CRIMES VIRTUAIS: as formas e os meios de investigação.

VIRTUAL CRIMES: the forms and means of investigation.

Caetano, Eduardo Sousa [1]

Plínio, James das Graças Nunes[2]

RESUMO

Este estudo foi realizado pela metodologia revisão bibliográfica. Em uma época marcada pelo desenvolvimento tecnológico, os criminosos não ficaram para traz. Crimes comuns ao mundo real os chamados “crimes impuros” passaram a ser cometidos também pelo meio virtual, o surgimento de crimes típicos do mundo virtual chamados “crimes puros” pois utilizam de habilidades e conhecimentos específicos de informática para sua pratica. Com o passar dos anos necessitando de uma adaptação das autoridades policias para a investigação e combate aos crimes virtuais. A popularização da DeepWeb contribui para o anonimato e a facilidade como o crime pode ser cometido pela internet, levando em consideração que seu tamanho é muito maior que a internet convencional, proporcionando um conteúdo muito maior.

Palavras-chaves: Investigação; Crimes Virtuais; Internet.

ABSTRACT

This study was carried out by the literature review methodology. In a time marked by technological development, criminals have not been left behind. Crimes common to the real world, so-called "impure crimes" have also been committed by virtual means, the emergence of typical crimes of the virtual world called "pure crimes" because they use specific computer skills and knowledge for their practice. With the passage of the years needing an adaptation of the police authorities for the investigation and fight against the virtual crimes. The popularization of DeepWeb contributes to the anonymity and ease of how the crime can be committed on the internet, taking into account that its size is much larger than the conventional Internet, providing content much larger.

Keywords: Research; Virtual Crimes; Internet.

[1] Aluno do curso de Pós-Graduação da PMGO, Turma Q de Goiânia-GO, do Comando da Polícia Militar de Goiás – CAPM, e-mail: caetasousa@gmail.com

[2] Professor Orientador(a): Comando da Academia da Polícia Militar de Goiás – CAPM, e-mail: jamespgn@pm.go.gov.br, Goiânia-GO, Maio de 2018.

INTRODUÇÃO

Este trabalho visa o estudo detalhado sobre o tema de Crimes Virtuais e discutir os crimes tipicamente cibernéticos (crimes virtuais puros) e os crimes que possuem o computador ou dispositivo eletrônico (crimes virtuais impuros). O código penal é do ano de 1940 foi atualizado no decorrer dos anos, porém boa parte dos crimes listados em 1940 podem se enquadrar como crime cibernético desde que tenha o computador ou dispositivo semelhante que proporcione ações criminosas por exemplo, as máquinas de cartão de crédito. Outros crimes necessitam de legislação específica para ocorrer a tipificação.

O surgimento da internet através do exército americano e chegando até o marco inicial de uma rede mundial que foi o surgimento do protocolo de comunicação entre redes TCP/IP, apesar de nos dias atuais tivemos evolução nessa tecnologia através das versões do IP. O IP versão 4 que por sua vez já esgotou a sua capacidade de expansão e possui alguns problemas de segurança que foram solucionados com a versão 6. A versão 6 possui uma maior capacidade de expansão e maior segurança todo desenvolvimento tecnológico no que se refere a redes de computadores tem como base o protocolo TCP/IP.

A internet é o meio de comunicação que possibilitou a comunicação entre várias empresas do mundo e com isso proporcionando uma enorme agilidade em seus processos. Outra grande mudança que ocorreu em todo o mundo, foi o surgimento das redes sociais que vieram para proporcionar a cada pessoa o uso do seu direito de liberdade de expressão, com isso diminuindo e muito o poder dos grandes veículos de comunicação em todo o mundo. Porém com toda essa liberdade também acarreta que as pessoas percam o limite ao falar sobre determinado assunto ou discutir sobre algum tema polêmico, os crimes de injúria, calúnia e difamação são normais no dia a dia na internet, tudo acobertado pelo suposto “anonimato” que a rede nos proporciona as pessoas tendem a se tornarem intolerantes umas com as outras, partindo assim para as ofensas gratuitas.

Este trabalho será feito com a metodologia de revisão de literatura. Entre os objetivos deste estudo está a análise sobre os principais crimes que ocorrem na rede mundial de computadores, a forma como e possível a investigação de tais crimes, o anonimato que a DeepWeb proporciona a quem deseja procurar no mercado negro armas e drogas entre outros tipos de crimes que são facilmente encobertos pela dificuldade de

acesso à rede. Observar as legislações que vêm sendo aplicadas no decorrer dos anos e analisar se existe a necessidade de alterações nas legislações vigentes, pois nossas legislações não evoluem de acordo com o crescimento tecnológico que vem acontecendo em todo mundo e com o surgimento com novos tipos penais decorrentes dessa evolução.

REVISÃO DE LITERATURA

SURGIMENTO DA INTERNET

A primeira rede de computadores nasce através do estudo de quatro universidades, foi construída entre as faculdades de Universidade de Utah, Stanford Research Institute, Universidade da Califórnia – Santa Bárbara e Califórnia - Los Angeles. Entrando em funcionamento a ARPANET (Advanced Research Projects Agency Network) na data de 1 de dezembro de 1969.

Durante o desenvolvimento foi criado um grupo com quatro estudantes de cada Universidade, esse grupo ficou conhecido como Network Working Group ou a sigla NWG. Entre os estudantes figurava Vinton Cerf que, mais tarde, virá a ser chamado de o "pai" da internet.

A rede de comunicação utilizada foi a telefónica, alugando alguns circuitos. Em agosto de 1972 o grupo anteriormente de quatro estudantes foi ampliado para trinta. Esta data e considerada o início e também um marco para atividade da primeira comunidade virtual.

ARPANET em 1972 foi rebatizada DARPANET a sigla D era um alerta aos pesquisadores a época pois lembrava Defense ou seja a rede dependia de recurso do Pentágono para o desenvolvimento, sendo assim tendo o governo acesso remoto aos dados. O que leva a criação de uma rede internacional que mais tarde viria a ser denominada "Internet".

A equipe coordenada por Vinton Cerf em SRI (Stanford) e Robert Kahn na darpa, entre os anos de 1973 e 1978, desenvolveram o protocolo que proporciona a interconexão e interoperacionalidade de diversas redes de computadores. O nome deste protocolo é o famoso e utilizado até os dias atuais, TCP/IP (Transmission Control Protocol - Protocolo de Controle de Transmissão) (Almeida, 2005, p. 4).

O protocolo TCP/IP é um marco para o desenvolvimento da internet sendo utilizado até hoje, segundo Rubem E. Ferreira:

> O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI), onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas, estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração (Ferreira, 2013, p.23).

Com o surgimento do protocolo TCP/IP as empresas multinacionais e governos abriram o olho para a nova tecnologia que possibilitava redução de custos.

Na década de setenta as companhias de aviação, dentro dos órgãos do governo federal e de muitas empresas multinacionais, surgiu a necessidade de comunicação de dados onde essas empresas eram obrigadas a recorrer às redes de telefonia ou de telex.

A Embratel no ano de 1976 iniciou os testes entre as redes de São Paulo e Rio de Janeiro, nesse período foram instaladas a primeiras redes de comunicação digital do Brasil, operando com circuitos a 4800bps de velocidade máxima. Esse foi o marco da etapa inicial do RNTD, inaugurado oficialmente em 1980, quando passou a se chamar de Serviço Digital de Transmissão de Dados via terrestre (TRANSDATA), inicialmente servindo a trinta cidades (Aguiar, 2001, p34).

HISTORIA DOS CRIMES

Muito se discute quem praticou o primeiro delito informático, para alguns o primeiro delito ocorreu no âmbito do MIT (Massachusetts Institute of Technology), em 1964, onde um aluno teria praticado o cibercrime. Outros dizem que o primeiro caso ocorreu em 1978, na Universidade de Oxford, onde um aluno copiou através da rede de computadores uma prova. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. O primeiro estado americano a fórmula leis sobre crimes informáticos foi a Flórida.

O primeiro Vírus do mundo prejudicou mais de 6 mil computadores no ano

de 1988, foi criado por Robert Morris. Mais tarde veio a ser o primeiro Hacker condenado pela então recém fundada Computer Fraud Act norte-americana. (Jesus, 2016, p. 19).

OS BENEFICIOS DA INTERNET

A tecnologia da informação hoje é para gente como foi a eletricidade ou o motor a época da revolução industrial, pela sua capacidade de distribuir a informação por todo domínio da atividade humana. A internet é a forma organizacional da informação entre organizações que estão distribuídas em todo mundo, assim construindo uma rede mundial de informação.

Pela primeira vez, é possível a comunicação de muitos com muitos em uma escala global, utilizando a internet como meio de comunicação. O uso da internet como sistema de comunicação e organizacional surgiu no último milênio. Principalmente em seu primeiro ano de uso no fim de 1995 com o protocolo de comunicação world wide web (www.),havia cerca de 16 milhões de usuários a rede e no início de 2001, eles já eram superiores a 400 milhões. A quantidade de usuários diz respeito também a qualidade de uso, como atividades econômicas, sociais, políticas e culturais essenciais por todo o planeta estão sendo estruturadas em torno da internet. (Castells, 2001, p. 8).

O aumento das transações utilizando a internet segundo Rodrigo Ventura:

> A Internet já alcançou mais de um quarto dos habitantes do planeta e está presente no cotidiano de seus usuários. Hoje, as pessoas buscam informação pela Internet, encontram outras pessoas pela Internet, se casam e se separam pela Internet, fazem compras, estudam, aprendem e trabalham utilizando a Internet. No futuro, a Internet estará cada vez mais presente na vida das pessoas. E isto também é válido para as empresas (Ventura, 2010, p. 7).

O impacto da internet em âmbito global levou Bill Gates, um dos fundadores da Microsoft, a citar a seguinte frase: “Daqui a algum tempo só existirão dois tipos de empresas: as que estão na Internet e as que não estão em lugar algum.”

CRIMES VIRTUAIS PUROS

Segundo o advogado Marco Aurélio Rodrigues da Costa o conceito de crimes virtuais puros, é "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas."

De acordo com a interpretação de Túlio Lima Vianna:

> Aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). Além do delito de acesso não autorizado a sistemas computacionais há ainda outras modalidades de crimes que têm como objeto a inviolabilidade dos dados informatizados e, portanto, podem ser classificados como delitos informáticos próprios (Viana, 2003, p. 40-41).

Nesses requisitos que se enquadram os chamados “Hackers” que utilizam de alto conhecimento técnico que proporciona meios de burlar sistemas de segurança. Um exemplo de crime virtual puro, seria por exemplo, os ataques de negação de serviço onde o criminoso utiliza de redes zumbis para gerar um grande número de acesso, causando assim a queda do sistema ou uma violação de proteção intelectual que é regulada pela lei 9.609/98.

A lei 12737 tipifica alguns dos tipos de crimes puros:

> Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Lei Nº 12.737**,** 2012).

CRIMES VIRTUAIS IMPUROS

São aqueles que utilizam o computador, celular e outros dispositivos eletrônicos conectados a internet como um meio de realizar uma conduta criminosa. Não é necessário que o infrator da lei seja um Hacker ou pessoa com muito conhecimento na área da informática.

Em 1998, no HC 76.689/PB, relatado pelo então Ministro Sepúlveda Pertence, onde o Supremo Tribunal Federal enfrentava o problema da pornografia infantil por meio da Internet. O Ministro explica que nem todos delitos cibernéticos necessitavam de nova tipificação, pois a tecnologia era apenas um novo meio para a concretização de delitos conhecidos. Vejamos:

> ‘Crime de Computador’: publicação de cena de sexo infanto juvenil (ECA, art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores. Tipicidade. Prova pericial necessária à demonstração da autoria: HC deferido em parte.
> 1. O tipo cogitado – na modalidade de ‘publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente’ – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para

> número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
>
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
>
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial.

DEEPWEB

A DeepWeb ou DarkNet é a parte da internet que não é possível acessar normalmente através dos buscadores convencionais como o Google, Yahoo!, Bing, entre outros. Esses sites são criados com o fim específico de dificultar o acesso a informação, para que uma página apareça nos buscadores normais é necessário que ela seja indexada no padrão dos serviços de busca.

O tamanho da DeepWeb é muito superior a internet convencional e a parte da internet que mais se desenvolve existe conteúdo para todo tipo de demanda ou mercado (Bergman, 2000).

Por ser um meio limitado de acesso por não utilizar os padrões de indexação, pois o conteúdo ali não está em páginas e sim em diversos bancos de dados. O rastreamento que normalmente seria possível caso estivesse na surface (a parte superficial da internet) não é possível na DarkNet. Para acessar os dados da DarkNet é necessário alterar as configurações de redes para acessar a internet, utilizar um navegador específico como por exemplo o Tor (The Onion Router). Os crimes como tráfico de pessoas, drogas e fraudes como comércio de cartões de crédito, são comuns pelo fato de estarem encobertos pelo anonimato (Freitas, 2016).

VESTÍGIOS, EVIDENCIAS, INDÍCIOS TECNOLÓGICOS

As palavras vestígio, indício e evidência, embora pareçam sinônimas, têm significados diferentes na ciência criminal e no Código Penal Brasileiro.

Vestígio: é qualquer sinal, objeto ou marca que possa, supostamente, ter relação com o fato criminoso;

Evidência: é o vestígio que após analisado tecnicamente pela perícia, constata-se ter ligação com o crime;

Indício: de acordo com o Artigo 239 do Código de Processo Penal, considera-se indício a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra (s) circunstância (s).

Nos crimes cometidos com recursos tecnológicos que envolvem a Internet, pois a maioria dos provedores de acesso e de serviços da rede mundial de computadores mantém em um histórico denominado "registros de eventos" ou "LOGs" (diário de bordo, em inglês) de cada um de seus usuários.

Ao serem resgatados, os LOGs geralmente apontam para um endereço de Internet, denominado endereço IP (Internet Protocol), que pode identificar o endereço físico da conexão que o usuário utilizou para acessar a rede na data e horário do fato delituoso.

Em praticamente todos os casos de investigação envolvendo recursos tecnológicos haverá a possibilidade de rastrear a origem e descobrir a localização física do terminal de computador, notebook, tablet, smartphone, celular, GPS ou outro recurso utilizado pelo (s) criminoso (s) ou vítima (s).

Até mesmo os criminosos que têm um maior grau de conhecimento, na maioria das vezes, descuidam-se num dado momento, deixando algum registro que possa identificá-los ou que possa ser juntado a outras informações nesse sentido.

Por outro lado, se o criminoso é leigo em tecnologia, provavelmente a investigação será facilitada, uma vez que ele certamente nem saberá que está deixando vestígios que irão identificá-lo numa futura investigação (SENASP, 2018).

INVESTIGAÇÃO

Os membros de uma equipe de investigação devem criar contas falsas de

vários serviços na Internet, tais como e-mail, bate-papo, chats, redes sociais, entre outras, para utilizar nos momentos de investigação

As contas falsas devem utilizar dados pessoais compatíveis com o perfil criado e utilizar fotografias que passem uma imagem real. A equipe de investigação tem que criar uma Estória Cobertura (EC), Estória Cobertura (EC) - termo utilizado em Inteligência Policial para expressar uma estória falsa, criada por um agente investigador infiltrado no ambiente criminoso com intuito de obter informações sobre o crime e o criminoso que cubra todas as possibilidades de questionamento de um investigado com o qual manterá contato na Internet, mas que, ao mesmo tempo, não exponham pessoas inocentes investigação.

O tratamento dado pelas autoridades com relação a crimes onde o autor utiliza malwares para atingir o objetivo é tentar rastrear a origem do crime analisando as ações do malware passo-a-passo. Esse tipo de análise é feito em ambiente virtual isolado e exclusivamente preparado para esse fim. Por isso, a ação deve ser tomada somente por pessoas especializadas, tais como peritos criminais da área de informática ou especialistas na área que disponham de toda a infraestrutura necessária.

As ferramentas mais úteis nesse caso são os softwares que analisam quais arquivos e registros do sistema operacional são acessados pelo malware e os “sniffers”, (SNIFFER é um aplicativo capaz de capturar e registrar - podendo até analisar - o conteúdo dos datagramas que trafegam na rede ou em pontos específicos dela. Eventualmente podem ser utilizados para fins criminosos) que são verdadeiros farejadores ou analisadores de tráfego de rede que possibilitam um estudo detalhado (bit-a-bit) da parte de tráfego suspeito.

Essas ferramentas vão ajudar a autoridade a identificar qual o ponto de comunicação do malware com o mundo exterior, ou seja, para onde ele envia as informações que colhe. Pode ser uma conta de e-mail, um servidor de arquivos, um banco de dados clandestino, um site na Internet ou qualquer aparato que possa guardar as informações furtadas de forma segura para que sejam acessadas posteriormente pelo criminoso. Esse trabalho é denominado “análise comportamental do malware”. Além disso, também pode ser efetuada, com ferramentas específicas, a chamada “engenharia reversa”, que é a análise do código do software para entender seu funcionamento. (SENASP, 2018).

.

RESULTADOS E DISCUSSÃO

O Código Penal e suas alterações como a lei 12737 incide o tema Crimes Virtuais, baseiam-se em duas teorias que seriam Crimes Virtuais Puros e Crimes Virtuais Impuros. O que diferencia um do outro é o meio o qual o criminoso utiliza para executar a sua ação.

Os crimes virtuais puros são novos tipos penais que surgiram para cumprir lacunas nas leis atuais e que só podem ser executados exclusivamente com a utilização de algum meio eletrônico. A lei 12737 tipifica o crime de invasão de dispositivos eletrônicos, porém não contribui em nada para a investigação dos crimes virtuais, a necessidade de obtenção do endereço IP dos provedores é sanada apenas por ordem judicial o que prejudica as investigações.

Falando sobre Crimes virtuais puros são aqueles que utilizam as tipificações penais existentes a época e que transforma o computador o celular ou outro meio eletrônico apenas em um meio para cometimento de crimes. O Ministros Sepúlveda Pertence, em 1998, no HC 76.689/PB, explica que não é pelo fato da tecnologia empregada para o cometimento do crime surgir posteriormente a tipificação penal que a lei não será aplicada.

Tratando-se de crimes virtuais que utilizam a DeepWeb a investigação é mais complexa principalmente pelo uso do Tor pelos infratores. O Tor é uma ferramenta de código aberta feita para acessar o conteúdo da DeepWeb garantindo o anonimato. Por garantir o anonimato e a impossibilidade de rastreamento é a rede mais utilizada para compra de armas de fogo, drogas, órgãos e inúmeras outras mercadorias que são consideradas ilegais no Brasil.

O motivo da impossibilidade de rastreamento em casos que envolve a DeepWeb e o Tor é pelo fato da impossibilidade da utilização dos logs para o rastreamento, pois os roteadores são os computadores de usuários comuns. As investigações nesses casos devem ser de forma a analisar contas de usuários e se infiltrar no ambiente criando contas falsas em diversas redes sociais.

CONCLUSÃO

O desenvolvimento tecnológico trouxe inúmeras melhorias a vida das pessoas, principalmente na agilidade em que as questões são resolvidas. Os responsáveis pela segurança publicam também tiveram que evoluir e combater os novos tipos de crimes e os crimes comuns, porem agora no mundo virtual, onde a falsa sensação de anonimato faz com que as pessoas tomem ações que talvez não as tomariam no mundo real.

Inúmeros crimes apenas mudaram de lugar sem a necessidade de criação de uma nova legislação, porem outros vieram com o desenvolvimento tecnológico se fazendo necessário a elaboração e aperfeiçoamento da nossa legislação.

Um dos objetivos desse estudo foi mostrar que crimes praticados em ambientes virtuais são sim passiveis de punição e a identificação do autor, existem algumas técnicas que possibilitam o rastreamento e a identificação, contudo não é possível que alguém de conhecimento um pouco avançado consiga praticar crimes sem sequer ser identificado.

A DeepWeb é um ambiente que dificilmente possibilitará a identificação do autor, principalmente pela forma que a sua rede é estruturada dificultando e muito a localização. O comercio de itens ilegais como: drogas, armas, pessoas e a mais variada quantidade de itens, a rede se torna muito atrativa as atividades criminosas.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, José Maria Fernandes, Breve história da INTERNET, Out-2005. <http://repositorium.sdum.uminho.pt/handle/1822/3396>

Ferreira, Rubem E. In: Novatec. Linux: Guia do Administrador do Sistema. Janeiro de 2013 2ª edição.

Aguiar, Sonia e Dantas, Vera, 2001, Memórias do computador: 25 anos de informática no Brasil, São Paulo, IDG.

Jesus, Damásio de Manual de crimes informáticos / Damásio de Jesus, José Antonio Milagre. – São Paulo : Saraiva, 2016.

Castells, Manuel, A galáxia da Internet, Reflexões sobre a internet, os negócios e a sociedade, 2001.

Ventura, Rodrigo, Mudanças no Perfil do Consumo no Brasil: Principais Tendências nos Próximos 20 Anos, 2010.

Felipini, D. “A Era da Internet”. Ecommerce, 2006. Acessível em: <http://www.e-commerce.org.br/Artigos>.

Marco Aurélio Rodrigues da Costa. Crimes de informática. In: Revista Eletrônica Jus Navigandi. <http://www.jus.com.br/doutrina/crinfo.html.>.

Túlio Viana. Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

Lei 12737 de 2012, Artigo 154A. CP. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

Ministro Sepúlveda Pertence, HC 76.689/PB de 1998.

Bergman, Michael K. "The Deep Web: Surfacing Hidden Value". < http://dx.doi.org/10.3998/3336451.0007.104 >.

Victor de Freitas Bernardes, Dos Crimes Virtuais Cometidos se Utilizando da Deep Weeb, 2016.

SENASP, Crimes Virtuais, 2018.