[1]DESAFIOS NO ENFRENTAMENTO DOS CRIMES VIRTUAIS/ CHALLENGES IN ADDRESSING VIRTUAL CRIMES

Janaina de Latres Ferreira [2]

Dienifer Talini Santiago da Silva

RESUMO: O presente artigo tratará dos desafios do Direito Penal frente aos crimes virtuais. Será abordado a origem da internet e como a mesma impactou os indivíduos e a sociedade. Será analisado como os criminosos exploram a internet e como a situação é alarmante, pois a medida que a tecnologia avança, os crimes virtuais também avançam na mesma velocidade. O artigo enfatiza a dificuldade na obtenção de provas dos crimes virtuais, pois trata-se de crime complexo e que exige muita técnica do investigador e estrutura adequada de tecnologia para se identificar autoria e produzir um conjunto probatório suficiente. São muitos os desafios para o enfrentamento dos crimes cibernéticos. A metodologia de pesquisa foi uma revisão bibliográfica, descritiva e exploratória envolvendo autores de artigos jurídicos e utilização da legislação pertinente que descrevem o tema abordado.

PALAVRAS-CHAVE: Internet. Crimes virtuais. Provas. Código Penal.

---

[1] Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito, orientado pela Professora Priscilla Paula de Oliveira Prado.

[2] Acadêmicas do Curso de Direito na Faculdade Integrado de Campo Mourão – PR. E-mails: janaina.latres@gmail.com e dienifertalini6@gmail.com.

ABSTRACT: This article will address the challenges of Criminal Law in the face of virtual crimes. The origin of the internet and how it impacted individuals and Society will be adressed. It will be analyzed how criminals exploit the internet and how alarming the situation is, because as technology advances, cybercrimes also advance at the same speed. The article emphasizes the difficulty in obtaining evidence of virtual crimes, as it is a complex crime that requires a loto f technique from the investigator and adequate technology structure to identify authorship and produce a suficiente body of evidence. There are many challenges to tackle cybercrime. The research methodology was a bibliographic, descriptive and exploratory review involving authors of legal articles and the use of relevant legislation that describe the topic addressed.

KEYWORDS: Internet. Virtual crimes. Evidences. Penal Code.

1 INTRODUÇÃO

A internet vem evoluindo exponencialmente. No Brasil, seu funcionamento ocorreu originariamente com a possibilidade de tão somente retirar arquivos de correio eletrônico, e, após o ano de 1991, houve a liberação para acesso nas instituições de ensino, até culminar com a liberação do acesso a banco de dados, transferências de arquivos e softwares.

Atualmente tem-se a utilização das redes sociais que a cada dia crescem mais e estão fazendo parte da vida e rotina diária de seus usuários, no entanto, apesar de todos seus benefícios, também tem seus pontos negativos, pois, alguns criminosos se aproveitam desse meio para realizar suas atividades ilícitas.

Desse modo, verifica-se que hoje, tem-se um grande desafio a ser enfrentado, pois o acesso ilimitado ao mundo digital, também trouxe grandes problemas no que se refere às práticas criminosas.

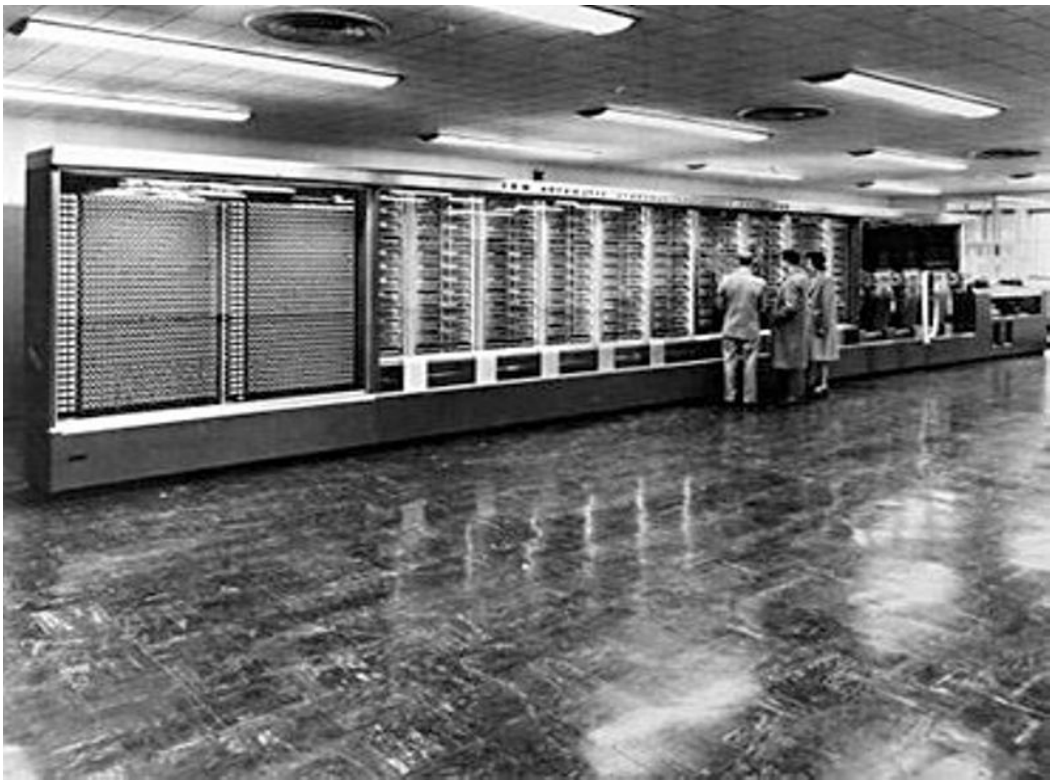
O maior problema dos crimes cometidos em meio virtual, está ligado a obtenção de provas para se identificar a autoria, pois são crimes complexos, rápidos e que a legislação tem dificuldade de acompanhar, dada a sua especificidade tecnológica. Assim, o presente artigo aborda estes aspectos que constituem os crimes virtuais.

2 EVOLUÇÃO HISTÓRICA DA INTERNET

2.1 O SURGIMENTO DA INTERNET

A internet nasceu na segunda guerra mundial em conjunto com a Universidade de Harvard. A marinha desenvolveu o computador eletromecânico Mark, conforme a figura abaixo demonstrada, com base na calculadora analítica de Babbage,projetado pelo professor Howard Aiken. (LEMOS, 2004).

Figura 1 – Havard Mark 1



Fonte: http://www.computerhistory.org/timeline/1944/

Sobre o surgimento da Internet, Castells afirma que:

> A história da criação e do desenvolvimento da Internet é a história de uma aventura humana extraordinária. Ela põe em relevo a capacidade que tem as pessoas de transcender metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo. Reforça também a ideia de que no processo a cooperação e a liberdade de informação podem ser mais propícias à inovação do que a competição e os direitos de propriedade.

A internet, começou com a ARPANET em 1969, foi criada pela ARPA e o objetivo era uma rede promissora para dados valiosos (Castells, 2001).

A transição de ARPANET para INTERNET ocorreu na década de 80. A ARPANET não foi a única responsável pela rede de internet, conforme Castells, é resultante de uma base de formação de computadores.

Sobre o desenvolvimento da internet Castells afirma:

> No início da década de 1990 muitos provedores de serviços da Internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais. A partir de então, a Internet cresceu rapidamente como uma rede global de redes de computadores.

O padrão IP/TCP protocolo de controle de transmissão/protocolo da internet (Transmission Control Protocol/Internet Protocol) estabelecido no ano de 1982, se tornou obrigatório a partir do ano de 1983, em 1990 foi desativada a ARPANET (Advanced Research Projects Agency Network), em português, Rede da Agência de Pesquisas em Projetos Avançados, e substituída pelos backbones da NSFNET (**National Science Foundation Network**)Rede Nacional de Fundação Científica.

2.2 A INTERNET NO BRASIL

No ano de 1994, a Embratel lançou um serviço para experimentar e conhecer melhor a internet, e surgiram serviços de bancos online em uma rede dada pela Pizza Hut. Os Ministérios de Comunicações, Ciência e Tecnologia iniciaram a internet para operação comercial em 1995 e a internet foi privatizada. Assim, iniciaram as contratações com a Rede Nacional de Pesquisas e Embratel.

No Brasil, a internet chegou quando o presidente Fapesp Oscar Sala fez os primeiros contatos para conseguir a conexão. No início quando ocorreu o primeiro funcionamento apenas era possível a retirada de arquivos e de correio eletrônico, após no ano de 1991, já houve a liberação para acesso nas instituições de ensino, liberando-se o acesso a banco de dados, transferências de arquivos e softwares.

O Instituto Brasileiro de Análises Sociais e Econômicas fez um convênio com a Associação para o Progresso das Comunicações em 1992, para organizar espaços não governamentais entre as redes de informação, o que mudou quando foi criada a Rede Nacional de Pesquisa, responsável por organizar oacesso a internet para todas as regiões do Brasil. A RPNRiscos por não Conformidades em 1995 estendeu seus serviços para todos setores da sociedade. No mesmo período, o Ministério da Comunicação e o Ministério da Ciência e da Tecnologia efetivaram a participação da sociedade para essa implantação da internet (RNP, 2017).

A internet desde a sua criação, evolui a cada dia e cada vez alcança um número maior de usuários.

A internet proporciona às pessoas vários benefícios, porém, ao mesmo tempo, trás desvantagens, relacionadas a vulnerabilidade tecnológica, e é neste ponto onde acontecem os crimes virtuais, que também podem ser chamados de: crimes digitais, informáticos, telemáticos, de alta tecnologia, delitos cibernéticos, fraude informática, dentre outros.

O mundo virtual é fascinante, tendo em vista a possibilidade das relações virtuais, só que este fato, também possibilita o anonimato, o que faz com que a prática desses delitos aumente e dificulte a investigação.

3 AS REDES SOCIAIS

Atualmente, as redes sociais fazem parte da rotina diária de seus usuários, através delas é possível ter acesso a informações, pesquisas e notícias no momento em que acontecem, o acesso é praticamente imediato em quase tudo.

Com o início da WEB ocorreu a maior revolução das redes sociais, conhecido atualmente como World Wild Web. “Por transposição, a rede é assim um instrumento de captura de informações” (FANCHINELLI; MARCON; MOINET, 2004)

CASTELLS (1999) ainda acrescenta que a abertura e porosidade é uma das características fundamentais para definição das redes sociais, possibilitam relacionamentos entre grupos de pessoas, sem diferenças, as redes sociais não são outra

forma de estrutura, mas sim uma quase não estrutura, porque uma parte de sua força está na habilidade de forma rápida se desfazer e fazer.

As ferramentas de mídias sociais se propagaram em meados dos anos 90, quando ocorreu a evolução da internet 2.0, o que permitiu aos usuários uma diversificada troca de informações e assuntos de interesse comum, sendo essas: mensagens de textos, redes sociais, compartilhamento de fotos ou vídeos, entre outras mídias sociais criadas.

Malini (2008) afirma que a democratização das ferramentas de produção através da internet caracterizam o sucesso tecnológico.

Wolton (2003) menciona que sem filtro, cada um pode agir sem intermediário, e produzir reflexos na esfera jurídica, porque essas trocas de informações podem causar danos, ensejando a necessária reparação.

Além do mais, as redes também tem sido exploradas como um instrumento para ativar movimentos sociais e culturais, algumas delas sendo: a luta pelos direitos humanos, ambientalistas, feministas, entre outros. E também na educação, com a participação em comunidades virtuais de debate e argumentação.

Diante de tanta complexibilidade de funções, constata-se que as redes são canais onde o fluxo de informação, valores, vínculos e discursos sociais é vultoso, e assim vem ampliando, delimitando e mesclando os territórios. As redes sociais convidam a refletir e repensar sobre as relações em tempo pós-modernos (MACHADO, 2012).

Com as ferramentas tecnológicas se desenvolvendo, surgem novas formas de relação, comunicação e organização de atividades humanas, uma delas inclusive, é o estudo das redes sociais virtuais.

Segundo Aguiar (2007) não há forma de garantir um controle de todas interações, porque o processo social nas redes vem ocorrendo de forma dinâmica e participativa entre grupos de referências.

Atualmente, a internet é o meio de comunicação mais utilizado no Brasil, e no mundo todo, algumas das redes sociais que foram surgindo no decorrer dos anos são:

Youtube, Google, Twitter, Facebook, Instagram, dentre outras, e, em cada uma delas os usuários tem livre acesso para publicações, fotos, manifestação de idéias, e mais uma infinidade de funções que podem ser utilizadas.

O lado positivo das redes é que, é uma forma rápida e prática para ter contato com outras pessoas, familiares que residem em lugares distantes, conhecer pessoas novas, porém, tem o lado negativo, muitas pessoas fazem mau uso dessa ferramenta, para denegrir a imagem de outro, proferir comentários ofensivos, cometer delitos, situações que movimentam o Judiciário.

3.1 VIOLAÇÃO À SEGURANÇA NAS REDES

A segurança de redes,trafegam na garantia de confidencialidade, integridade e disponibilidade. Entretanto as ameaças e riscos intencionais ocorrem de forma comprometedora, os mecanismos de defesa para a proteção computacional são vulneráveis.

A identificação pode ser utilizada como exploração para que as vulnerabilidades sejam controladas.

As redes sociais não são mais limitadas ao relacionamento entre seus usuários, mas também são fontes de pesquisas e notícias, e tem como atributos a interatividade e participação, possibilitando alémdo acesso à informação, a capacidade de produzi-la.Pode-se perceber que tudo o que for publicado na internet pode ser recriado, modificado mais facilmente que na via impressa.

Verifica-se que o acesso a internet e as redes sociais trouxeram ampla liberdade de informação e de acesso, sendo que cada vez se utiliza mais e mais estas ferramentas, o que facilita a vida das pessoas mas também trazem inconvenientes, principalmente quando relacionado aos delitos praticados virtualmente.

Assim, um dos maiores problemas é controlar, combater e fiscalizar os chamados “cibercrimes” que são comuns atualmente no mundo virtual e que tem gerado muito transtorno por causa da violação de segurança e práticas como fraudes bancárias,

violação de direitos autorais e ciberextorsão, por exemplo, têm sido frequentes infelizmente.

São vários os problemas que circundam os crimes virtuais, no entanto a falta de conhecimento dos usuários, tornam a prática comum e faz com que os criminosos cada vez mais “invistam” neste tipo delito, dado a facilidade de acesso às vítimas.

Deste modo, a prevenção dos crimes é extremamente importante, ou seja, é importante que se veicule informações acerca dos crimes para que as pessoas se conscientizem da existência dessas práticas e tomem certos cuidados na utilização das redes.

4 CRIMES VIRTUAIS

4.1CONCEITO

Os crimes digitais são condutas típicas, antijurídicas e culpáveis que são praticadas contra os sistemas de informática, ou até mesmo utilizando-os contra seus usuários.

Sérgio Marcos Roque (2005, p. 25) conceitua crimes cibernéticos como “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.”

Na maioria dos crimes digitais ocorridos, o computador é a ferramenta mais utilizada por esses criminosos, pois permite acesso a vários tipos de sistema, tornando mais fácil o acesso a vítima.

Os crimes virtuais ocorrem quando o indivíduo sem autorização para utilizar o sistema, o invade com o objetivo de subtrair, danificar e modificar dados que são essenciais para o funcionamento desse sistema.

Pinheiro (2010, p. 46) para conceituar crimes virtuais, afirma:

> Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação

> ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes.

Essa conceituação se refere ao acesso em sistemas de informação que não são permitidos, e que geram transtornos e alteração de dados sigilosos.

Essas situações tendem a aumentar, com o crescimento de pessoas que estão utilizando à rede, é um espaço onde circula muitas informações, o que expõe a privacidade do usuário e o deixa vulnerável a prática delituosa.

4.2 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Os crimes informáticos podem ser classificados, segundo Vianna (2003)em Crimes Informáticos Impróprios, Próprios, Mistos e Mediatos ou Indiretos.

Vianna os define como:

a) Crimes Informáticos Impróprios: é aquele em que o computador é usado para a execução do crime, porém, não ocorre a ofensa ao bem jurídico inviolabilidade da informação que são os dados.
b) Crimes Informáticos Próprios: quando o bem jurídico protegido pela norma penal é a inviolabilidade das informações, ou seja, os dados.
c) Delitos Informáticos Mistos: são crimes em que, além da proteção da inviolabilidade dos dados, também visa tutelar bem jurídico de natureza diversa.
d) Crimes Informáticos Mediatos ou Indiretos: é quando o delito não é informático, herdou esta característica de delito meio-informático que é realizado para possibilitar sua consumação.

Os crimes virtuais segundo Guimarães e Furlaneto Neto (2003), também podem ser classificados como Virtuais Puros, Mistos e Comuns, definidos como:Crime Virtual Puro: qualquer conduta ilícita que atenta o hardware e/ou software de um computador, tanto a parte física quanto a virtual.

a) Crime Virtual Misto: utiliza a internet para realizar a conduta, o objetivo é diferente do acima citado, como por exemplo, transações ilegais de valores de contas correntes.
b) Crime Virtual Comum: quando o indivíduo utiliza da internet apenas para realizar um delito, como por exemplo, a distribuição de conteúdo pornográfico infantil por vários meios.

Existem vário tipos de crimes cibernéticos, e mesmo sem lei específica que tipifique cada conduta, não ficarão impunes, dada a possibilidade de enquadramento no Código Penal e demais normas penais existente no ordenamento.

Os principais crimes virtuais ocorridos no Brasil são:

a) Pirataria: que é cópia de dados em CDs, DVDs ou qualquer base de dados sem autorização que entende-se como pirataria de acordo com a Lei 9.610/98.
b) Dano ao Patrimônio: pode ser simples ou qualificado, só é qualificado quando for contra patrimônio da União, Estado, Município, entre outras, está previsto no art. 163 do Código Penal.
c) Sabotagem Informática: é a invasão de determinado estabelecimento, em que visa roubar e/ou prejudicar dados, podendo ser feitas através de vírus ou programas destrutivos.
d) Pornografia Infantil: é o compartilhamento de materiais pornográficos de crianças e/ou adolescentes, entre outras situações que são proibidas pelo art. 241 do Estatuto da Criança e do Adolescente.
e) Difamação, Injúria e Calúnia: podem ser ocorridos por meio de publicações, mensagens, nas redes sociais, quando divulgam informações falsas sobre alguém, ofendam a dignidade ou acusem de algum fato criminoso.
f) Falsa Identidade: quando alguém mente seu nome, sexo, estado civil, entre outras, para prejudicar ou obter vantagem de alguém.

Existem diversos tipos de crimes cibernéticos, mas muitos não possuem ainda *modus operandi*conhecido, e muitos, nem mesmo foram descobertos.

5 PROBLEMÁTICAS EM RELAÇÃO AO COMBATE DOS CRIMES VIRTUAIS

Os crimes virtuais são de difícil comprovação e combate, devido a legislação existente não ser suficiente, além de ter havido um aumento considerável da prática destes delitos. Não é possível punir os autores sem saber quem são e há dificuldades em identificá-los.

Carlos Eduardo Sobral, que é chefe da unidade de Repressão a Crimes Cibernéticos da Polícia Federal, afirmou que, o número de pessoas capacitadas para realizar as investigações desse crime não é maior que o volume de crimes cometidos atualmente. (Apud. Canuto, Luiz Cláudio, 2015).

O artigo 386 do Código Penal, informa que faz-senecessário ter certeza da autoria e materialidade do crime, ou que existam fortes indícios para que seja aplicada a sanção penal.Veja:

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal;IV - Estar provado que o réu não concorreu para a infração (...) V - Não existir prova de ter o réu concorrido para a infração penal;
>
> (BRASIL, 1941, Art.386)

Por isso, a grande dificuldade de repressão a este tipo de delito está adstrita a dificuldade de identificação do autor e sem certeza de autoria ou ao menos fortes indícios, a punição resta prejudicada.

A comprovação da materialidade e autoria devem ocorrersempre de forma lícita e de acordo com o que estabelece a lei quanto ao procedimento, deste modo, para se chegar ao autor do crime, terão que ser identificados, como ocorreu o crime, o local, e endereço de IP,e para isso a autoridade policial responsável pela investigação necessita de autorização do Juiz para pedir tais diligências para as plataformas que armazenam as informações de localização do autor, e esta tarefa não é tão simples, isso porque, o artigo 5º, incisos X e XXII da Constituição Federal protegem a privacidade de dados, tornando este esse processo de obtenção de provas mais demorado e complexo.

Importante salientar que algumas provas só podem ser colhidas com autorização, pois, se não autorizadas não serão válidas e com isso não poderão ser utilizadas.

> [...] a admissibilidade, ou seja, ter condições de ser usada no processo; autenticidade, ser certa e de relevância para o caso; a completude, pois esta não poderá causar ou levar a suspeitas alternativas; a confiabilidade, não devem existir dúvidas sobre sua veracidade e autenticidade; e a credibilidade, que é clareza, o fácil entendimento e interpretação.

Mas, se tratando de meios virtuais, muitas das vezes não se atendem tais requisitos, o perito precisa preservar a integridade desses dados. Outro procedimento que é essencial é a localização, realizada através da identificação de endereço de IP.

Assim, a verificação e a identificação é por demais complexa, pois demanda muita técnica e aparelhamento das autoridades que detém o poder de investigação.

6 PROVA

5.1PERÍCIATÉCNICA

Para a perícia atuar nesses casos de crimes virtuais, necessita de muito conhecimento técnico para descobrir a origem do fato, são delitos considerados novos no ordenamento jurídico, somente com conhecimento técnico pode se ter alguma noção para saber onde e como ocorreram. Além disso, precisa de uma estrutura, equipamentos para processar as informações e ferramentas que auxiliam nessa busca.

Identificado o endereço IP, as possíveis provas serão analisadas. Essa análise será feita por peritos especializados, “é um ato extremamente complexo, considerando a presença de programas de computador cujo objetivo é o mascaramento da verdadeira identidade do autor” (PECK, 2016, p. 16), os computadores estão localizados em locais e redes públicas.

Segundo Corrêa:

> “Os operadores jurídicos, tem que utilizar o bom senso para dirimir questões jurídicas relacionadas à Internet, analisar sempre relacionar a parte técnica com o ordenamento jurídico em exercício. Devendo análises simples e lógicas que possibilitarão um eficaz entendimento das questões cotidianas de nossos tribunais, sendo, principalmente, os bancos acadêmicos os futuros responsáveis pela construção deste, já que é neles que existe uma verdadeira interdisciplinaridade, essencial para a resolução dessas novas questões”.18 (CORRÊA, 2000, p.107)

Contudo, além de ter experiência, o perito precisa se atentar com os dados, porque serão trabalhados com algoritmos, e conforme passa o tempo essas informações se modificam ou são apagadas, o que acaba impedindo a coleta dos materiais para descobrir o autor do fato e do local do crime. É necessário agir com prevenção para que isso não ocorra.

6.2 ENDEREÇO DE IP

O endereço de IP, é uma das primeiras provas que são averiguadas, ele corresponde a um endereço acompanhado de um número identificador. E este endereço recebe uma faixa que pode ser identificada com os padrões que são atribuídos àquele usuário.

“O endereço IP é uma sequência numérica e consistem em um conjunto de quatro grupos de números, separados por pontos, sendo que X corresponde a números que podem variar entre 0 a 255.

Por exemplo, o número 200.142.34.3 é o número IP que identifica o site www.prsp.mpf.gov.br”. (DORIGON; SOARES, 2018)

Com isso, todo crime cometido através da internet, busca-se primeiro identificar o endereço de IP, para que através deste endereço se identifique o autor.

Geralmente, os órgãos públicos, as empresas entre outros segmentos públicos ou privados, utilizam IP estáticos, que são faixas de IP que tem o mesmo padrão e não muda,quanto aos usuários domésticos esses podem se utilizar de IP dinâmicos que se alteram a cada acesso, ou seja, serão sempre modificados, o que dificulta ainda mais na identificação da autoria.

Para saber quem é o provedor de internet do criminoso virtual o endereço de IP é inserido em links que hospedam os sites. E com isso, identifica-se quem fornece o serviço ao criminoso, são solicitadas as informações a respeito dousuário que seria o suposto autor do crime, e também alguns outros dados que podem ser utilizados como provas para o delito.

6.3 INVESTIGAÇÃO POLICIAL

Após a ocorrência do delito, este deve ser apurado através da polícia civil e/ou federal, a investigação é fundamental nos crimes digitais. Os profissionais responsáveis precisam constantemente se atualizarempois os crimes ocorridos no ambiente virtual alteram o *modus operandi* com frequência, por isso todos os profissionais envolvidos devem estar em constante aperfeiçoamento da técnica, a fim de enfrentar os desafios tecnológicos destes tipos de crimes.

Para Jorge:

> “A criminalidade do ciberespaço deve ser combatida com as mesmas armas, ou seja, desfrutando das ferramentas oferecidas pelo próprio ambiente informático na prevenção, investigação, prova e repressão dos crimes virtuais. Para isso, fazem-se necessárias unidades policiais especializadas nestes crimes, assegurando a manutenção da integridade das provas/vestígios ao mesmo tempo em que possibilitaria a adequação dos órgãos policiais à velocidade dos crimes digitais”. (JORGE, 2012, p. 21)

Conforme Alessandro e Renan o “investigador deve observar as peculiaridades que destacam os indícios de tal modalidade delitiva.” (DORIGON, 2018)

As evidências desse crime não tem estabilidade, possuem caráter inconstante e podem ser apagadas, alteradas ou perdidas. Quando o investigador for agir, o aconselhável é que seja cauteloso, para que não ocorra essas adulterações e consiga preservar a prova.

6.4 COMPETÊNCIA

Nos crimes cibernéticos, é difícil definir uma competência, pois, são crimes que podem ocorrem em diversos lugares e também ao mesmo tempo, bem como podem

ser praticados fora do território brasileiro. Na internet tudo ocorre de forma rápida e instantânea.

Para Ferreira:

> É necessário de início, ter em mente que os crimes cibernéticos não causam efeitos apenas no território nacional brasileiro, pois devido ao fato de o meio utilizado para a realização de tais delitos gozar de uma rapidez considerável, poderão tais crimes abarcar também outros territórios, ou seja, poderão afetar outros países. (FERREIRA, 2005, p. 43)

No entendimento de Roque "a competência para julgar ações penais no âmbito da informática deve observar qual o território e a jurisdição sobre a qual o crime se encontra". (ROQUE, 2007, p. 33)

Para Alessandro e Renan, "o maior problema está no fato de ter a rede caráter internacional. Na *internet* não há fronteiras" (DORIGON; SOARES, 2018), ou seja, quando algo é publicado ou compartilhado na internet, ao mesmo tempo já está disponível para o mundo, e não somente naquele local onde foi publicado.

O Código Penal trás dois tipos de crimes, que podem ajudar a entender qual seria a competência dos crimes virtuais, que são os crimes à distância e crimes plurilocais.

Crimes à distância estão definidos no art. 6º do Código Penal: "Art. 6º. Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado".(VADE MECUM SARAIVA, 2018, p. 435)

Em relação aos crimes plurilocais, pode ser utilizado o art. 70 do Código de Processo Penal, onde a competência determina-se pelo lugar onde o crime foi consumado, ou, onde realizou-se a última atuação no caso de tentativa.

Sendo assim, EvandoPassini e como complemento, o artigo 70, do Código de Processo Penal, entende que a regra para determinação da competência é "inegável, portanto, ser a regra, para determinação da competência penal, o foro do local da infração". (CAMARGO,2020)

Esta regra ainda pode ser complementada com o art. 14, inciso I, do Código Penal, que entende-se que, há consumação do crime quando observado que estão reunidos todos os elementos.

Os autores desses crimes, executam suas ações de forma escusa, invadindo a vida íntima, ou lesando o patrimônio de suas vítimas, sendo elas, pessoas físicas ou jurídicas, e muitos desses crimes, ocorrem ainda contra vítimas extremamente vulneráveis, como crianças, sendo o crime ainda mais grave. Portanto, a regra de definição de competência não pode ser um entrave para apuração deste tipo de delito.

7 CONCLUSÃO

O crime digital é muito complexo, por que a dificuldade na obtenção da prova depende de habilidades técnicas da autoridade investigativa, bem como de estrutura dessas autoridades.

Outro desafio está no fato de que a sociedade em geral não tem conhecimentos básicos sobre a forma como ocorrem esses delitos e muita vezes nem sabem da existência deles. Portanto, faz-se necessário, políticas públicas no sentido de conscientizar a população acerca dos delitos ocorridos através da internet, para que assim possam ser mais cautelosos na utilização das redes.

Assim, diante do evidente aumento da criminalidade no meio informático, é muito importante que ocorra um efetivo aparelhamento e treinamento das autoridades responsáveis pela investigação para que possam obter provas e assim gerar a reprimenda adequada aos autores de cibercrimes.

A tecnologia evolui a cada dia e assim também deve ser os órgãos de proteção dos indivíduos e da sociedade, bem como a legislação também deve acompanhar as novas condutas que se apresentam.

REFERÊNCIAS

AGUIAR, M. A. F(2007). **Psicologia aplicada à administração**: teoria, crítica e a questão ética nas organizações. São Paulo: Excellus.

Bom Dia Brasil, B. H. (26 de 09 de 2017). G1. Fonte: Portal G1: https://g1.globo.com/minas-gerais/noticia/ameacas-virtuais-de-revelarintimidades-nas-redes-sociais-crescem-12-em-2017.ghtml.

CAMARGO, EvandoPassini Ferraz. **Determinação da competência penal dos crimes cibernéticos e a criação de vara especializada.** Âmbito Jurídico, [S.I], Mar. 2020. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-processual- penal/determinacao-da-competencia-penal-dos-crimes-ciberneticos-e-a-criacao-de- vara-especializada/>. Acesso em: 08 Out. de 2022.

CASTELLS, Manuel.(1999) **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**; tradução Maria Luiza X. de A. Borges; revisão Paulo Vaz. – Rio de Janeiro: Jorge Zahar Ed.

CASTELLS, Manuel. **A sociedade em rede**. 2. ed. São Paulo: Paz e Terra, 1999.

CRUZ, Diego; RODRIGUES, Juliana: **crimes cibernéticos e a falsa sensação de impunidade.** Disponível em <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em 10 de Setembro de 2022.

DORIGON, A.; SOARES, R. V. O. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova de materialidade**. Jus.com.br, [S.I], Jan. 2018. Disponível em: <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/2>. Acesso em: 07 Out. 2022.

FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimentel**, São Paulo, v. 13, n. 2, p. 35-45, set. 2000.

FERREIRA, I. S. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2. ed. São Paulo: QuartierLatin, 2005.

FRANCHINELLI, A. C., MARCON, C., & MOINET. (05 de 01 de 2006). scielo. Fonte: scielo: http://www.scielo.br/pdf/ci/v34n2/28559.pdf.

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes virtuais. Revista de Doutrina da 4ª Região**, Porto Alegre, n, 55, ago. 2013. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 09 set. 2022.

JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos- Ameaças e procedimentos de investigação**. Rio de Janeiro: Braspot, 2012.

LEMOS, André L. M.(2004) **Estruturas antropológicas do ciberespaço. Textos de Cultura e Comunicação**, Salvador, n. 35, p. 12-27.

MACHADO, Joice megue Ribeiro; (2012) TIJIBOY, Ana Vilma. **Redes Sociais Virtuais: um espaço para efetivação da aprendizagem cooperativ**

MALINI, Fábio. **Modelos de Colaboração nos meios sociais da internet: uma análise a partir dos portais de jornalismo participativo**. In:ANTOUN, Henrique (Org.). Web 2.0: participação e vigilância na era da comunicação distribuída. Rio de Janeiro: Editora Mauad, 2008.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Disponível em: <**http://www.cjf.jus.br/revista/numero20/artigo9.pdf**>.

PECK, Patricia Pinheiro. **Direito digital.** 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. (2010) Direito digital. 4ª ed. São Paulo: Saraiva.

REEDY, J.; SCHULLO, S.; ZIMMERMAN, K. Marketing Eletrônico: **a integração de recursos eletrônicos ao processo de marketing**. Porto Alegre: Bookman, 2001. 7 RNP. (2017).

RNP. Fonte: **Rede Nacional de Pesquisa**: https://www.rnp.br/institucional/quem-somos

ROCHA, Patrícia Gomes. ***Crimes Cibernéticos: uma pesquisa bibliográfica sobre as problemáticas enfrentadas diante dos crimes virtuais*** ConteudoJuridico, Brasilia-DF: 01 set 2022, 04:44. Disponivel em: https://conteudojuridico.com.br/consulta/artigos/59098/crimes-cibernticos-uma-pesquisa-bibliogrfica-sobre-as-problemticas-enfrentadas-diante-dos-crimes-virtuais. Acesso em: 10 set 2022.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos Acesso em: 09 set. 2022.

SEGUNDO, ronaldocassiano de oliveira. *Crimes virtuais contra a honra e meios de prova* ConteudoJuridico, Brasilia-DF: 22 nov 2021, 04:10. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/57539/crimes-virtuais-contra-a-honra-e-meios-de-prova. Acesso em: 16 set 2022.

Vademecum Saraiva / obra coletiva de autoria da Editora Saraiva com a colaboração de Lívia Céspedes e Fabiana Dias da Rocha. – 25. ed. atual. e ampl. – São Paulo: Saraiva Educação, 2018.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**. Rio de Janeiro: Forense, 2003.

WOLTON, D. (2003) **Internet, e depois?** Porto Alegre: Sulina.