# PROCESSO PENAL: A metodologia utilizada no procedimento investigativo dos crimes cibernéticos e sua presença nas normas vigentes

# CRIMINAL PROCEDURE: The methodology used in investigative procedures of cybercrimes and their presence in current norms

Laís Dimas Saraiva de Oliveira[1]

Msc. Guilherme Tomizawa[2]

## RESUMO

O objetivo desse estudo é conceituar de forma sucinta o que é o crime cibernético e o procedimento investigativo, além de demonstrar sua presença e efetividade presente no Direito brasileiro. Para isso, utiliza-se do método teórico, tendo em vista que é possível através de fontes pré-existentes, ou seja, pesquisas bibliográficas já realizadas anteriormente, como livros, artigos periódicos e revistas, para que de forma dedutiva, seja possível alcançar o estudo específico do tema, através de fontes mais amplas. Portanto, busca-se entender como ocorre atualmente, a fim de que seja possível averiguar possíveis necessidades de aperfeiçoamento do sistema jurídico brasileiro, dando assim, maior celeridade e eficiência nos processos penais de crimes cibernéticos.

Palavras-chave: Cibercrime. Investigação. Brasileiro.

## *ABSTRACT*

The purpose of this study is to succinctly conceptualize cyber crime and its investigative procedure, as well as to demonstrate its presence and effectiveness present in Brazilian Law. For this, the theoretical method is used, considering that it is possible through pre-existing sources, that is, previous bibliographical researches, such as books, periodical articles and magazines, so that in a deductive way, it is possible to reach the study of the theme, through broader sources. Therefore, it is sought to understand how it is currently occurring, so that it is possible to ascertain possible needs for the improvement of the Brazilian legal system, thus giving greater speed and efficiency in criminal proceedings for cyber crimes.

Keywords: Cybercrime. Investigation. Brazilian.

[1] Laís Dimas Saraiva de Oliveira, estudante de direito no 8° período, da Instituição de ensino FMF – Wyden, endereço eletrônico: lalahdimas@gmail.com
(Saraiva de Oliveira, 2018)

[2] Orientador: Guilherme Tomizawa, professor na instituição de ensino FMF – Wyden, endereço eletrônico: professorguilhermet@yahoo.com.br
(Tomizawa, 2018)

## 1. INTRODUÇÃO

Com a modernização dos meios de comunicação, grande parte dos litígios presentes atualmente se dá de modo cibernético. Com isso, novas normas são necessárias para o devido amparo e garantia de direitos pessoais. Os crimes cibernéticos não possuem legislação própria, o que torna muitas vezes o processo ineficaz ou imprevisível, visto a dificuldade de não possuir seus próprios meios de resolução. A escolha do presente tema se dá pela necessidade de discussão nos dias atuais, e o quão prejudicial é a falta de alguns aspectos na legislação vigente. É de extrema importância regular de forma eficaz algo que ocorre diariamente, e que afeta milhares de pessoas.

Isso porque os crimes cibernéticos são atos ilícitos cometidos virtualmente, ou seja, por meio da rede de computadores e redes de Internet, os quais são suas principais ferramentas para a realização do crime. São geralmente atos de maior dificuldade de apuração, pois o âmbito virtual é facilmente manipulado, possuindo autores anônimos que se escondem por trás dos dispositivos, necessitando de uma equipe própria para localização por meios de códigos e infiltrações, nas quais muitas vezes podem causar complicações por necessitarem usar da invasão de privacidade, devido às informações pessoais ali resguardadas.

Portanto, traz como objetivo a discussão sobre tal tema tão popular e recente: O procedimento utilizado no processo penal de crimes cibernéticos e sua presença nas normas vigentes, de forma a propiciar um melhor esclarecimento sobre o processo penal de crimes virtuais e seus métodos de investigação, apuração de fatos e provas e medidas adotadas no ordenamento jurídico brasileiro atual, além de explicar o conceito e analisar de modo crítico os meios utilizados atualmente na forma como se dá o processo e apuração de fatos e provas de crimes cibernéticos, e discutir seus limites conforme o ordenamento jurídico brasileiro.

Para se alcançar tais objetivos com este artigo, utiliza-se o método de abordagem teórico, que se dará por meio de pesquisas bibliográficas, tendo em vista que será realizado o estudo por meio de fontes pré-existentes, como periódicos, artigos e outros textos científicos, cominando em revisão de literatura, com o objetivo de serem utilizadas referências de autores atuais, ao passo que os crimes eletrônicos também são litígios surgidos atualmente, com análise crítica,

demonstrando pontos de vista, a fim de chegar em uma solução para determinado problema, como também por método dedutivo, pois partirá de uma ampla visão, para então chegar a análises específicas em casos concretos. Utilizando-se também de princípios, leis e teorias já comprovadas, consideradas indiscutíveis e verdadeiras que justificam o caso concreto.

## 2. DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são os delitos cometidos por meio da internet, podendo ser por redes domésticas, públicas ou privadas, com a finalidade de furto de informações, crimes contra a honra e a dignidade da pessoa humana, invasões de privacidade, e até mesmo invasão à websites governamentais e perfis privados em redes sociais. Tendo em vista o meio utilizado, torna-se difícil de ser apurado, necessitando de uma equipe especializada para a localização do infrator.

De acordo com Cassanti (2016) “Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão”. Dentre eles, estão os crimes de fraude financeira, os quais consistem em alterar de forma não autorizada dados pessoais, ou inserindo instruções não autorizadas, e até mesmo usar de processos não permitidos; tão como alterar, destruir, suprimir ou roubar informações, geralmente para ocultar transações não autorizadas.

É possível até mesmo o tráfico de entorpecentes online, que geralmente se dá por meio da Darknet, que segundo Michel Salát: é toda página, fórum ou loja virtual que está escondido e inacessível aos meios de busca comuns, como por exemplo o Google ou Bing, mas que usam protocolos padrões HTTP/HTTPS para ser possível acessar por um navegador de rede comum, como o Edge, Chrome e Firefox.

Ainda segundo Michel Salát:

> Tanto a deepnet como a darknet são frequentemente palco de atividades ilegais, por exemplo, a distribuição de bens e serviços ilegais. Você pode comprar drogas, armas e malware na web profunda e na darknet, e infelizmente, até serviços de assassinos profissionais. A darknet, no entanto, fornece mais anonimato do que a deepnet, e provavelmente por isso, é mais popular entre os cibercriminosos. A darknet é acobertada pelos nós e criptografia da rede Tor, mas algumas informações vazadas indicam que a NSA (agência de inteligência americana) pode ter métodos para rastrear usuários da Tor. (SALÁT, 2017, https://blog.avast.com/pt-br/mergulhando-nasprofundezas-da-internet-a-darknet)

Tendo em vista a gravidade de tais crimes, constantemente profissionais especializados trabalham para desenvolver meios mais eficazes e ágeis a fim de colher informações pertinentes à localização dos infratores e suas motivações. Podendo assim, trazer ao Judiciário para apuração na esfera criminal.

Portanto, tendo em vista o quão vasto é o espaço cibernético, há de acrescentar que se tornou alvo de oportunidade para o cometimento de delitos e infrações contra bens jurídicos alheios. Isso porque por ser tão abrangente, o ambiente virtual é bastante aberto e de livre expressão (limitado por leis nacionais e internacionais).

> Crime virtual nada, mas é que o termo utilizado para se referir as atividades ilícitas praticadas onde envolvem um computador ou uma rede de computadores qual é invadida sem autorização e utilizada como uma ferramenta, uma base de ataque ou como meio de crime. JOANONE, 2017, http://www.conteudojuridico.com.br)

Por conta da maior facilidade em realizar atos ilícitos em anonimato, a quantidade de crimes cibernéticos é frequente, sendo registrado 54 crimes virtuais por minuto em 2012, segundo a multinacional Symantec, empresa de segurança na internet. A rede de computadores está entre os meios mais utilizados para a propagação de pedofilia e roubo de informações de contas bancárias, porém, entre os mais frequentes, estão os crimes contra a honra.

Crimes estes cometidos por hackers, que podem até mesmo serem proliferados através de vírus, como o que ocorre com o Vírus Ransomware, que consiste na criptografia de todas as informações e dados contidos na máquina, sob a ameaça de publicar todas essas informações ou deletá-las permanentemente, mas que pode não fazê-lo sob a condição da vítima pagar o valor que lhe foi imposto a fim de reaver o computador e dados afetados.

Os crimes podem ocorrer de inúmeras formas, pela proliferação de inúmeros vírus, ou até mesmo roubo de dados advindos de qualquer outra modalidade, como invasão direta da máquina.

## 3. DOS ASPECTOS GERAIS DA INVESTIGAÇÃO DO CRIME

De acordo com Waldek Fachinelli Cavalcante, o primeiro passo é descobrir que dispositivo foi utilizado na hora do crime, como por exemplo redes sociais, e-mails, blogs, entre outros.

A partir daí, ocorre a investigação pelas camadas mais internas de tais plataformas, como em logs que "é o processo de registro de eventos relevantes num sistema computacional". Tal registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Por IP (Internet Protocol) que é o endereço eletrônico de conexões de redes locais com a internet, dos quais levam à endereços físicos de onde o delito foi cometido. Além destes, há também como localizar informações de responsáveis por domínios de endereços eletrônicos chamados websites, solicitando ao gestor de cada país, no caso, www.registro.br é o gestor de tais dados em domínios brasileiros.

Além do IP, há o DNS, que é o Sistema de Nomes de Domínios. Ele consiste em armazenamento de dados sobre um domínio, o qual pode ser gerenciado por várias organizações diferentes, a depender de quem comprou. É o que chamamos de hoster, pois consiste em ser o “mantedor” dos websites, que são subdomínios do host, ou seja, do DNS em questão.

Há também os cabeçalhos de e-mails, que possuem informações relevantes para localizar o remetente, como endereço de IP, fuso-horário, data e hora, cujas informações fornecidas podem variar dependendo da plataforma usada.

Além destes principais, há outros meios em que podem ocorrer crimes eletrônicos, com seus próprios meios de averiguação.

Autoridades competentes do setor informático do Brasil, entre outros meios, de acordo com a 2ª Câmara de coordenação e revisão, 2013, podem utilizar-se do WHOIS, que de forma sucinta, é a base de dados públicos, mantidos por organizações envolvidos no modelo de governança. Elas oferecem dados e informações de indivíduos ou corporações que são responsáveis por um domínio ou registro de IP na Internet. É através dela que é possível chegar a verificar quem responde por ocorrências ilícitas na rede.

É portanto, uma das ferramentas mais populares para coleta de informações por meio do IP, e pode ser utilizado em vários sistemas operacionais, como o Linux, MacOS, como diversos outros Unix, estes possuem o software disponível para instalação já como padrão.

Há de salientar a importância de saber o registro de IP de um domínio, pois é através dele que é possível a obtenção de detalhes essenciais à localização física de onde o usuário está geograficamente. Porém, ao comprar um domínio, o comprador possui a liberdade de associá-

lo a qualquer endereço IP, portanto, o nome de domínio não é o suficiente para revelar a localização geográfica de um website na internet.

Já para a obtenção de informações detalhados sobre DNS, é feita a consulta de registros do domínio, os investigadores brasileiros utilizam-se do Dig (domain information groper), que assim como o WHOIS, possui instalamento padrão em sistemas Unix e similares. Com ele, são realizadas perguntas aos servidores DNS e exibe as respostas advindas, sendo possível até mesmo reconhecer um endereço IP a partir do nome de um domínio.

Através dos recursos citados, é possível a coleta de informações diretamente através das autoridades brasileiras, e em algumas situações, é necessária a sagacidade do investigador para que em segundos encontre caminhos mais ágeis a fim de localização do criminoso ou de qual instituição será capaz de agilizar o procedimento através de auxílio.

## 3.1 DAS PROVAS NO CIBERCRIME

De forma similar à ciência forense, os crimes consolidados na internet consistem na aquisição, preservação, análise e apresentação das provas, de acordo com o Roteiro de Atuação sobre Crimes Cibernéticos feito pela 2ª Câmara de Coordenação e Revisão do Ministério Público Federal. Neste, é explicado que graças ao contraditório, a defesa pode contestar a legitimidade das evidências, dos procedimentos investigativos e até mesmo laudos periciais, levando à maiores análises e demonstrações das informações contidas no trâmite processual.

Pode-se entender como evidências digitais uma espécie derivada do mundo físico, a diferença é que muitas podem ser manipuladas, como operações em sistemas e assim por diante, podem ser facilmente removidas, tornando apenas possível ao investigador averiguar o que lhe resta após o acontecimento dos fatos.

Para garantir que as provas não sofreram alterações, é necessário o procedimento pericial em dispositivos de armazenagem de arquivos e dados, como Pen drives, discos rígidos, e assim por diante.

Como dito anteriormente, com a devida autorização judicial é possível que se tome medidas técnicas com os instrumentos permitidos pelo judiciário, a fim de possibilitar a coleta de dados

sobre o criminoso, podendo ser desde infiltrações, intercepções telemáticas, inoculações até engenharia social (2ª Câmara de coordenação e revisão, 2013).

Para que essas evidências sejam válidas em juízo, é necessário que sejam preenchidos os requisitos. No Brasil, são aceitas as recomendações dadas pela RFC 3227 (Guidelines for Evidence Collection and Archiving), a qual auxilia os meios de conservação e coleta das provas obtidas eletronicamente. Entre elas, estão as recomendações de que a evidência deve ser: Admissível, autêntica, completa, confiável e convincente, e de acordo com o mesmo Roteiro de Atuação mencionado, é determinado que as evidências devem ser:

> Admissível: ou seja, estar em plena conformidade com a lei para que possa ser apresentada à justiça.
> Autêntica: as provas devem ser comprovadamente relacionadas ao incidente/crime investigado. O trabalho de uma documentação de qualidade é essencial para o cumprimento deste item.
> Completa: o conjunto de evidências deve fornecer uma apresentação completa acerca do evento investigado. Nunca deve depender de elementos faltantes ou duvidosos. Deve "contar a história" completa, e não apenas fornecer perspectivas particulares.
> Confiável: não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação. Convincente: além de todas as características anteriores, deve ser documentada e apresentada de forma clara e organizada.
> (2ª CÂMARA DE COORDENAÇÃO E REVISÃO, Roteiro de Atuação Sobre Crimes Cibernéticos).

Todavia, a fim de preservar tais provas, é também necessário que o investigador realize seu trabalho deixando a menor possibilidade de ser rastreado possível, porque assim como o criminoso (o qual grande parte das vezes, está dedicando-se a cometer os atos em anonimato), precisa precaver-se, e para maior celeridade na investigação, é necessário que o criminoso não saiba que está sendo investigado. Tem-se então a necessidade de que assista quanto aos rastros deixados durante o procedimento.

Sucessivamente, a fim de filtrar as provas cabíveis em juízo, é necessário que se adequem à causa, ou seja, que apenas o pertinente à ação esteja em tela. Para esse processo, segundo o Roteiro de Atuação, é chamada a “redução”, que remete à filtragem de dados e evidências obtidas naquele objeto, e consiste em pôr de lado tudo aquilo que seja inútil ao processo investigativo, com bastante cautela quanto à possibilidade de excluir uma prova importante sem intenção, ou que seja útil futuramente.

Após os procedimentos citados, é iniciada a etapa de análise das evidências digitais e o preparo do documento que apresenta todas as provas digitais úteis contidas de forma concisa, a fim de que seja apreciada pela justiça, além da elaboração de argumentos desprovidos de suposições. É importante analisar também a natureza do documento, muitas vezes o juízo pede apenas certos documentos específicos, como pareceres ou notas técnicas.

## 4. LEGISLAÇÃO ADOTADA ATUALMENTE NO BRASIL

De acordo com o portal eletrônico do Conselho Nacional de Justiça, atualmente há duas leis que tipificam os crimes cibernéticos no Brasil, ambas foram sancionadas no ano de 2012, e contam com a alteração do Código Penal brasileiro. Graças a elas, hoje é possível a penalidade tipificada para os crimes ocorridos no âmbito virtual em casos de invasão de computadores, disseminação de vírus e até mesmo de códigos para roubos de senhas, assim como os utilizados no uso irregular de cartões de crédito e débito de titularidade alheia.

Entre elas, a lei mais específica é a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como a Lei Carolina Dieckmann, cujo caso deu origem à tipificação dos crimes descritos na lei, são eles: atos de invasão à computadores, a invasão de dados de usuários e websites. Entretanto, vale ressaltar que tal lei já era alvo de discussões entre legisladores, tendo em vista a quantidade de casos ocorridos diante destes atos ilícitos.

Crimes de menor potencial ofensivo, como a invasão de dispositivos eletrônicos ou informáticos, podem sofrer pena de três meses a um ano de prisão e multa. Já os de maior potencial ofensivo, como os que por consequência de tal invasão receberem conteúdos de comunicação privados, segredos de comércio e indústria, ou informações sigilosas, podem sofrer pena de seis meses a dois anos de prisão e multa.

A segunda lei, sancionada em 2014, é o Marco Civil da Internet (Lei 12.965/2014), que, regula quanto aos direitos e deveres dos usuários, bem como a proteção dos dados pessoais e privacidade. A ideia sobre a punição à retiradas de conteúdo do ar inicialmente se deu por meio desta lei, que a acolheu de forma genérica, sem especificidades, abarcando apenas os casos em que se necessita de ordens judiciais, exceto nos casos de “pornografia de vingança”, como chama o Conselho Nacional de Justiça, crimes estes que receberam maior regulamentação na Lei 12.737/2012.

Além dessas regulamentações, a Lei 12.965/14 também garante o direito à liberdade de expressão como um dos mais importantes princípios, e de forma mais especifica os direitos à proteção dos internautas perante o judiciário.

## 4.1. DA INCLUSÃO DOS CRIMES CIBERNÉTICOS NO NOVO CÓDIGO PENAL

Atualmente, nos casos em que não há tipificado a conduta nas Leis previamente discutidas, utiliza-se as sanções contidas no Código Penal (Decreto-Lei 2.848/40), o que torna a celeridade dos procedimentos prejudicada, tendo em vista que os crimes ocorridos no âmbito físico possuem menor complexidade quanto a produção de provas, o contrário do que ocorre nos mesmos crimes ocorridos em âmbito virtual, que podem ser consumados de inúmeras formas diferentes, como por e-mails, redes sociais, portais de notícias, conversas privadas em redes de bate-papo, e assim por diante.

Diante do impacto causado pelos meios virtuais que possuem abrangência extensa, há de se destacar a importância das sanções, que possuem a função de evitar o acontecimento desses crimes, e por isso, discute-se a necessidade da inclusão de capítulos dedicados aos crimes virtuais no Código Penal brasileiro, como na proposta de reforma do Código, a PLS 236/2012, denominada de "Novo Código Penal Brasileiro", em que discute-se questões sobre os crimes cibernéticos.

De acordo com o artigo publicado por André de Paula Viana no portal eletrônico "Observatório do Governo Eletrônico" com parceria da UFSC, a proposta do Novo Código Penal foi inspirada na Convenção de Budapeste, também conhecida como "A Convenção sobre o Cibercrime", a qual traz vertentes de direito penal e direito processual penal como soluções de conflitos ilícitos virtuais.

A Convenção sobre o Cibercrime foi criada em 2001 na Hungria, através do Conselho da Europa, e vem sendo utilizada na prática desde 2004, que após ser ratificada em cinco países, passou a englobar cerca de 20 países (EDERLY, 2008 apud SOUZA; PEREIRA, 2015 p. 5). Tem a finalidade de regular e auxiliar as apurações de cibercrimes, bem como dispor de penas e sanções aos usuários que agirem de forma ilícita na internet de forma padronizada. Sobre a Convenção, Gills Lopes Macêdo Souza e Dalliana Vilar Pereira conceituam:

> Segundo seu Preâmbulo, a Convenção prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da

> cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada". Ademais, ainda em seu escopo inicial, ressalta o obrigatório respeito: (i) à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); (ii) ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à (iii) Convenção das Nações Unidas sobre os Direitos da Criança (1989); e (iv) à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999). (SOUZA; PEREIRA, 2015 p. 5).

Portanto, trata-se de uma possibilidade a ser implementada futuramente neste ordenamento jurídico, a fim de atualizar as normas para que se adaptem às necessidades na resolução de conflitos jurídicos ao bem alheio. De forma a ajudar na celeridade processual nos cibercrimes ocorridos no território brasileiro, tornando assim, a possibilidade de padronização quanto aos outros países que adotam a referida Convenção como meio de tipificar ou regulamentar os atos ilícitos ocorridos pela internet.

## 5. CONCLUSÃO

Nos últimos anos, é perceptível o aumento de pesquisas quanto aos cibercrimes. Por se tratar de um assunto extremamente atual e recorrente, faz-se necessário a discussão sobre o tema, a fim de possibilitar o avanço técnico e jurídico quanto aos crimes cometidos no âmbito virtual.

Os crimes virtuais são atos criminosos que ocorreram por meio da internet, ou qualquer outro serviço de rede e informático, os quais contam como o principal instrumento utilizado ao cometer o crime. Acredita-se que o motivo para tamanha quantidade destes atos cometidos diariamente se dá pela facilidade do anonimato na rede de computadores, facilitando assim o cometimento das infrações.

De acordo com VIANA, 2017, a legislação atual não é o suficiente para que se dê a eficiência na tramitação processual dos crimes, isso porque não possuímos leis que tipificam uma quantidade ampla de crimes virtuais, tornando o procedimento baseado apenas o que há no Código Penal Brasileiro, e como se sabe, crimes cometidos em âmbitos físicos tornam a busca por evidências e trâmites processuais diferentes. Como diz JOANONE, Bruno, 2017, a forma como é permanecida as normas do Direito Penal sem adição de capítulos específicos para os cibercrimes, é responsável pela demora processual dos mesmos. É daí que surge a discussão sobre a implementação da Convenção de Budapeste, como disse SOUZA, Gills Lopes Macêdo, ET AL., 2015, ou até mesmo a reforma do Código Penal brasileiro, a fim de que se adapte de

forma padronizada com os países que aderiram à regulamentação presente na Convenção de crimes cibernéticos.

Segundo o periódico virtual publicado por ARAÚJO, Marcos, 2017, foram constatados em Belo Horizonte cerca de 65 crimes virtuais no dia. Pela quantidade de crimes cometidos constantemente, necessário se faz a celeridade processual, a fim de apurar juridicamente a ocorrência desses crimes. No entanto, de acordo com o Roteiro de Atuação sobre Crimes cibernéticos, é possível visualizar a dificuldade investigativa que os profissionais da informática enfrentam para a possibilidade de se obter provas em juízo, isso ocorre pelo fato de ser extremamente fácil a modificação e exclusão de provas pelos próprios criminosos, e a necessidade burocrática para apuração das mesmas.

**REFERÊNCIAS BIBLIOGRÁFICAS**

2ª CÂMARA DE COORDENAÇÃO E REVISÃO MATÉRIA CRIMINAL E CONTROLE EXTERNO DA ATIVIDADE POLICIAL, 2013. **Roteiro de Atuação Sobre Crimes Cibernéticos**. 2. Ed rev. – Brasília: MPF/2°CCR,2013, 472p.

ARAÚJO, Marcos, 2017. **Minas Gerais registra 65 crimes na internet por dia.** Notícias. Disponível em: https://tribunademinas.com.br/noticias/cidade/08-10-2017/minasgerais-registra-65-crimes-na-internet-por-dia.html. Acesso em: 13 de maio de 2018

Associação do Ministério Público de Minas Gerais, 2012. **Brasil registra 54 crimes virtuais por minuto.** Disponível em: https://amp-mg.jusbrasil.com.br. Acesso em: 15 de maio de 2018

BUDAPESTE, 2001. **Convenção sobre o Cibercrime**, Budapeste

CASSANTI, Moisés de Oliveira, 2016. **O que são crimes virtuais?** Disponível em: < http://idciber.eb.mil.br/index.php?option=com_content&view=article&id=795:o-quesao-crimes-virtuais&catid=78&Itemid=301. Acesso em: 10 de abril de 2018

CAVALCANTE, Fachinelli Waldek, **Crimes cibernéticos: noções básicas de investigação e ameaças na internet**. Disponível em: https://www.conteudojuridico.com.br/pdf/cj054548.pdf. Acesso em: 15 de abril de 2018

COSTA, Thabata Filizola, 2016. **Desafios para a investigação de crimes virtuais**. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/351838651/desafios-para-ainvestigacao-de-crimes-digitais. Acesso em: 13 de maio de 2018

DORIGON, Alessandro, ET AL., 2018. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova de materialidade**. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-naobtencao-de-indicios-da-autoria-e-prova-da-materialidade/2. Acesso em: 30/11/2018

FRANCO, Deividson Pinheiro, 2016. CSI do Século XXI | **A computação Forense e a Investigação de Crimes Cibernéticos. Banco de notícias**. Disponível em: < https://cryptoid.com.br/banco-de-noticias/csi-do-seculo-xxi-computacao-forense-einvestigacao-de-crimes-ciberneticos/. Acesso em: 20 de maio de 2018

JOANONE, Bruno, 2017. **Crimes virtuais e a necessidade de uma legislação específica**. Disponível em: http://www.conteudojuridico.com.br/artigo,crimes-virtuaise-a-necessidade-de-uma-legislacao-espeficica,588942.html. Acesso em: 17 de maio de 2018

OLIVEIRA, Bruna Machado de ET AL., 2017. **Crimes virtuais e a legislação brasileira. Revista do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo**. Disponível em: http://local.cnecsan.edu.br. Acesso em: 20 de maio de 2018

SILVA, Walber Carlos da, 2018. **Normas, princípios e regras no ordenamento jurídico brasileiro**. Disponível em: https://jus.com.br/artigos/64137/normas-principios-eregras-no-ordenamento-juridico-brasileiro. Acesso em: 17 de maio de 2018

SOUZA, Gills Lopes Macêdo, ET AL., 2015**. A Convenção de Budapeste e as Leis brasileiras**. Disponível em: http://www.egov.ufsc.br/portal/conteudo/convenção-debudapeste-e-leis-brasileiras. Acesso em: 27/11/2018

VIANA, André de Paula, 2017**. Crimes virtuais e a necessidade de uma legislação específica**. Disponível em: http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-enecessidade-de-uma-legisla%C3%A7%C3%A3o-especifica. Acesso em: 27/11/2018

WENDT, Emerson e JORGE, Higor Vinícius Nogueira, 2013, **Crimes Cibernéticos: Ameaças e procedimentos de investigação** - 2 ª Edição, Ed. Brasport, Rio de Janeiro