

# **AS DIFICULDADES DE SE IDENTIFICAR CRIMES CIBERNÉTICOS E SUA POSSÍVEL AUTORIA.**

THE DIFFICULTIES OF IDENTIFYING CYBERNETIC CRIMES AND ITS POSSIBLE AUTHORSHIP.

**Rodolfo Eduardo Padovani<sup>1</sup>**

**Paula Fernandes Canedo Teixeira<sup>2</sup>**

## **RESUMO**

O presente trabalho discorre sobre as barreiras que as autoridades encontram para apurar um crime cibernético, desde a identificação do crime, a colheita de provas e quem é competente para julgar crimes dessa natureza. Tem por objetivo demonstrar a história da internet no Brasil, bem como o desenvolvimento tecnológico no decorrer do tempo, analisando alguns crimes que são praticados pela internet, a definição da autoria, colheita de provas e qual é a justiça competente para julgar o caso concreto. Para isso, utilizou-se de pesquisas doutrinárias, artigos postos na internet sobre o tema e jurisprudência que possibilitam o esclarecimento de dúvidas sobre o tema posto, tendo como principais resultados deste artigo, a necessidade de leis que funcionem de forma concreta e que puna de maneira efetiva o agente que pratica o cibercrime.

Palavras – chave: Internet. Crimes. Autor. Provas. Competência.

## **ABSTRACT**

This paper discusses the barriers that the authorities encounter in detecting a cyber crime, since the identification of the crime, the gathering of evidence and who is competent to try crimes of this nature. It aims to demonstrate the history of the Internet in Brazil, as well as technological development over time, analyzing some crimes that are practiced by the internet, the definition of authorship, evidence gathering and which is the competent justice to judge the concrete case. For that, we used doctrinal research, internet articles on the subject and jurisprudence that make it possible to clarify doubts about the topic, having as main results of this article, the need for laws that work in a concrete way and that puna effective way the agent that practices cybercrime.

Keywords: Internet. Crimes. Author. Evidences. Competence.

---

1. Aluno do Curso de Pós Graduação do Comando da Academia de Polícia Militar de Goiás - CAPM, padovaniadv@gmail.com, Goiânia-GO, Junho de 2018.

2. Professora Orientadora: Professora do Programa de Pós-Graduação e Extensão do Comando da Academia da Polícia Militar de Goiás - CAPM, paulapft@hotmail.com, Goiânia-GO, Junho de 2018.

## INTRODUÇÃO

Este artigo visa analisar quais são as dificuldades encontradas para identificar o crime cibernético e a possível autor. Diante das inúmeras possibilidades do uso malicioso da internet para o cometimento de crime, aflorou o interesse em discorrer sobre este tema, haja vista ser a internet um meio de comunicação amplo, de fácil acesso e que requer cuidados, para que o cidadão de bem não se torne vítima desses criminosos que usam um dos meios de comunicação mais utilizados no mundo para praticar crime.

Objetiva-se com esse artigo, analisar o surgimento da internet no Brasil, com enfoque no desenvolvimento e na evolução tecnológica no decorrer do tempo. Visa examinar os crimes mais comuns praticados utilizando a internet, a autoria, as possíveis provas a serem produzidas bem como a competência para julgar os crimes cibernéticos.

Para tanto, a abordagem metodológica utilizada para a construção desse trabalho foi pesquisas em livros, artigos postos na internet sobre o tema e jurisprudências que possibilitam o esclarecimento de dúvidas pertinentes das pessoas que navegam nesse mundo virtual e que não sabem o potencial perigo que se encontram ao navegar de forma inadequada.

Tendo por base a descrição do tema posto, pretende-se realizar uma abordagem legal, doutrinária, visando demonstrar a problemática que envolve a dificuldade de se identificar a autoria e a materialidade do crime, como também determinar o juízo competente para o julgamento desses delitos.

A confecção deste artigo é de suma importância para colaborar com o órgão de inteligência da Polícia Militar do Estado de Goiás, tendo em vista ser este órgão que colabora com outros órgãos da Segurança Pública do Estado de Goiás na investigação de crimes, bem como para a população goiana ter ciência dos riscos em se navegar na rede mundial de computadores sem a devida cautela.

Portanto, este artigo aborda as barreiras encontradas para identificar as pessoas que utilizam a internet para cometer crimes. Conceitua o que é a internet, analisa os crimes cibernéticos mais comuns, bem como discute a colheita de provas e qual é o órgão competente para investigar, processar e julgar os cybers crimes, sob o ponto de vista de grandes pensadores da doutrina penal brasileira.

## Revisão Literária

### 1.1 A história da Internet no Brasil

A internet, na definição de Marco Antônio Zanellato, é “um suporte ou meio que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”. É um sistema mundial de rede de computadores que interligam entre si, utilizando um conjunto de protocolos (IP ou TCP/IP).

A Lei 12.965/2014, que trata do marco civil na internet, em seu artigo 5º, inciso I, conceitua internet como sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

A internet no Brasil surgiu em meados dos anos de 1988 e primeiramente ligava algumas instituições de ensino do país a instituições nos Estados Unidos. O Instituto Brasileiro de Análises Sociais (Ibase) e Econômicas no mesmo ano começou a testar o primeiro serviço de internet não acadêmica e não governamental, que se denominou AlterNex. Inicialmente o serviço somente era utilizado de forma restrita pelo Instituto Brasileiro de Análises Sociais e Econômicas e pelos membros associados, tendo se tornada pública a partir de 1992.

A internet nos dias de hoje, é um dos meios de comunicação mais utilizados entre as pessoas, tanto por pessoas físicas, como pelas pessoas jurídicas, cada uma realizando diferentes tarefas e serviços disponíveis, algumas a utilizam para navegar com fins de realizar pesquisas escolares, outras para realizar operações financeiras, enfim, há inúmeros modos de utilização que não elencamos aqui.

Para trocar alguma informação pela internet é necessário uma identificação, chamado de endereço lógico ou IP, é análogo ao Registro Geral de uma pessoa, pois é através do IP que se identificará o computador ligado a internet.

A Lei 12.965/2014 traz também o conceito de IP no artigo 5º, inciso III, o definindo como código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais. Sendo assim, para se identificar um computador que está ligado a rede mundial de computadores, internet, basta rastrear o seu endereço lógico ou IP que se terá a localização exata de onde partiu a mensagem.

Gabriel Zaccaria (2009) fala que existem duas categorias de computadores segundo a sua função, os computadores clientes e os computadores

servidores. O computador servidor utiliza programas para providenciar o acesso a rede; já o computador cliente, é o que faz o acesso ao serviço disponibilizado pelo servidor. Nada obsta que um computador desempenhe a duas funções ao mesmo tempo.

Outrossim, cumpre salientar que todas as comunicações realizadas através da internet, são feitas de forma indireta, haja vista, que são feitas tendo como intermediário seus servidores e provedores.

Geralmente, os criminosos que utilizam a internet como meio de praticar os crimes cibernéticos, utilizam-se de várias técnicas. a técnica mais conhecida e utilizada pelos criminosos para praticar os crimes cibernéticos é o Vírus, um *software* que tem a capacidade de destruir ou modificar os dados do computador infectado. Os vírus ao se proliferarem dentro do computador infectado podem invadir outro computador, bastando que se utilize um *pen drive* no computador infectado e posteriormente usa-lo em outro computador sem proteção que, dessa forma, não está a salvo do vírus.

O mais conhecido dos vírus entre os internautas que navegam pela Rede é o *Trojan Horse* ou Cavalo de Tróia, em que sua principal função é controlar integralmente o sistema do computador infectado, dando a possibilidade a quem envia esse tipo de vírus de ler arquivos, alterá-los e até mesmo de excluí-los.

Com tanta variedade de técnicas que são utilizadas pelos criminosos é necessário termos cautela ao se navegar pela internet, nos prevenindo de eventuais vírus invasores que podem danificar o sistema do computador, com um antivírus. Sendo que, uma vez infectado o sistema o computador por um vírus, tem-se a brecha para que possamos ser uma possível vítima daqueles que praticam crimes cibernéticos, sofrendo violação de informações sigilosas ou outros arquivos vulneráveis

## **1.2 DOS CRIMES PRATICADOS PELA INTERNET**

### **1.2.1 Do Estelionato**

O artigo 171, *caput*, do Código Penal, prevê a conduta classificada como crime de estelionato. O bem juridicamente tutelado pelo crime de estelionato é o patrimônio. Segundo Rogério Sanches (Parte Especial 2016), tem proteção à inviolabilidade patrimonial, “tutela-se com a incriminação do estelionato a inviolabilidade patrimonial, aviltada pela prática de atos enganosos pelo agente”.

Qualquer pessoa poderá ser sujeito ativo do crime, da mesma forma, qualquer pessoa poderá ser sujeito passivo do crime, haja vista que qualquer pessoa que venha a sofrer lesão patrimonial ou que se sujeitou a uma ação fraudulenta realizada pelo agente, será vítima do crime. Ressalta-se que o prejuízo econômico nem sempre incide sobre a pessoa que sofre o engano.

É pacificada a jurisprudência do Supremo Tribunal Federal, em que pese o sentido do sujeito passivo no crime em estudo, ser a pessoa que foi enganada, como também a pessoa que foi prejudicada, não dando importância que a pessoa seja um ente federado.

Nas palavras de Rogério Sanches, o artigo em estudo visa punir a conduta do sujeito ativo que age através da esperteza, da falsidade, para retirar sem violência, da vítima, parte de seu patrimônio que lhe foi entregue de modo voluntário pelo sujeito passivo, veja-se:

“Pune-se aquele que, por meio da astúcia, do engodo, da mentira, procura despojar a vítima do seu patrimônio fazendo com que esta entregue a coisa visada espontaneamente, evitando-se assim, retirá-lo por meio violento. Em suma o agente busca lesar a vítima em seu patrimônio, de maneira sutil, mas sempre segura”. (CUNHA, Parte Especial 2016, pág. 341).

Para a conduta ser tipificada como crime de estelionato, faz se indispensável preencher três elementos, a fraude, a vantagem ilícita e o prejuízo alheio.

O elemento subjetivo do tipo penal em estudo é o dolo de induzir ou manter alguém a erro, com o fim de obter para si ou para outrem vantagem indevida. Deve-se envolver não somente o ato de induzir ou manter a vítima em erro, como também outro meio fraudulento capaz de ludibriar a vítima, a vantagem ilícita e o prejuízo alheio. Leciona Rogério Sanches:

“Consiste no dolo de induzir ou manter alguém em erro a fim de obter indevida vantagem, para si ou para outrem. O dolo deve abranger não só o ato de indução ou manutenção da vítima ao equivoco, como também o meio fraudulento empregado, a vantagem ilícita a ser obtida e o prejuízo alheio”. (CUNHA, Parte Especial 2016, pág. 345)

O Código Penal no artigo 171, parágrafo terceiro, traz uma majorante aumentando a pena de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de ordem economia, popular assistência social ou beneficência.

Rogério Sanches cita em sua obra a definição de entidade de direito público, de instituto de economia popular, de assistência social ou beneficência dada por Nelson Hungria:

“Entidade de direito público é a que integra a organização administrativa do Estado ou gravita na órbita dessa organização (União, Estados federados, Distrito Federal, Territórios Municípios, Autarquias ou entidades paraestatais; Instituto de Economia popular é todo aquele que serve a direito de interesse econômico do povo ou indeterminado número de pessoas (bancos populares, cooperativas, caixa Raiffeisen, sociedade de mutualismo etc.). Instituto de assistência social ou beneficência é a que atende a fins de filantropia, de solidariedade humana, de caridade, de altruístico socorro aos necessitados em geral, de desinteressado melhoramento social ou educacional.” (CUNHA, Parte Especial 2016, pág. 354)

Aumenta-se a pena em razão de que nesse crime a lesão provocada pela conduta do agente é o patrimônio da coletividade.

Em 2015 foi publicada a Lei 13.228 que trouxe outra majorante ao crime de estelionato, essa lei dobra a pena do crime de estelionato, caso seja praticado contra pessoa com idade igual ou superior a sessenta anos. Com essa alteração no Código Penal, o legislador quis dar a punição proporcional e adequada quanto à reprovação social da ação.

Sendo assim, há possibilidade da prática do crime de estelionato ser realizado via internet, de modo pelo qual o criminoso utilizará de meios para induzir ou manter a vítima em erro, obtendo para si ou para outrem vantagem ilícita, como por exemplo, através de fraude, em que o agente cria uma falsa página de internet ou um link falso, dando ao sujeito passivo uma falsa percepção da realidade.

Destaca Gabriel Cesar Zaccaria de Inellas:

“Nesse caso, a conduta do agente ativo consiste no emprego do meio informático, para induzir ou manter a vítima em erro, obtendo com isso vantagem ilícita, para si ou para outrem. Tais condutas são denominadas fraudes eletrônicas. Nesse caso, a conduta utilizada é a de levar a vítima a erro, mediante ardil. Ardil é o engano praticado por intermédio de insídia. Os outros meio executórios, para enganar a vítima, induzindo-a ou mantendo-a em erro, podem ser o artifício ou qualquer outro meio fraudulento. Artifício é o engodo empregado por meio de aparato matéria, encenação. Por fim, o legislador previu, como meio executório qualquer outro meio fraudulento. Assim, qualquer espécie de fraude configura o delito”. (INELLAS, 2009, pág. 65)

A maneira mais utilizada por quem comete esse tipo de crime é o usuário da internet (vítima) acessar indevidamente correio eletrônico em seu computador, especialmente aqueles que verificam saldos bancário, através da internet. Nesses

casos, os criminosos copiam os dados de cartões e senhas das vítimas e ingressam no sistema bancário do usuário e, utilizando destas senhas e dos números dos cartões copiados, fazem transferências de valores da conta da vítima para sua conta ou compras pela internet, por exemplo.

Há inúmeras jurisprudências de Tribunais Superiores analisando o crime de estelionato praticados via internet, em uma delas o Tribunal Regional Federal analisou o crime no qual o criminoso utilizou de dados de cartão de crédito para fazer comprar pela internet:

PENAL. PROCESSUAL PENAL. ESTELIONATO. UTILIZAÇÃO DE DADOS DE CARTÕES DE CRÉDITOS DE TERCEIROS PARA AQUISIÇÃO FRAUDULENTE DE MERCADORIAS. (CP, ART. 171, § 3º) CONTINUIDADE DELITIVA. FORMAÇÃO DE QUADRILHA (CP, ART. 288). ASSOCIAÇÃO ESTÁVEL E PERMANENTE DE AGENTES PARA A PRÁTICA DE INDETERMINADO NÚMERO DE CRIMES. CONFIGURAÇÃO. CORRUPÇÃO DE MENORES. ART. 244-B, CAPUT, DA LEI N. 8.069/90. AUTORIA E MATERIALIDADE DELITIVAS DEMONSTRADAS. PRELIMINARES DE NULIDADE DA PROVA PRODUZIDA. REJEIÇÃO. 1. Rejeição das preliminares de ilicitude da prova produzida. 2. Materialidade e autoria dos delitos de estelionato ficaram demonstradas pelo conjunto probatório que revela haverem os acusados efetuado inúmeras compras, via internet, mediante a utilização de dados de cartões de créditos de terceiros, obtendo vantagem ilícita em prejuízo da Caixa Econômica Federal e de outras administradoras de cartões de crédito. 3. De igual forma, encontra-se provada a materialidade e autoria dos crimes de formação de quadrilha ou bando e de corrupção de menores. 4. Se a quadrilha foi constituída justamente para a prática de diversos crimes de estelionato em continuidade delitiva, a prática destes crimes não exclui a imputação pela prática do crime de quadrilha, que são autônomos entre si. 5. No que se refere à dosimetria, não merece censura a sentença, que, ao fixar as penas, indica objetivamente os motivos e fundamentos pertinentes. 6. Apelações improvidas. (TRF-1 - ACR: 00435735920104013400, Relator: JUIZ FEDERAL PABLO ZUNIGA DOURADO (CONV.), Data de Julgamento: 03/02/2015, QUARTA TURMA, Data de Publicação: 27/02/2015)

Contudo, é possível encontrar sites navegando pela internet que tentam combater esse tipo de crime que utiliza a internet como meio para lesar o patrimônio da vítima. Tem por objetivo passar informações ao usuário de quão é perigoso o uso negligente da internet ao acessar contas bancárias, e-mails desconhecidos, bem como dá suporte para as pessoas que foram vítimas desse tipo de crime fazer denúncias, como o intuito de ajudar a polícia a capturar os criminosos.

### **1.2.2 Da Pornografia infantil**

O crime de pornografia infantil há de ser considerado o mais comum e mais praticado pela internet. Existem inúmeros esforços da mídia mundial para

influenciar as autoridades do mundo inteiro a criar normas com medidas rígidas e efetivas para quem comete esse crime que tende a ser cruel.

Entretanto, são cometidos alguns equívocos pela mídia ao tratar como sinônimo, pedofilia e pornografia infantil. Pornografia infantil pode ser conceituada como qualquer representação, independente do meio de veiculação, de uma criança ou adolescente envolvida em atividades sexuais explícitas, reais ou simulada, ou qualquer reprodução dos órgãos sexuais de uma criança com o objetivo principalmente de cunho sexual. Já a pedofilia diz respeito aos transtornos de personalidade causados pela preferência sexual por crianças e adolescentes.

O artigo 234 do Código Penal envolve os dois conceitos. Nesse crime o bem juridicamente tutelado é o pudor público, haja vista que a divulgação do material com conteúdo obsceno que ofende a moral da coletividade.

Não se exige do sujeito ativo, qualquer condição especial para a prática desse crime, logo, pode ser praticado por qualquer pessoa. Já quanto ao sujeito passivo, além da pessoa que teve contato direto com o material divulgado, seja pelo escrito ou objeto obsceno, também será sujeito passivo toda a coletividade.

É necessário para que se configure o crime previsto no artigo 234 do Código Penal, que o agente pratique qualquer uma das condutas descritas no tipo penal, que tenha por finalidade o comércio, a distribuição ou exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno. Ensina Rogério Sanches:

“consiste o crime em fazer (produzir criar), importar (fazer ingressa no país), exportar (fazer com que saia do país), adquirir (obter título gratuito ou oneroso) ou ter sob sua guarda (reservar o material), para fins de comércio, de distribuição ou exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto”. (CUNHA, Parte Especial 2016, pág. 515)

Constitui elemento subjetivo do tipo penal, o dolo, a vontade livre e consciente de fazer, importar, exportar, adquirir ou ter sob sua guarda, escrito desenho, pintura, estampa ou qualquer objeto obsceno. Primordial para a configuração do crime, a presença de dois elementos subjetivos, como bem doutrina Rogério Sanches, a finalidade de comercio, de distribuição ou de exposição pública, e também, o propósito de ofender a moralidade pública.

Impreterível destacar que as condutas previstas tanto no *caput*, como no parágrafo único do artigo em estudo, for praticada contra criança ou adolescente, será aplicado não a regra prevista no Código Penal, mas sim as normas previstas dos artigos 240 a 241-E do Estatuto da Criança e do Adolescente, por força do

princípio da especialidade. Esse princípio resolve um conflito aparente de normas penais, e deve ser compreendido como capaz de afastar a lei geral para a aplicação da lei especial, haja vista a esta norma engloba todos os elementos da lei geral acrescido de elementos particulares.

O artigo 240 do Estatuto da Criança e do Adolescente visa tutelar a integridade moral da criança e do adolescente. No presente caso, o sujeito ativo do crime será qualquer pessoa que pratique as condutas previstas no *caput* ou no parágrafo primeiro do artigo 240 do Estatuto da Criança e do Adolescente. O sujeito passivo do crime, sempre será a criança ou o adolescente envolvido.

Não é necessário para configurar o crime que o agente pratique todas as condutas que foram definidas, mas basta praticar uma que restará caracterizado o ilícito previsto, tendo em vista que o artigo em estudo é um crime de ação múltipla, no qual dispõe de vários núcleos do tipo necessitando a prática da conduta de um ou mais núcleos, porém será punida somente uma das condutas por força do princípio da alternatividade.

O Estatuto da Criança e do Adolescente, também se preocupou em proibir a pornografia infantil que utiliza a internet como meio de propagação no artigo 241-A e seguintes.

Sendo assim, aquele que veicula imagens ou ilustrações que contenhas cena de sexo explícito ou pornografia envolvendo criança ou adolescente, está praticando o crime previsto do artigo supracitado.

Não é nada incomum encontrar algumas dessas condutas quando se navega pela internet em sites de cunho pornográfico. Ao visitar esses sites que estão hospedados na internet, verifica-se que existem várias condutas que se enquadram nas dos núcleos do tipo penal em estudo, em que disponibilizam ou publicam conteúdos pornográficos ou cenas de sexo explícito envolvendo criança ou adolescente.

Gabriel Zaccaria (2009) descreve que desde o ano de 1998 o Supremo Tribunal Federal, afirma que o artigo 241-A do Estatuto da Criança e do Adolescente se aplica aos atos praticados pela internet que envolvam cenas de sexo explícito ou pornografia envolvendo criança ou adolescente, haja vista que o referido artigo é norma penal aberta, configurando o crime pela singela publicação do conteúdo pornográfico, independentemente do meio utilizado para disseminação do conteúdo.

Em que pese existir legislações que visam coibir a prática o crime de pornografia infantil pela internet, existe uma facilidade imensa para que tal crime

ocorra, em razão do procedimento simplificado para se publicar e ter acessos a esse tipo de conteúdo.

Resta configurado o crime em apreço, mesmo que essas publicações não recebam nenhum acesso, levando em consideração que foi realizada a conduta descrita no tipo, publicar e o meio de informática pelo qual se publicou o conteúdo.

Carlos Alberto Di Franco em seu artigo publicado na internet, Internet e Pornografia, propôs algumas soluções para reduzir a ocorrência desse tipo de crime, bem como aplicar penas mais rigorosas que a atualmente prevista, veja-se:

“Algumas medidas, no entanto, podem ser adotadas. Quando identificados, os responsáveis pela divulgação de pornografia infantil, racismo ou incitamento ao ódio, devem ser rigorosamente punidos. A censura prévia, indesejável e tecnicamente inviável, não elimina o necessário enquadramento do criminoso comprovado. Pode-se, também, estimular mecanismos de autorregulamentação. Associações de provedores, à semelhança do que ocorre na área da publicidade, com o Conar, poderiam definir um código de ética, conferir selos de qualidade para quem assumisse o compromisso de não difundir material imoral ou antissocial, publicar listas negras com nomes indesejáveis no ciberespaço”.

Enquanto a impunidade dos autores que pratica esse crime com alto índice de reprovabilidade por maioria da sociedade continuará, há de se ver em circulação na internet, imagens contendo cenas de sexo explícito ou de conteúdo pornográficos envolvendo criança e adolescente que por vezes nos deixam desestabilizados.

## **1.3 As Dificuldades de se Identificar Crimes pela Internet**

### **1.3.1 Da Autoria**

Quando a internet se torna meio para práticas de crime, surgem vários obstáculos para apurar a autoria, para a colheita de provas concretas da materialidade delitiva, bem como de saber a quem compete processar e julgar o crime.

Entretanto, para fins de se apurar a autoria de um determinado crime, deve-se observar as teorias existentes que envolvem o conceito de autor, haja vista que o Código Penal, não diferenciou autor de partícipe.

A doutrina brasileira é majoritária em entender que são várias as teorias que explicam a autoria de um crime. São elencadas cinco correntes que discorrem sobre a autoria de um crime. A teoria unitária, teoria extensiva, teoria do domínio teoria objetiva ou dualista. O Brasil, de acordo com a doutrina majoritária, adotou a

teoria objetiva, utilizando-se do critério objetivo-formal, ao prevê no artigo 29 do Código Penal, “quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade”. Logo, percebe-se que, é possível distinguir o autor (imediato), do partícipe, do autor mediato.

A teoria objetiva ou dualista estabelece a diferença entre autor e partícipe, e têm dois desdobramentos, a teoria objetiva que se utiliza do critério objetivo-formal e outra com critério objetivo-material, segundo Rogério Sanches.

Para a teoria objetiva, quando se utiliza do critério objetivo-formal, autor do crime é aquele que pratica a conduta descrita no tipo penal, já a figura do partícipe, é definida por aquele que contribui de qualquer maneira para que se cometa o crime.

Utilizando-se do critério objetivo-material, autor do crime, pela teoria objetiva, será aquele que de forma objetiva e mais eficiente para que seja produzido o resultado, independentemente da prática do núcleo do tipo. Partícipe é considerado aquele que de forma menos expressiva contribuiu para que fosse alcançado o resultado, mesmo que para isso, tenha praticado qualquer conduta descrita no núcleo do tipo. Ensina Rogério Sanches:

“(C) Teoria objetiva ou dualista: estabelece clara distinção entre autor e partícipe. A teoria objetiva pode ser subdividida em duas: (C.1) Objetivo-formal: autor é quem realiza a ação nuclear típica e partícipe quem concorre de qualquer forma para o crime. (C.2) Objetivo-material: autor é quem contribui objetivamente de forma mais efetiva para a ocorrência do resultado, não necessariamente praticando a ação nuclear típica. Partícipe, por outro lado, é o concorrente menos relevante para o desdobramento causal, ainda que sua conduta consista na realização do núcleo do tipo. (CUNHA, Parte Geral 2016, pág. 372)

Corriqueiramente, quem utiliza a internet como meio para práticas de crimes, adota uma identificação que não corresponde com a verdadeira, valendo-se de dados falsos, sendo esse um dos motivos determinantes que dificultam o trabalho policial de identificar quem realmente é o criminoso. Por isso, é de suma importância a participação das Provedoras de Acesso a internet, em que pese fornecer dados para elucidar a autoria do crime.

Sendo que ao IP é a identificação do usuário que acessa a internet, as provedoras de acessos podem atuar de forma a fornecer essa identidade quando

solicitado por autoridade judicial de maneira mais rápida. Haja vista que o IP se compõe de códigos numéricos que necessitam ser traduzido para descobrir de onde o crime foi praticado.

Por isso, conseguir determinar a autoria do crime cibernético, demanda técnicas eficientes, em razão de o agente utilizar dados falsos, que pode remeter a um endereço que se encontre em outro país, onde as leis brasileiras podem ser inaplicáveis.

### **1.3.2 Da Prova**

A apuração dos crimes praticados pela internet encontra-se outra barreira no que diz respeito à busca de indícios suficientes de prova da materialidade do crime.

Deve ser observado quando da colheita de provas, a teoria da prova, adotada pelo ordenamento jurídico brasileiro. O que se pretende é chegar à verdade real dos fatos, sendo que para isso, deverão ser reconstruídos os fatos em investigação, da maneira quase idêntica a real história.

Com isso, é perceptível que a produção da prova é bastante complexa, exigindo de quem compete colhe-las, observar uma série de regras e princípios previstos na Constituição Federal, como as garantias e direitos individuais, do acusado e de terceiros, tutelados pela inadmissibilidade das provas ilícitas. Leciona Eugênio Pacelli:

“Para a consecução de tão gigantesca tarefa, são disponibilizados meios ou métodos de prova, com os quais (e mediante os quais) se espera chegar o mais próximo da realidade dos fatos investigados, submetidos, porém, a um limite previamente definido na Constituição Federal: o respeito aos direitos e às garantias individuais, do acusado e de terceiros, protegidos pelo imenso manto da *inadmissibilidade das provas obtidas ilicitamente*.” (PACELLI, Curso de Processo Penal 2015, pág. 328)

Assim, abrange os direitos e garantias individuais, por exemplo, o princípio da ampla defesa e do contraditório e o princípio da identidade física do juiz.

Nos termos do artigo 5º, inciso LVI da Constituição Federal, prevê o princípio da inadmissibilidade das provas ilícitas, ao dizer “são inadmissíveis, no processo, as provas obtidas por meios ilícitos. Princípio assegurado também no

Código de Processo Penal, no artigo 157, com redação idêntica ao artigo supracitado.

A finalidade desse princípio é inibir a autoridade competente pela investigação, funcionando como controle de regular atuação estatal na persecução penal, de práticas ilegais no momento da colheita da prova, por exemplo, que se obtenha confissão subtraindo o acusado a tortura.

Essa vedação de provas ilícitas, também não pode deixar de ser observada, em relação aos efeitos produzidos, aos resultados angariados por essa prova produzida na ilegalidade. Para ilustrar, a interceptação de dados, poderá ser ou não lícita, tendo em vista que se autorizada judicialmente importará na licitude da prova.

Entretanto, a prova obtida através de interceptação de dados sem a devida autorização judicial, será considerada ilícita, por lhe faltar amparo na lei. Diante dessa situação, o resultado da prova é ilegal por afrontar a um dos requisitos de validade da prova. O artigo 157 do Código de Processo Penal determina que, a prova que foi obtida de maneira ilícita deverá ser desentranhada dos autos do processo, ou seja, a prova não irá mais estar nos autos e não poderá ser usada como suporte para uma eventual condenação.

Importante ressaltar, que por força do princípio da ampla defesa, o princípio da inadmissibilidade de prova ilícita, comporta uma única exceção, haja vista que aquele princípio permite ao acusado utilizar a prova obtida a margem da lei em seu benefício. Nesse caso, deve ser observado também o princípio da razoabilidade, por existirem duas garantias em conflitos, de um lado a inadmissibilidade da prova ilícita e do outro a presunção de não culpabilidade. Ensina Eugênio Pacelli:

“E por fim, é de se registrar mais uma vez, que a ampla defesa autoriza até mesmo o ingresso de provas obtidas ilicitamente, desde que, é claro, favoráveis a defesa. E nem poderia ser de outro modo. Primeiro, porque, quando a obtenção da prova é feita pelo próprio interessado (o acusado), ou mesmo por outra pessoa que tenha conhecimento da situação de necessidade, o caso será de exclusão da ilicitude, presente, pois umas das causas de justificação: estado de necessidade. Mas mesmo quando a prova foi obtida por terceiros sem o conhecimento da necessidade, ou mesmo sem a existência da necessidade (porque ainda não iniciada a persecução penal, por exemplo), ela poderá ser validamente aproveitada no processo, em favor do acusado, ainda que ilícita sua obtenção. E assim é porque o

seu não aproveitamento, fundado na ilicitude, ou seja, com a finalidade de proteção do *direito*, constituiria um insuportável paradoxo: a condenação de quem se sabe e se julga inocente, pela qualidade probatória da prova obtida ilicitamente, seria, sob quaisquer aspectos, uma violação abominável ao *Direito*, ainda que justificada pela finalidade originária de sua proteção (do Direito).” (PACELLI, Curso de Processo Penal 2015, pág. 330)

Em decorrência do princípio da inadmissibilidade de prova ilícita, deve-se observar a teoria dos frutos da árvore envenenada, prevista no artigo 157 do Código de Processo Penal. Por esta teoria, a nova prova colhida de forma lícita, decorrente de uma prova que foi obtida de maneira ilegal também será considerada ilícita, por derivação.

O artigo 157, § 1º, do Código de Processo Penal, traz exceção em relação a esta teoria, ao possibilitar a utilização da prova ilícita derivada, quando não se evidencia o nexo de causalidade entre umas e outras, ou quando as provas derivadas puderem ser obtidas por uma fonte independente da primeira. O § 2º, considera fonte independente, aquela que por si só, em que se seguem os trâmites típicos e de praxe, próprios de investigação ou instrução criminal, seria capaz de produzir o objeto da prova.

O meio de prova mais utilizado pelas autoridades policiais para apurar o crime praticado pela internet é a interceptação de dados, previsto na Constituição Federal e regulada pela Lei 9.296/96. O artigo 1º, parágrafo único da Lei 9.296/96, é claro ao dizer que a referida lei se aplica aos casos que serão necessários a realização de interceptações do fluxo de comunicação em sistema de informática e telemática.

Entretanto, para que seja possível interceptar essas comunicações, é necessária ordem judicial devidamente fundamentada pelo magistrado, desde que, a finalidade seja para a instrução criminal ou em instrução processual penal e que interceptação seja indispensável para a colheita da prova, esteja presente indícios razoáveis de autoria ou participação e o crime que está sendo investigado ser punido com pena de reclusão.

Apesar do artigo 5º inciso XII da Constituição Federal, não mencionar o sigilo das informações informáticas e telemáticas, é pacificado na doutrina e jurisprudência, ser constitucional o parágrafo único do artigo 1º da Lei 9296/96. Doutrina Eugênio Pacelli:

“A possibilidade de autorização judicial também para interceptação do fluxo de comunicações em sistema de informática e telemática, como ali previsto, é perfeitamente constitucional, e vem completar o rol de proteção do inc. XII do art. 5º da CF, estabelecendo que, em todas as hipóteses ali mencionadas, a quebra de sigilo exigirá autorização judicial fundamentada.” (PACELLI, Curso de Processo Penal 2015, pág. 355)

Necessário também para se apurar o crime cometido através da internet, que seja realizada a perícia do material apreendido com o criminoso, ou seja, proceder com o exame de corpo de delito.

O referido exame deverá ser realizado de forma cuidadosa, desde a busca e apreensão, realizada com o devido mandado judicial, até a análise dos dados coletados. Ao cumprir o mandado de busca e apreensão na residência do acusado, é de suma importância que se apreenda todo e qualquer dispositivo capaz de armazenar dados, bem como prezar pelo zelo, para que não ocorra nenhum dano nos dispositivos de armazenamento.

As provas colhidas, que estão armazenadas no computador do criminoso ou em outro aparelho que possibilita o armazenamento de dados, sempre serão reproduzidas para ser periciadas, com o objetivo de preservar a prova original até o fim do processo, caso surja eventual dúvida, possa ser reexaminada a prova. Gabriel Zaccaria:

“Mas porque os exames devem ser realizados em uma cópia e não na mídia original? Além da preservação da prova, decorre da necessidade de se estabelecer o que se chama na Computação Forense de *timeline* ou linha do tempo, que é uma cronologia de eventos relacionados ao caso em avaliação. Os arquivos possuem características que permitem identificar sua data de criação, última alteração e último acesso, conhecidos como *metadados*. O simples fato de abrir-mos um arquivo de computador altera o seu estado, que pode ser desde a data do último acesso, como informações relativas à máquina em que ele foi trabalhado” (INELLAS, *apud* COSTA, 2009, p.146)

Nota-se que tem grande relevância à cronologia do crime praticado pela internet, haja vista, a possibilidade de se verificar todo o desenvolvimento do caso investigado, de forma a comprovar a organização do crime, bem como o procedimento para cometer a conduta criminosa.

### 1.3.3 Da Competência

Competência pode ser definida como o limite jurisdição. Na doutrina de Eugênio Pacelli, ensina que a jurisdição é una, no sentido de se tratar de intervenção do Estado junto aos jurisdicionados, para fins de atuação do Direito ao caso concreto.

O Código Penal, em seu artigo 5º, adotou para fins de aplicação da lei penal, o princípio da territorialidade, pelo qual, será aplicada a lei penal brasileira aos crimes cometidos no território nacional, sem prejuízo de convenções, tratados e regras de direito internacional.

Dessa maneira, em razão do princípio da territorialidade, a lei penal brasileira somente terá vigência dentro dos limites onde o Estado brasileiro seja soberano.

O problema que se encontra nos crimes praticados pela internet relaciona-se com a possibilidade do crime ser iniciado em um lugar e o resultado se dar em outro, resta saber se os locais diferentes se localizam no mesmo país ou em países diversos. Ensina Gabriel Zaccaria:

“acontece que, via de regra, nos crimes cometidos pela *Internet*, o *iter criminis*, se desenrola em lugares diferentes. Surge aí o grande problema da competência. Primeiramente, urge saber se os lugares diferentes, encontram-se no mesmo País ou em outro País. Os crimes que se desenvolvem em diferentes lugares, dentro do nosso território, denominam-se delitos *plurilocais*; os delitos que se desenvolvem em Países diferentes, são chamados de *crimes à distancia*.” (INELLAS, 2009, p.121)

Para se determinar a competência de um órgão jurisdicional, devem ser considerados alguns critérios definidos na Constituição Federal, bem como nas leis infraconstitucionais, que são os critérios em razão da matéria (*ratione materiae*), funcional (*ratione personae*) e a territorial.

Em regra, o Código de Processo Penal, estabelece no artigo 70, que a competência será estabelecida pelo lugar em que se consumar a infração, e caso seja praticada na modalidade tentada, a competência será o juízo do lugar onde foi praticado o último ato de execução, assim, o Código de Processo Penal, adotou a teoria do resultado para definir a competência pelo lugar da infração.

Alcançando os atos de execução países diversos, estaremos diante de crimes à distância. Diante dessa situação, o Código de Processo Penal, no §1º, artigo 70, define que caso seja iniciada a execução do crime no Brasil, e o delito se consumir em outro país, competente será aquele juízo do lugar onde tiver sido praticado, no Brasil, o ultimo ato de execução. Já o §2º do referido artigo, define competente o juízo do lugar onde o crime, mesmo que de forma parcial, produziu o deveria produzir o resultado, no caso do ultimo ato executório ser praticado fora do território nacional.

Entretanto, caso não seja possível determinar o limite do território entre duas ou mais jurisdições, ou não se sabe a jurisdição em razão, do crime ter se consumado ou tentado nas fronteiras entre duas ou mais jurisdições, o §3º do artigo 70 do Código de Processo Penal, dispõe que a competência será firmada pela prevenção.

Nem sempre, a competência para o julgamento do crime praticado pela internet, será da Justiça Federal. O artigo 109, da Constituição Federal, dispõe sobre a competência dos juízes federais. Desse modo, para que o crime cometido pela internet seja julgado pela Justiça Federal, deve encontrar amparo nos incisos IV e V do artigo 109 da Constituição Federal.

No conflito de competência 121.431-SE suscitado perante o Superior Tribunal de Justiça, julgado em 11/4/2012, Rel. Min. Marco Aurélio Bellizze, a Terceira Seção do STJ, diz que, a Justiça Federal não será competente para julgar todo e qualquer crime praticado pela internet, haja vista, que somente lhe compete, processar e julgar os crimes que ofenda bens, serviço ou interesses da União ou que o crime esteja elencado nos tratados ou convenções internacionais em que o Brasil é signatário e se comprometeu combater, como por exemplo, o crime de pornografia infantil:

“CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER.

AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.

1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais,

tais como as redes sociais "Orkut" e "Twitter", não atraindo, por si só, a competência da Justiça Federal.

2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal." (CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012)

O Superior Tribunal de Justiça tem entendido que, para definição da competência para julgar o crime do artigo 241-A do Estatuto da Criança e do Adolescente, será necessário analisar se houve ou não a internacionalidade da conduta do agente criminoso, caso seja demonstrado que a publicação do material contendo cena de sexo explícito ou pornografia envolvendo criança ou adolescente transcendeu os limites do território brasileiro, internacionalizando o crime, a competência recairá sobre a Justiça Federal para apurar e julgar o crime, tendo em vista que, qualquer pessoa poderá acessar a imagem de qualquer lugar do mundo desde que esteja conectado na internet.

No caso do crime pornografia infantil praticado pela internet, compete a Justiça Federal julgar por estar o crime previsto na Convenção sobre Direitos da Criança e do Adolescente, aprovada pelos Decretos Legislativos 28/90 e 99.710/90, configurando a hipótese prevista no artigo 109, inciso IV da Constituição Federal, e se por ter a possibilidade do conteúdo publicado no Brasil, ser acessado de qualquer lugar do mundo, verificando a transnacionalidade do crime.

Da mesma forma, compete a Justiça Federal, processar e julgar, se publicação da imagem de cunho pornográfico contendo criança ou adolescente, for publicada no estrangeiro. Nesse caso, a aplicação da lei brasileira, segue-se a regra do artigo 7º, inciso II, alínea "a" do Código Penal, pois são os crimes previstos em tratados ou convenções internacionais que o Brasil se obrigou a reprimir.

Porém, para que se aplique a lei brasileira ao agente, no exemplo supracitado, necessário observar o artigo 7º, §2º do Código Penal, que determina que ele adentre em território nacional, o fato constitutivo do crime também configure crime no país em que foi praticado, o crime deve estar previsto entre os quais o Brasil autoriza a extradição, não ter sido o agente absolvido ou cumprido a pena no

estrangeiro e não ter sido o agente perdoado no estrangeiro, ou por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

Assim, enquadrando-se o agente nos requisitos expostos, será aplicada a regra do artigo 88 do Código de Processo Penal, que determina a competência para julgar os crimes cometidos fora do território nacional. Se o agente jamais residiu no Brasil será competente a Justiça Federal da Seção Judiciária da Capital da República, caso contrário, conforme decisão do Supremo Tribunal Federal, a competência para o julgamento passa a ser da Justiça Federal, respeitando o que está disposto no artigo 109, inciso V da Constituição Federal.

#### **1.4 Resultado e Discussões**

Neste artigo foi discutido o quão trabalhoso é para se identificar e apurar a autoria dos crimes cibernéticos, primeiramente foi abordado de forma simplória à história da internet no Brasil, bem como definiu o conceito de internet que consta no artigo 5º da Lei 12.965/2014, que trata do marco civil da internet no Brasil.

Adiante, abordou a maneira como as informações são trocadas na rede mundial de computadores, mostrando todo o processo de transferências de dados de um computador para o outro, sendo que para que ocorra essa troca de informação, necessário se faz que o computador esteja conectado na internet e possuir uma identificação, na qual é chamada de IP, que a Lei 12.965/2014 atribui o conceito de código atribuído a um terminal que permite identificar a máquina.

Uma forma rotineiramente utilizada por pessoas que utiliza a internet como meio de prática de crime é o Vírus, que é um *software*, um programa capaz de destruir e modificar os dados do computador infectado, o vírus mais conhecido é o *Trojan Horse*. Com a proliferação desse vírus no computador infectado, caso se utilize um *pen drive* neste computador e depois utilizar esse mesmo *pen drive* em outro computador, o computador que recebe as informações do *pen drive*, que não tenha um sistema de segurança, poderá ser infectado e se tornar mais uma vítima nas mãos desses criminosos.

Posteriormente, estudou possíveis crimes que são praticados pela internet, como o estelionato, previsto no artigo 171, do Código Penal, analisando o sujeito ativo e passivo do crime, o bem jurídico tutelado por este tipo penal. Assim, verificou-se que, quem usa a internet para praticar este tipo de crime, pratica crime contra o patrimônio, utiliza de meios que engana a vítima para que possa conseguir os dados necessários para consumação do cyber crime.

No praticar o crime de estelionato, consolidou a jurisprudência do STF que, não importa se a pessoa enganada ou que teve o prejuízo econômico tenha que ser um ente público, configurando o crime da mesma forma.

Outro crime muito praticado pela internet é o de pornografia infantil. Há um esforço midiático mundial para que possa influenciar as autoridades mundiais para que criem normas penais com penas mais rígidas e efetivas para quem comete esse crime.

O Código Penal no artigo 234 envolve tanto o conceito de pedofilia quanto o de pornografia infantil. O bem jurídico tutelado pelo direito penal nesse crime é o pudor público, pois divulgar material obsceno para criança ou adolescente, atenta contra a moral da coletividade. Por se tratar de crime comum, qualquer pessoa está sujeita a ser o autor do crime. Caso nas imagens reproduzidas ou veiculadas envolva crianças ou adolescentes, aplicar-se-á ao ator do fato as normas previstas nos artigos 240 a 241-E do Estatuto da Criança e do Adolescente.

O diploma protetor dos direitos e garantias da criança e do adolescente se preocupou em incriminar aquela conduta que utiliza a internet como meio de propagação de conteúdo pornográfico, que cujo conteúdo contenha crianças ou adolescente, no artigo 241-A. Da mesma forma, o sujeito ativo desse crime pode ser qualquer pessoa, basta veicular na rede mundial de computadores conteúdo de cunho pornográfico contendo menores.

O STF entende desde 1998 que o artigo supracitado, tem total aplicabilidade as condutas que utiliza a internet como meio de praticar esse crime, por entender que se trata de norma penal aberta, consumando o crime qualquer publicação pornográfica envolvendo menor de idade, seja qual for o meio utilizado para disseminar o conteúdo.

O autor Carlos Alberto Di Franco, o seu artigo internet e Pornografia, até propôs soluções para se reduzir o cometimento desse crime na internet, e uma delas é tirar a sensação de impunidade com penas mais severas e com maior eficácia, quando da identificação do autor.

Consequente, o presente artigo no tópico relacionado às dificuldades da identificação do autor do crime cibernético foi discutido as teorias existentes norteadoras do conceito de autor de crime, sendo que no Brasil, a maioria dos doutrinadores existem cinco as correntes que discorrem sobre a autoria e partícipe do crime.

O Código Penal brasileiro, não diferenciou o autor do fato com partícipe, adotando a Teoria Objetiva no artigo 29, conforme Rogério Sanches e a maioria da doutrina. Assim, aquele que ajuda na prática do crime, será pela justiça julgado e apenado conforme a pena prevista para o crime de acordo com a sua culpabilidade.

Quando o autor utiliza a internet para praticar crime, ele adota uma identidade falsa, que não corresponde com a que é apresentada na rede mundial de computadores. Por esse motivo, encontra-se uma barreira para se identificar quem realmente é o autor, pois ao usar dados inverídicos, o setor de inteligência da polícia militar, bem como os órgãos competentes para identificar o criminoso, necessitam de maior tempo e mão de obra para se chegar ao criminoso.

Por isso, necessário se faz a colaboração das Provedoras de Acesso a Internet, juntamente com as forças policiais, fornecendo os dados necessários para se chegar ao local do crime, disponibilizando o IP, a identidade do computador ligado a rede, exemplificando, de forma eficiente e rápida.

Por ser a produção de prova bem complexa, exige-se do órgão competente da colheita a observância de uma série de regras e princípios previstos na Constituição Federal, como garantias e direitos individuais do acusado e não admitindo qualquer prova que fora colhida de forma ilícita.

Eugenio Pacielli, processualista penal brasileiro, diz que essa gigantesca tarefa de colher provas, deve sempre respeitar os preceitos constitucionais, para não comprometer a produção da prova, tornando-a ilícita, e conseqüentemente inservível para o processo que apura a autoria.

O princípio da vedação da prova ilícita previsto constitucionalmente, também deve ser observado quanto aos efeitos produzidos pela prova produzida. No caso do crime cibernético, não tendo a autoridade competente autorização judicial para interceptar os dados, ela será totalmente ilícita e não prestara para provar a materialidade delitiva e a autoria.

O Código de Processo Penal, no artigo 157, foi fiel ao princípio constitucional da vedação da prova ilícita, pois possui redação idêntica ao preceito constante no artigo 5º inciso LVI da constituição.

Por o crime praticado na internet deixar vestígio, as provas armazenadas no computador do criminoso deverão ser reproduzidas para ser periciadas, com objetivo de preservar a prova original, pois se futuramente no decorrer da investigação ou processo ocorrer dúvidas, poder ser sanadas.

Quando da produção da prova, a autoridade competente por produzi-la, deve seguir uma ordem cronológica, para que se possa entender toda a dinâmica do crime, com fim chegar na verdade real do fatos, identificando o autor, e provando a materialidade delitiva.

Por fim, abordou-se de quem é a competência para julgar o autor e os crimes praticados pela internet. No Brasil, para fins de aplicação da lei penal, o Código Penal, no artigo 5º, adotou o princípio da territorialidade, em que se aplica aos crimes praticados no território brasileiro a lei penal brasileira, sem prejuízo da aplicação das convenções, tratados e regras do direito internacional.

A Constituição Federal trás critérios para definir a competência do órgão julgador, assim como as leis infraconstitucionais, utilizando os critérios em razão da matéria, funcional e territorial.

A regra adotada pelo Código de Processo Penal no artigo 70 estabelece que a competência seja determinada pelo lugar em que se consumar o crime, em caso de tentativa, será competente o juízo do lugar onde ocorreu o ultimo ato de execução do crime.

Verificada a situação em que não seja possível determinar o limite do território entre duas ou mais jurisdições, o §3º do Código de Processo Penal, diz que a competência será determinada pela prevenção.

A Constituição Federal, no artigo 109, dispõe sobre a competência dos juízes federais. Assim, os crimes praticados pela internet, somente será da competência da Justiça Federal caso se enquadre nos incisos IV e V do referido artigo.

O Superior Tribunal de Justiça, entende que a competência para julgar o crime do artigo 241-A do ECA será definida depois de se analisar se ocorreu ou não a internacionalidade da conduta criminosa, se restar comprovado que a publicação do material pornográfico infantil transcendeu os limites do território nacional, internacionalizando o crime, a competência recairá sobre a Justiça Federal para apurar e julgar o crime, pois qualquer pessoa em qualquer lugar do mundo, poderá acessar o conteúdo publicado.

No caso do crime pornografia infantil praticado pela internet, compete a Justiça Federal julgar por estar o crime previsto na Convenção sobre Direitos da Criança e do Adolescente, aprovada pelos Decretos Legislativos 28/90 e 99.710/90, configurando a hipótese prevista no artigo 109, inciso IV da Constituição Federal, e

se por ter a possibilidade do conteúdo publicado no Brasil, ser acessado de qualquer lugar do mundo, verificando a transnacionalidade do crime.

Portanto compete a Justiça Federal, processar e julgar, a publicação da imagem de cunho pornográfico contendo criança ou adolescente no estrangeiro. Nesse caso, a aplicação da lei brasileira, segue-se a regra do artigo 7º, inciso II, alínea “a” do Código Penal, pois são os crimes previstos em tratados ou convenções internacionais que o Brasil se obrigou a reprimir.

## **Considerações Finais**

O presente trabalho analisou o tema, as dificuldades de se identificar crimes pela internet, em que foram abordados os aspectos históricos, o funcionamento da internet, possíveis crimes que podem ser praticados utilizando a internet como meio, bem como os obstáculos encontrados para identificar o agente, na colheita de provas e na competência para julgar o crime praticado pela internet.

A intenção deste trabalho foi de verificar quão é trabalhoso desvendar a autoria do crime praticado pela internet, a facilidade de se modificar as provas do crime, a maneira e as técnicas utilizadas por quem pratica esse tipo de crime, que normalmente são eficazes.

O presente trabalho também mostra que ao se navegar pela internet, deve-se ter cautela quando acessamos *sites* desconhecidos, ou ate mesmo aqueles acessados com maior frequência, haja vista que a não observância dos detalhes de segurança que a página virtual possui, pode-se estar diante de uma página falsa, tornando-se vulnerável para que, posteriormente, os criminosos invadam o computador e capturem informações sigilosas que poderão ser utilizadas para o cometimento de outros crimes.

Por vezes, os crimes cibernéticos, são praticados em *lan house* ou em *cyber cafés*, onde nem sempre o usuário possui um registro, ou são praticados fora dos limites da soberania do Estado brasileiro, o que dificulta identificar a autoria, a colheita de provas, bem como a quem compete julgar o crime.

Sendo assim, necessário seria criar normas que regulamentassem esse tipo de crime, não bastando à previsão de penas rigorosa ou desmedidas, mas normas de cooperação entre os países que por ventura punem os crimes praticados pela internet, ou entre os países e provedoras de acesso, em busca para coibir e punir quem pratica os crimes cibernéticos.

## REFERÊNCIAS

INELLAS, Gabriel Zaccaria de. Crimes na Internet. 2ª ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009.

MIRABETE, Julio Fabbrini. Manual de direito penal, volume 1: parte geral, arts. 1º ao 120 do CP. – 30. ed. rev. e atual. São Paulo : Atlas, 2014.

CAPEZ, Fernando. Curso de direito penal: parte geral, volume 1 (arts. 1º a 120). 7. ed. rev. e atual. São Paulo: Saraiva, 2004.

CUNHA, Rogério Sanches. Manual de direito penal: parte geral (arts. 1º ao 120). 4. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2016.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 8. ed. rev., ampl. e atual. Salvador: JusPODIVM, 2016.

OLIVEIRA, Eugênio Pacelli de. Curso de processo penal. 19. ed. rev. e atual. São Paulo: Atlas, 2015.