem-se como objetivo geral analisar as condições e dificuldades de investigação policial de crimes cibernéticos no contexto brasileiro. Como objetivos específicos traçou-se os seguintes pontos a serem discutidos: conhecer as peculiaridades da investigação policial a partir das características específicas de crimes cibernéticos; analisar as condições de investigação policial relacionando com o aparato

legislativo e infraestrutura de trabalho; identificar meios de suporte para a investigação policial de crimes cibernéticos.

Realizar-se-á uma pesquisa bibliográfica tendo como eixo de trabalho os seguintes pontos: revisão histórica do tema, atualização sobre o tema, respostas aos problemas formulados e discussão dessas respostas por meio de levantamento de paradoxos.

A pesquisa bibliográfica, consequentemente, tem a finalidade de explorar problemas a partir de pressupostos teóricos sobre a abordagem do tema em pesquisas científicas, de forma que esta referência "não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras" (MARCONI; LAKATOS, 2006, p.71).

Os dados serão coletados por revisão bibliográfica ou de literatura, cujos dados secundários serão obtidos na Constituição Federal, nas Leis Codificadas, na legislação ordinária e doutrina.

2 A INTERNET COMO CAMPO FÉRTIL PARA PRÁTICA DE CRIMES

É sabido que a sociedade vem evoluindo a cada dia, e em detrimento da evolução humana, é acrescentado ao ser humano, como meio de sobrevivência, o Direito. Assim sendo, este Direito ganhou amplitude, em razão da capacidade de direcionar o homem tanto em sua vida física, quanto também em sua vida virtual.

Cumpre destacar que a vida humana virtual vem acontecendo por meio das necessidades de comunicação: no mundo contemporâneo, a informação é ponto essencial para a sobrevivência do homem. Portanto, o Direito vem ganhando diferentes ramos de atuações, e a tecnologia é um destes, no caso do Direito Processual Civil que já utiliza a tecnologia para acessar dados virtuais, com a conhecida penhora *online*, como forma de segurança jurídica, dando acesso ao bloqueio de determinada conta bancária, ao poder judiciário.

Da mesma forma, acontece com o Direito do Consumidor, instruindo que há uma necessidade de informar, divulgar produtos para o conhecimento de diversas pessoas com a propaganda via internet, pois é de conhecimento que a grande massa da população tem a internet como atração maior no mundo tecnológico.

Portanto, no que tange ao Direito Penal e Processual Penal, a nova realidade jurídica, em seu meio virtual vem abrindo portas para mais regularizações, como forma de combater os pontos negativos que advém como consequências de tamanha amplitude na comunicação e informação. A internet vem se mostrando um caminho facilitador para também cometimentos

de crimes e impunidades, haja vista que hoje há a necessidade da regulamentação jurídica específica.

A vida humana se tornou totalmente dependente do meio digital, assim é perceptível que na sociedade é quase que inimaginável ter uma população sem a utilização de aparelhos eletrônicos, bem como também de aplicativos, pois a imediaticidade tornou-se um desejo de muitos, com o avanço da tecnologia. O mundo virtual ganha, portanto, seu próprio espaço, chamando-se de ciberespaço, como exemplifica o autor logo a abaixo:

> O ciberespaço encoraja um estilo de relacionamento quase independente dos lugares geográficos (telecomunicações e telepresença) e da coincidência dos tempos (comunicação assíncrona) (...) a extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade (LÉVY, 1999, p.49).

Como destaca-se acima, a comunicação se tornou algo fácil, independe do local onde se esteja, o homem tem a agilidade de receber e passar informações em tempo hábil. Conforme o autor, a facilidade é o motivo de tamanha relevância para as relações humanas estarem enquadradas no ambiente virtual. A internet está sendo um retrato mais fácil da realidade, mas diante de tamanho crescimento virtual vem com ele a vulnerabilidade dos direitos assegurados à humanidade.

Há atualmente uma necessidade de controle quanto ao uso da internet, pois os fatos da vida humana estão sendo colocados no mundo virtual; desde o momento em que se publica uma foto, por exemplo, deixando exposta a localização de tal pessoa, por conta de aplicativos que os rastreia. Cabe também salientar os pontos negativos trazidos por conta desta agilidade do ambiente digital, e o Direito precisa acompanhar o andamento das inovações tecnológicas para tentar combater a inviolabilidade dos direitos inerentes ao homem, ressaltando que os crimes podem tornar-se velados.

O excerto abaixo aponta que há quatro vertentes de condutas praticadas na internet, e indica que na busca da proteção e vigilância do meio cibernético, acaba-se por tornar todos os usuários da internet em criminosos potenciais pela facilidade de acesso e velocidade de disseminação da ação.

> De Acordo com Assange *et al* (2012), essa perspectiva se legitima sobretudo por meio da ideia de que há quatro cavaleiros do apocalipse da informação: pornografia infantil, terrorismo, lavagem de dinheiro e guerra contra as drogas, de modo que, sob o argumento de garantir a maior segurança da população, acaba-se legitimando a ampliação dos mecanismos de vigilância e transformando, portanto, todos os indivíduos em criminosos potenciais (MOTA, HAYASHI, FERNANDES, 2016, p.125).

Agora, conseguintemente, o Código Penal, de 1940, não se deve atentar somente para os crimes do meio físico, pois é chegada a hora de atentar para os chamados crimes de informática. É notório que a facilidade das trocas de comunicações e informações por meios virtuais diminui a segurança entres as pessoas que se utilizam destes, uma vez que entra em riso a divulgação das intimidades, privacidades, de seus usuários. Sabe-se que os benefícios desta evolução tecnológica são perceptíveis, porém também deve-se atribuir uma ferramenta de estabilidade na segurança dos usuários, devendo isto ser alvo de debates para os legisladores.

Vale ressaltar então o texto da carta magna em seu artigo 5º, *caput* e inciso X, da Constituição Federal Brasileira de 1988, que traz o seguinte:

> 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 (BRASIL, 1988).

Deste modo, é de direito a todo e qualquer cidadão ter segurança jurídica quanto a sua vida íntima, não podendo, de forma alguma, sofrer violações de tais garantias dadas pela Constituição Federal Brasileira. Porém, em decorrência de elevadas condutas humanas ilícitas adentrando ao mundo virtual, houve a necessidade de se especificarem determinadas regulamentações jurídicas que fossem diretamente ao ponto dos chamados crimes cibernéticos.

3 INTRÓITO AO ESTUDO DE CRIMES CIBERNÉTICOS

O Direito é um mecanismo que tem como dever orientar a vida em sociedade, por meio de seus instrumentos legais. Deve-se conforme a legislação não só aplicar a lei, mas também buscar melhorias nos departamentos especializados, proporcionar aos agentes que executam as leis uma condição humana de buscar resultados satisfatórios, dando assim incentivos no âmbito do trabalho, fiscalizando os mesmos, para lograr êxito nas punições dos autores.

Neste caso têm-se o surgimento da Lei de nº 12.735/12, que com base na necessidade de especialidades para tal crime, deu-se a criação de polícia especializada na tentativa de

combater crimes cibernéticos, e veio também a incriminação da conduta, caracterizando assim o crime virtual, no artigo 154-A, do Código Penal Brasileiro, que diz:

> 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 [...] (BRASIL, 1940).

Conforme citado, há uma conceituação do que seria a consumação de tal crime, uma vez que, se em períodos da antiguidade houve guerras sangrentas, de povos contra povos, surge nos tempos modernos a necessidade de demonstrar formas de prevenir as guerras atuais por meio da internet, pois já se tem uma grande massa de crimes realizados, detectados na chamada "Era Digital". Portanto, é válido concretizar em palavras a dimensão do crime.

Invadir, como traz o artigo acima mencionado, é o verbo predominante, onde pode-se entender que se trata de uma ação executada contra coisa alheia sem o conhecimento dela, em dispositivos informáticos, para fins de violar intimidades de outrem. Agindo de forma ilícita, o agente adentra na privacidade de alguém com objetivo de oferecer danos a determinado aparelho o qual tenha o acesso sob falha de segurança ou até mesmo burlando tal segurança colocada pelo proprietário legal do bem, formando assim todas essas condutas, elementos de um crime.

A lei de nº 12.737/12, trouxe de modo perceptível benfeitorias no que tange a área dos crimes virtuais, complementando e aperfeiçoando, em busca de resguardar os direitos da informática. A denominação do crime cibernético ainda não pode ser vista como a predominante, uma vez que a doutrina não deixa claro o conceito, podendo assim variar, sendo chamado também de crime de informática, crime virtual e outros. Diante do que se pode estabelecer, têm-se a explicação de Castro:

> [...] São denominados de crimes de informática as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados) (CASTRO, 2003, p.1).

A conceituação a qual o autor acima determina, traz o entendimento que, crime cibernético é quando existe uma ação ilegal, se utilizando do meio tecnológico de informática, como exemplo, praticar invasões contra sistemas utilizados no meio virtual de uma empresa, com a finalidade de furtar dados não autorizados pela empresa proprietária.

3.1 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Doutrinadores costumam discutir sobre classificações de crimes existentes no Código Penal Brasileiro, assim, os meios utilizados para o crime, os danos provocados, a natureza das ações e suas motivações são fatores adicionais para classificação do crime cibernético (GARCIA; MADACAR; LUCIANO, 2018). Pois sendo no ramo do crime digital, diante das discussões, prevalecem duas divisões conhecidas como: puros, mistos e comuns; e próprios e impróprios.

3.1.1 Puros, mistos e comuns

Esta classificação traz consigo a ideia de que crime puro é todo e qualquer crime praticado de modo ilegal, que tenha a finalidade de atacar o alvo de modo objetivo, podendo ser o computador em si. Já em razão do crime de modo misto, tem-se o entendimento que o mundo digital é a forma indispensável para a ação delituosa se concretizar.

Sendo assim ao crime comum, a conceituação é de crime já existente no mundo real, fazendo parte do Código Penal vigente, mas que necessita de uma ação humana ilícita, com o uso dos meios tecnológicos, para ratificar tal crime.

3.1.2 Próprios e impróprios

Sabe-se que o Código Penal, não pune infrações que não estão previstas em leis, e seguindo essa linha, vale ressaltar que neste ponto encontra-se uma dificuldade de punir criminosos quanto ao cometimento do chamado crime cibernético, uma vez que para receber a classificação de crime próprio, precisa estar com sua devida previsão legal. Em contrapartida, no que tange ao crime impróprio, é quando se utiliza recursos informáticos para auxiliar o autor ao cometimento dos delitos, no entanto não depende somente deste meio para a efetivação do crime cometido, podendo neste caso caber punição.

No caso de crime impróprio, pode ser perceptível na situação de um crime de homicídio, quando através de dados de informações sobre medicação, um agente de forma ilícita acessa uma rede de informática de determinado estabelecimento hospitalar, induzindo os profissionais de saúde a medicar o paciente com uma dosagem elevada, levando o mesmo ao óbito.

Exemplificando um tipo de conduta que acarretaria a classificação para crimes próprios, seria o cometimento do crime que traz o art.313-B, incluído no Código Penal pela

lei n° 9.983/03, como segue: Art.313-B. *Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: pena- detenção, de 3 (três) meses a 2(dois) anos, e multa*.

O artigo em epígrafe retrata a sociedade atual, que tem como direito receber do poder estatal um amparo quanto a segurança jurídica em razão dos crimes inovadores, através das redes de informática, atentando-se para as transformações sociais, que elevam os campos para cometimentos de delitos. Portanto, o Legislativo vem buscando soluções quanto as punições e investigações do crime cibernético, sendo o artigo mencionado, uma inovação feita através da lei ora citada.

3.1.3 Lugar do crime

O local do crime é um tema relevante para a doutrina, pois há discussões no Direito Penal, em detrimento da punição do autor do delito, quanto a regulamentação de determinado lugar. Em razão dos crimes comuns, prevalece o entendimento que será dada a punição ao autor, conforme a legislação local de onde se consumiu tal delito.

Diante de tal conhecimento, atualmente a questão vai muito além do simples espaço dos atos executórios ou consumados, pois com as evoluções da sociedade seguidas de crescimentos no mundo digital, é necessária a percepção de enquadrar-se a nova denominação de lugar, quando se trata de crimes cibernéticos.

Nesta linha, segue o entendimento a seguir:

> Sob uma ótica prática, uma pessoa que vive no Brasil pode modificar dados armazenados na Itália, transferindo-os para Alemanha de modo a obter vantagem ilícita. Da mesma forma um vírus de computador pode ser desenvolvido em um país e disseminado por milhares de máquinas por todo o globo terrestre. A transmissão de dados pode envolver diversos países, de modo que o lugar do crime seja determinado de forma quase fortuita (CRESPO *apud* ROCHA, 2013).

Assim, é possível perceber a fragilidade da segurança jurídica quanto a questão da denominação de espaço territorial do lugar do crime, quando se trata de mundo virtual.

3.1.4 Competência

O artigo 70 do Código de Processo Penal traz o texto que diz ser o foro competente para julgar os crimes comuns, aquele onde foi consumado ou no caso de tentativa, onde foi

feito os últimos atos executórios, porém a questão é que tratando deste crime específico, não é tão fácil assim determinar a Justiça competente.

Doutrinadores discutem sobre qual seria a justiça competente para julgar os crimes digitais, uma vez que nem mesmo sua classificação, e nem sua conceituação, ainda possuem uma estabilidade. Apesar de terem conquistado inovações na legislação que determina tal crime, e pune o criminoso, ainda precisa ter uma atenção maior do Estado, pois trata-se de um tipo de crime global.

E o que define a maioria da doutrina, é que mesmo sendo um crime de expansão territorial, com inúmeras redes de internet espalhadas, não será da competência Federal, se não for contra a União e preencher os requisitos do artigo 109, incisos IV e V da Constituição Federal, ficando, portanto, responsável o Estado onde tenha sido cometido o delito, conforme identificação da atuação do autor. O que parece é que existe a falha ainda do Estado, visto que é necessária uma legislação que delimite a competência para ações e julgamentos dos crimes cibernéticos.

4 A EVOLUÇÃO DA LEGISLAÇÃO NO BRASIL

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 coadunada 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 as novas condutas realizadas pelos meios informáticos. Tal debate acalorou-se quando da repercussão do episódio ocorrido com uma figura pública, em que esta teve vazadas por meio de invasão do seu computador fotos de sua intimidade.

Este cenário culminou na publicação da Lei º12.737/2012, pela qual o Código Penal Brasileiro foi alterado, através da tipificação penal para os crimes cibernéticos. Especificamente o dispositivo 154-A do Código Penal Brasileiro, o qual tipifica a conduta de:

> 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.

A publicação da Lei também trouxe alterações aos artigos 266 e 298 do Código Penal, conforme resumem os seguintes autores:

> A Lei 12.737/12 introduziu no ordenamento jurídico 3 tipificações penais no Código Penal: o artigo 154- A que versa sobre a invasão de dispositivo informático alheio, o artigo 266, §1º e 2º que fala sobre a interrupção ou perturbação de serviço telefônico, telegráfico, informático, telemático ou de informação de utilidade pública, artigo 298,§ único, que tipifica falsificação de cartão de crédito ou débito (MAUES, DUARTE, CARVALHO, 2018, p.173).

> A nova Lei ainda alterou a redação do artigo 266 do Código Penal, que acrescentou ao crime de "interrupção ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento", o parágrafo 1° que dispõe que incorrerá na mesma pena aquele que interrompe serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar-lhe o restabelecimento, bem como também acrescentou ao artigo 298 o parágrafo único, o qual dispõe que para fins de falsificação ou alteração, equiparasse o documento particular o cartão de crédito (HARAKEMIV; VIEIRA; 2014, p. 425).

A crítica tecida a esse dispositivo diz respeito a não determinação do que seriam dos dispositivos informáticos e as vulnerabilidades, bem como a responsabilização dos provedores de internet (ROCHA, 2013).

Ainda, Harakemiv e Vieira (2014) diz que mesmo os artigos inclusos no Código Penal 154-A e 154-B, presentes no título I do Código, referindo-se aos crimes contra honra, referem-se também a intimidade, a vida privada e o direito ao sigilo de dados constantes em dispositivos informáticos, tutelam também o patrimônio do titular do dispositivo violado.

No que concerne ao sujeito ativo dos crimes cibernéticos poderá ser qualquer pessoa, sendo classificado como crime comum, e quanto ao sujeito passivo considera-se qualquer pessoa que utilize ou não o meio eletrônico.

> No crime em questão, adicionado ao Código Penal pela Lei 12.737/12, considera-se que pode incorrer como sujeito ativo qualquer pessoa, já que o seu tipo penal não exige nenhuma qualidade especial do seu agente, sendo, portanto, um crime comum. Quanto ao sujeito passivo dos crimes informáticos considera-se que possa ser qualquer pessoa que utilize ou não o meio eletrônico, podendo existir mais de um indivíduo desde que tenham seus bens jurídicos ameaçados ou lesados pela mesma conduta delituosa, como por exemplo, uma série de e-mails contendo o mesmo

> conteúdo viral cujo objetivo é lesar quem os recebe (HARAKEMIV; VIEIRA, 2014, p.424).

São crimes que não necessitam de um resultado material, portanto, crimes formais, aonde a invasão do dispositivo ou instalação de vulnerabilidades no equipamento, admitido em sua forma tentada e somente suportando a forma dolosa da conduta.

A lei estabelece como pena para a prática deste tipo detenção de 3 (três) meses a 1 (um) ano, e multa, o parágrafo único estabelece que na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com intuito de permitir a conduta descrita no *caput* do artigo 154-A. E se resultar em prejuízo econômico a pena aumenta de um sexto a um terço. Ainda, o artigo discorre a forma qualificada do crime, nos parágrafos 3° e 4° que prenunciam "se da invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto de dispositivo não autorizado", a pena de reclusão será de 6 (seis) meses a 2 (dois) anos, e multa, sendo aumentada de 1 a 2 terços se houver divulgação, comercialização, ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, caso a conduta não constitua crime mais grave.

Ainda, a Lei nº 12.735/12, que foi proposta à época pelo deputado federal Eduardo Azeredo (PSDB), e teve como objetivo alterar o Código Penal, o Código Penal Militar e a lei contra o racismo, tipificou condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados (MAUES; DUARTE; CARVALHO; 2018, p.172).

Ainda, cita-se o marco civil da internet, Lei nº12.965/2014, que no âmbito civil estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, especialmente assegura em seu artigo 3º: liberdade de expressão, comunicação e manifestação do pensamento, sendo vedado o anonimato previsto no artigo 5º, inciso IV da Constituição Federal. A lei trouxe, conforme acentua Maues, Duarte e Carvalho (2018, p. 176) "a guarda e proteção de dados por provedores de conexão e de aplicação, apontando medidas de transparência na requisição de dados cadastrais pela administração pública e parâmetros para a apuração e fiscalização de infrações".

Ainda é válido ressaltar que Barreto e Brasil (2016) aponta que a própria Constituição Federal Brasileira através dos dispositivos que capitulam os princípios e garantias das liberdades fundamentais dos indivíduos aplica-se aos cibercrimes, a exemplo dos artigos 1º, 3º, 4º, 5º, 6º, 215, 218, 219, 220.

5 CRIMES CIBERNÉTICOS E A INVESTIGAÇÃO POLICIAL

É sabido que as atribuições da Polícia Judiciária foram descritas no artigo 144 da Constituição Federal Brasileira de 1988. As polícias são instituições de Direito Público que buscam manter junto à sociedade a paz pública e a segurança. Desta forma cabe à Polícia duas funções, uma de cunho administrativo e uma de cunho judiciário. Assim, a atuação se dá preventiva e repressivamente para disciplinar, regular e fiscalizar direitos e interesses dos cidadãos (BRENE; LEPORE, 2017).

A magna carta preceitua em seu artigo 144, Parágrafo 4º, que cabe às polícias civis, dirigidas por Delegados de Polícia de carreira, ressalvadas as competências que tocam a Polícia Federal e militares, as funções de polícia judiciária e a apuração de infrações penais.

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 a elucidação destes crimes. Outro ponto a ser discutido seria o destacado por Rocha (2013) no trecho transcrito abaixo:

> Estudiosos sobre o tema ainda afirmam que uma alteração no Código Penal não é conditio *sine qua non* para que se possa combater e coibir de forma eficaz os cibercrimes. O professor de Direito Penal da Faculdade Federal de Minas Gerais e Mestre em Ciências Penais pela UFMG Túlio Lima Vianna assevera que o nosso ordenamento não necessita de lei regulamentadoras e sim, um aparato técnico e específico nas investigações forenses por parte das polícias quanto a estes delitos e uma ação conjunta entre os diversos entes que corporificam o Poder Judiciário e o Ministério Público (ROCHA, 2013, p.8).

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 do mais, considera-se que a motivação para a prática de crimes virtuais é diversificada: Garcia, Macadar e Luciano (2018) apontam que esta depende de dois fatores, um a recompensa final e outro o risco envolvido, além de diferenças individuais. Os autores

enumeram categorias de classificação, conforme a motivação para a prática do crime, dos autores de crimes cibernéticos: novatos, *punks* cibernéticos, *insiders* ou colaboradores, pequenos ladrões, *hacker* da velha guarda, criminosos profissionais, guerreiros da informação (ROGERS, 2006 *apud* GARCIA, MACADAR e LUCIANO, 2018).

O fato de os crimes cibernéticos serem praticados em espaços que não têm fronteiras dificulta a identificação do criminoso e ainda essas inúmeras motivações acabam por dificultar a tarefa do Estado, que tem como incumbência essencial a identificação do autor do delito, conforme explica Harakemiv e Vieira (2014) no trecho abaixo:

> Contudo, da mesma forma que é fácil identificar um crime cibernético, a identificação do autor do delito é praticamente impossível, tendo em vista que para acessar a internet não há nenhuma forma de controle e nem a necessidade de identificação. Desta forma qualquer pessoa pode ser autora do crime, e sua identificação é muito difícil, pois os usuários se conectam à rede através de uma tecnologia conhecida como Tcp/ip (*transmission control protocol –internet protocol*) cujo software normalmente reside no sistema operacional, onde todos os programas e aplicativos utilizados na máquina compartilham do mesmo número (ip) que é único e se altera automaticamente a cada novo acesso à internet, sendo assim o agente pode se conectar de qualquer dispositivo eletrônico e de qualquer lugar cometer o ilícito penal utilizando apenas conhecimentos próprios e se valendo indiscriminadamente desse meio ciente de que após cometer a infração e se desconectar da internet a única forma possível para sua identificação, ou seja, o número de ip utilizado momentos antes pelos programas empregados na prática delituosa foi apagado, sendo gerado um novo ip em uma conexão à internet futura (HARAKEMIV; VIEIRA, 2014, p.424).

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), conforme indica Barreto e Brasil (2016): "[...] 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 o 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, p.15).

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.

Ainda segundo os autores, é mencionado que quanto a preservação do conteúdo até apresentam a diferença entre preservação e arquivo de dados: 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.

O provedor de aplicação de internet Facebook disponibiliza uma plataforma denominada *Law Enforcemen 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).

Dados cadastrais podem ser solicitados diretamente aos provedores, sem necessidade de ordem judicial. Em casos como risco de morte ou risco a 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.

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, contribuiriam para aplicação da lei, facilitando também a desburocratização das demandas.

É salutar que a principal questão quanto à investigação policial, como já abordado, 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". Ainda os autores Maues, Duarte e Cardoso (2018) fazem um apontamento além da necessidade de especialização policial, conforme explicitado abaixo:

> Ou seja, delegacias de polícias precisam ser especializadas em crimes cibernéticos, os juízes devem se atualizarem nas jurisprudências e doutrinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil (MAUES, DUARTE, CARDOSO, 2018, p.178).

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 e 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).

CONSIDERAÇÕES FINAIS

Neste seguimento, entende-se que a principal demanda apontada frente ao combate dos crimes cibernéticos é a premente necessidade de aperfeiçoamento contínuo dos policiais que trabalham diretamente com a investigação criminal. No entanto, verifica-se que a adoção de medidas como a identificação do prosseguimento a tomar nesses casos já vem sendo discutida na doutrina, o que torna o enfrentamento a essas condutas mais eficazes. Dentre essas medidas, destaca-se o trabalho realizado pela polícia junto aos provedores de aplicação

de internet, que contribuem para elucidação destes crimes. Outro ponto a ser ressaltado, seria a necessidade de cooperação entre as polícias estaduais e federal, e também a necessidade de troca de informações entre as polícias internacionais, de modo a sempre incrementar as práticas. Em suma, não se buscou o esgotamento da temática, porém, a apresentação do cenário atual da investigação destes crimes e algumas alternativas a precariedade do aparato estatal.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernético à luz do Marco Civil da internet**. Rio de Janeiro: Bransport, 2016.

BRASIL, **Código de Processo Penal Brasileiro**: promulgado em 03 de outubro de 1941. Decreto-Lei nº 3.689 de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm . Acesso em 14 de dezembro de 2018.

BRASIL, **Código Penal:** promulgado em 7 de dezembro de 1940. Lei Nº 12.735, de 30 de novembro de 2012**.** Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em 15 de dezembro de 2018.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: senado, 1988.

BRENE, Cleyson; LEPORE, Paulo. **Manual do Delegado de Polícia Civil**: Teoria e Prática. Salvador: Editora Juspodvim, 2017.

CASTRO, Aldemario Araujo. **A internet e os tipos penais que reclamam ação criminosa em público**. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf . Acesso em 14 de dezembro de 2018.

DIAS, Virgínia Soprana. **Aspectos da segurança jurídica no âmbito dos crimes cibernéticos**. 2007. Disponível em: http://icofcs.org/2007/ICoFCS2007-pp12.pdf. Acesso em 14 de dezembro de 2018.

GARCIA, Plínio Silva; MACADAR, Marie Anne; LUCIANO, Edimara Mezzono. A influência da injustiça organizacional na motivação para a prática dos crimes cibernéticos.

Jistem usp, Brazil, vol. 15, 2018. Disponível em: http://www.scielo.br/pdf/jistm/v15/1807-1775-jistm-15-e201815002.pdf . Acesso em 01 de junho de 2019.

HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. Crimes Cibernéticos. **Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais**, 2014. Disponível em: http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-an%C3%A1lise-do-processo-investigat%C3%B3rio-e-desafios-enfrentados. Acesso em 15 de dezembro de 2018.

LEVY, Pierre. **Cibercultura**. Tradução de Carlos lrineu da Costa. São Paulo: Editora 34, 1999. (Coleção TRANS).

MARCONI, M. A.; LAKATOS, E. M. Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliografia, projeto e relatório, publicações e trabalhos científicos. 6.ed. São Paulo: Atlas, 2006.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladerson Ronny da Silva (2018). CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira. **Revista Científica da FASETE. Disponível em :** http://www.egov.ufsc.br/portal/sites/default/files/crimes_virtuais_2.pdf . Acesso em 01 de junho de 2019.

MOTA, Bárbara Maria Farias; HAYASHI, Renato; FERNANDES, Antônio Alves Tôrres. Hancking político: crime cibernético ou manifestação legal de protesto. **Argum**. Vitória, v.8., n.3, p.122-132, set/dez. 2016. Disponível em: file:///C:/Users/emanu/Downloads/13396-40958-1-PB.pdf. Acesso em 01 de junho de 2019.

ROCHA, Carolina Borges (2013). **A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.** Disponível em: http://www.amab.com.br/fileadmin/user_upload/A_evolucao_criminologica_do_Direito_Penal.pdf. Acesso em 14 de dezembro de 2018.

SILVA, Paulo Quintiliano. **Crimes cibernéticos e seus efeitos internacionais**. 2006. Disponível em: http://icofcs.org/2006/ICoFCS2006-pp02.pdf . Acesso em 14 de dezembro de 2018.