REFLEXÕES SOBRE OS CIBERCRIMES E SUA COMPETÊNCIA

Eliel GERALDO Filho[1]
Gabriel VIDEIRA da Silva[2]

RESUMO: A presente pesquisa bibliográfica teve por objeto os cybercrimes, em um primeiro momento buscou-se conceituar esses crimes, bem como explicar um panorama geral de seu funcionamento, pontuando algumas classificações e casos emblemáticos, posteriormente discutiu-se a disciplina legal no Direito Brasileiro, findando com uma análise da competência atinente a esses crimes no âmbito nacional.

Palavras-chave: Internet**,** Cibercrimes, Legislação, impunidade, competência.

1 INTRODUÇÃO

O objetivo do presente trabalho é explicar os cibercrimes e discutir acerca deste problema que causa danos no mundo todo, trazendo conceitos e classificações bem como discutir acerca da competência jurídica brasileira.

Na primeira parte busca-se ilustrar sinteticamente do surgimento da internet no Brasil e suas consequências, logo mais busca-se ilustrar o que são os cibercrimes, trazendo conceitos e classificações e os problemas que eles causam, apresentando também alguns exemplos de cibercriminosos que causaram enormes danos e despesas com seus atos.

Na segunda parte trazemos a base legal que engloba os cibercrimes e como surgiu no Brasil a Lei Carolina Dieckmann ajudando na tentativa de combater estes delitos, em seguida expondo discussões acerca da competência para julgar os cibercrimes, tanto em território nacional como internacional.

Por fim a conclusão acerca do que foi demonstrado e discutido no presente artigo.

2. Breve explicação acerca da internet

[1] Discente do 3º ano do curso de Direito do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente. eliellsgfilho@gmail.com
[2] Discente do curso de Direito do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente.gabvs97@hotmail.com

A internet, uma rede que interliga milhões de computadores ao redor de todo o hemisfério, possui um papel extremamente relevante na sociedade atual. Sua história no Brasil se inicia 1988 por iniciativa da comunidade acadêmica de São Paulo (Fapesp) Fundação de Amparo à Pesquisa do Estado de São Paulo) e Rio de Janeiro UFRJ (Universidade Federal do Rio de Janeiro) e LNCC (Laboratório Nacional de Computação Científica), mas sua real exploração no âmbito comercial ocorreu em 1994 com um piloto realizado pela Embratel, mais tarde diferentes empresas de telefonia e comunicação criaram tecnologias para propagar o acesso.

Esta realização, trouxe infinitas possibilidades e realizações, tornando-se imprescindível á inúmeros trabalhos, com um acesso rápido e fácil á pesquisas, comunicação, entretenimento e etc., contudo também facilitou a pratica de crimes cibernéticos. Tamanho é o perigo que isso causa e pode causar que cabe ao nosso ordenamento se adaptar afim de conter tal ameaça garantindo a todos que a usem não sejam prejudicadas e que os infratores tenham punições apropriadas ao dano causado.

2.1. Conceitos de cibercrimes e problemáticas

O cibercrimes em sua definição literal é “o nome dado aos crimes que envolvam qualquer atividade ou prática ilícita na rede”. Dentre a definição citada existem inúmeras classificações, uma utilizada por vários autores diz que os cibercrimes se subdividem em próprios e impróprios. Os cibercrimes próprios são novos delitos praticados contra a informática como por exemplo: violação de e-mail, danos causados por vírus, pirataria de softwares e etc... Enquanto por outro lado os crimes impróprios já se encontram tipificados no código penal, como por exemplo falsidade ideológica, estelionato, calunias difamações e dentre outras, contudo o seu meio para realização se encontra diferente sendo estes agora praticados no ambiente virtual [Neto and Guimaraes 2003, Bueno and Coelho 2008, Redivo and Monteiro 2009].

Nota-se que estes crimes não podem ser realizados por qualquer um, mas sim por alguém com grande conhecimento de informática, também conhecidos como Hackers.

O hacker pode ser apenas um indivíduo ou grupos organizados, estes se aproveitam do sistema pelo fato de que podem praticar inúmeras condutas ao mesmo tempo e em lugares diferentes, tirando proveito do anonimato e do difícil rastreio de suas façanhas, causando danos a milhares de pessoas e empresas.

Para que seja possível combater essa ameaça faz-se necessário profissionais qualificados para conte-los, contudo não só no Brasil como no mundo inteiro isso ainda é escasso.

Tamanha é a dificuldade de prender esses criminosos, que o FBI quer contratar “Hackers éticos” para serem ciberagentes especiais, pois, a lógica é que para combater um hacker você precisa ser um, além do mais algumas faculdades estão implementando cursos voltados para uma formação especifica para criar indivíduos que atuariam na área de segurança virtual e administradores de sistema como é o caso da Faculdade de Informática e Administração Paulista (Fiap).

2.1.1. Dos ataques dos cibercrimes e seus danos

Apesar de o alvo dos cibercriminosos serem geralmente pessoas comuns, muitas empresas, governos e até zonas militares já foram alvos de ataques cibernéticos. Casos mais famosos como o de Kevin Mitnick, o mais conhecido hacker da atualidade, que em 1990 invadiu várias operadoras de telefonia e provedores de internet tornando-se um dos cibercriminosos mais procurados do mundo, foi preso 5 anos após estes acontecimentos.

Albert Gonzales também um hacker foi acusado de realizar o maior roubo de cartões já registrado. Entre 2005 e 2007, o grupo que Gonzalez liderava vendeu mais de 170 milhões de números de cartões. Ao ser preso a polícia havia encontrando mais de 1,6 milhões de dólares enterrado no quintal de sua casa.

Com apenas 15 anos, Jonathan James foi o primeiro adolescente a ser preso por crimes digitais. Em 1999, nos EUA, ele hackeou os computadores da Nasa

e do Pentágono coletando usuários e senhas dos dois sites, roubou um software de quase 2 milhões de dólares e interrompeu milhares de mensagens sigilosas. Este se suicidou em 2008.

Considerado como o pai dos Vírus para computadores Robert Morris Morris criou um vírus que prejudicou cerca de 6 mil computadores, em 1988, mais ou menos 10% dos computadores que existiam na época causando prejuízos superiores a 15 milhões de dólares foi condenado, mas não chegou a cumprir pena. Este hoje trabalha em um dos maiores centros de inteligência dos Estados Unidos.

Um caso que teve grande destaque no Brasil, a ponto de ser aprovada uma lei para a tipificação da conduta, foi o ataque de Hackers ao e-mail pessoal da Atriz Anna Dieckman, onde foram divulgadas diversas fotos intimas da atriz.

3 CYBERCRIMES NO BRASIL

3.1 Breve Introdução

Os cybercrimes aterrorizam o mundo todo, no Brasil, segundo a Revista Galileu[3] esse tipo de crime faz cerca de 28,3 milhões de vítimas anuais, cerca de 75% dos brasileiros conectados. Segundo a mesma revista, não só no número de vítimas que o país se destaca, os “criminosos virtuais” do país também ganham destaque no mundo, sendo a 4ª maior fonte de malawares do planeta.

Esses crimes não só fazem vítimas muitas vítimas no Brasil, como possuem alto custo e tempo de solução, segundo relatório da Norton[4], em nosso país a solução dos cybercrimes leva em média 43 dias e custa aos cofres públicos mais de 1.400 dólares.

3.2 Base Legal

[3]https://noticias.bol.uol.com.br/bol-listas/10-famosos-hackers-do-mal-do-mundo.htm
4http://revistagalileu.globo.com/Revista/Common/0,,EMI320627-17770,00 CYBERCRIME+FAZ+MILHOES+DE+VITIMAS+NO+BRASIL+TODOS+OS+ANOS.html>

A base constitucional do chamado “direito a informática pode ser atribuída às pilastras do direito à informação, considerando isso, tem-se os dispositivos insculpidos na constituição, como art.5º IV que assegura a livre manifestação de pensamento vedando o anonimato, o V que assegura o direito de resposta, o IX que assegura a liberdade de expressão, o XIV que permite o livre acesso à informação, bem como o sigilo de fonte, e a própria regulação do Habeas Data. Todas essas questões se aplicam claramente ao cenário virtual, e demonstram de forma tímida que há um alicerce constitucional mínimo para resguardar os usuários virtuais.

Antes de 2012, o Brasil carecia de legislação específica para regulamentação dos crimes virtuais, então a solução encontrada pelos tribunais foi pacificar entendimentos de forma a enquadrar os cybercrimes dentro da legislação vigente, a principal forma para isso, foi considerar que a maioria dos crimes virtuais não são crimes específicos, como anteriormente explicado, existem os cybercrimes impróprios, de forma que o ambiente virtual se apresenta apenas como um meio para execução desses crimes, logo por essa lógica cerca de 95% dos crimes já estariam tipificados em nosso Código Penal.

Nessa lógica de aproveitar o que temos, o STJ[5] pacificou inúmeros entendimentos, como considerar que o envio de pornografia infantil pelo e-mail e âmbitos digitais era abarcado pelo art.241 da Lei 8069/90, também pacificou a questão do enquadramento das transferência bancárias mediante fraude virtual, que para o STJ[6] é considerado furto qualificado mediante fraude e não estelionato, dentre outras adequações dos dispositivos. Em esfera de sanção cível também não é incomum a concessão de danos morais em virtude de crimes contra honra que ocorreram pelo meio virtual.

A situação da legislação brasileira sobre crimes cibernéticos ganhou um novo capítulo a partir de 2012, com a aprovação da Lei 12.737/2012, mais conhecida como “Lei Carolina Dieckmann”, tal nome se dá em virtude do ataque de hacker a caixa de e-mails da atriz Carolina Dieckmann, os hackers em maio de 2012 após a invasão buscaram extorquir a atriz pedindo R$ 10,000,00 para que fotos

[5] https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual
[6] https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual

intimas não fosse divulgadas, o pagamento não foi realizado, de forma que os criminosos soltaram 36 fotos de Carolina na internet,[7] com esse caso e com a fama de que o congresso trabalha quando gente importante se torna vítima, ocorreu então a aprovação dessa lei.

A Lei Carolina Dieckmann acrescentou art.154-A[8] ao Código Penal, tal dispositivo tipifica o crime conhecido como "Intrusão Informática"[9], vejamos a redação do dispositivo:

> 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 obtidos. § 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."

Tal crime como observado por Masson, consiste em crime formal[10] que visa proteger a liberdade individual e a "inviolabilidade dos segredos", o crime claramente como se vê na redação visa coibir os ataques hackers à informações e arquivos pessoais com finalidade de obter vantagens ilícitas como os 10 mil reais

---

[7] http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html
[8] http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm
[9] Masson, Cleber. Direito Penal Esquematizado, p.331, 2016.
[10] Masson, Cleber. Direito Penal Esquematizado, p.331-334, 2016.

que os criminosos almejavam quando extorquiram a atriz Carolina Dieckmann. O artigo 154-B também acrescentado pelo dispositivo em discussão, colocou que o crime do 154-A de possui ação penal pública condicionada a representação, com exceção de quando o crime for praticado contra a administração pública direta ou indireta.

Além disso a Lei Carolina Dieckmann alterou a redação do artigo 266 do Código Penal[11], acrescentando o §1º ao dispositivo possibilitando que a conduta de interrupção ou de perturbação de "serviço telemático" ou "serviço de utilidade pública", donde estão inseridas a figura da internet, seja abarcada pelo crime do 266.[12]

Por fim a última alteração trazida pela Lei 12.737/12 foi a inserção o parágrafo único ao artigo 288 do Código Penal, inserindo ao crime de falsificação de documento particular, as condutas de falsificar de crédito ou débito, equiparando esses a figura do "documento particular" citado pelo caput.

A QUESTÃO DA COMPETÊNCIA NOS CYBERCRIMES

É sabido que o Estado divide a prestação jurisdicional em parcelas, e que a essas parcelas do poder jurisdicional distribuídas entre os órgãos do judiciário, dá se o nome de competência.

Vários critérios são utilizados para a determinação da competência, dentre eles, os principais são: da matéria, da pessoa e do território.

A regra principal de estabelecimento da competência territorial no Processo Penal é, segundo o artigo 70, caput, do Código de Processo Penal, o local em que se consumou o delito.

Quanto a competência dos cybercrimes a disciplina legal é escassa no ordenamento jurídico brasileiro, ante a isso muito do pensamento sobre a competência dos crimes digitais é ditada pelo pensamento jurisprudencial. O grande problema é que os crimes digitais têm ligação com a rede mundial de computadores, e isso torna difícil a determinação do local da prática do delito, pois, muitas vezes os

[11] http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm
[12] http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html

“provedores” que hospedam determinado site onde ocorrerem os atos delitivos estão no exterior, ou o indivíduo se valeu de recursos parar burlar a sua localização, ou ainda na maioria dos casos o crime ganha conotação de plurilocal, já que a ação pode partir em provedor x e o resultado ocorrer em provedor de localização y.

O STJ no CC 97201/RJ, entendeu que a competência nos crimes digitais segue a premissa maior do art.70 do Código de Processo Penal, sendo o local da consumação tido como local onde se hospeda o servidor, vejamos a ementa:

> **Ementa:** CONFLITO NEGATIVO DE COMPETÊNCIA. QUEIXA-CRIME. CALÚNIA PRATICADA, EM TESE, POR JORNALISTA. CARTA PUBLICADA EM BLOG. LEI DE IMPRENSA. NORMA NÃO RECEPCIONADA PELA CONSTITUIÇÃO DE 1988. ART. 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DO JUÍZO SUSCITADO. 1. Não recepcionada a Lei n. 5.250/1967 pela nova ordem constitucional (ADPF n. 130/DF), às causas decorrentes das relações de imprensa devem ser aplicadas as normas da legislação comum, inclusive, quanto à competência, o disposto no art. 70 do Código de Processo Penal. 2. O crime de calúnia (art. 138, caput, do Código Penal) consuma-se no momento em que os fatos "veiculados chegam ao conhecimento de terceiros" (CC n. 107.088/DF, Relatora Ministra Maria Thereza de Assis Moura, DJe de 4/6/2010). 3. Tratando-se de queixa-crime que imputa a prática do crime de calúnia em razão da divulgação de carta em blog, na internet, o foro para processamento e julgamento da ação é o do lugar de onde partiu a publicação do texto tido por calunioso. 4. In casu, como o blog em questão está hospedado em servidor de internet sediado na cidade de São Paulo, é do Juízo da 13ª Vara Criminal dessa comarca a competência para atuar no feito. 5. Conflito conhecido para declarar competente o suscitado.

A questão, porém, suscita muita discussão como dito, principalmente pelo fato de que muitos provedores se encontram localizados fora do país, como solucionar esses problemas? A lei não resolve isso diretamente, portanto ganha status especulativo e depende no mínimo de uma pacificação e manifestação jurisprudencial. Uma solução que alguns artigos científicos e que inclusive é trazida em artigo da Rede de Ensino Luiz Flávio Gomes[13], seria utilizar toda disciplina dos parágrafos do art. 70[14] do Código de Processo Penal consoante a plurilocalidade dos crimes, vejamos o que tal dispositivo coloca:

---

[13] https://lfg.jusbrasil.com.br/noticias/2659329/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site

[14] http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3o Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.

E também ainda como dispõe o artigo[15], a disciplina do artigo 88, vejamos:

> Art. 88. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.

O entendimento não é pacífico, no entanto percebe-se que de regra a atribuição de competência dos cybercrimes segue uma conotação principalmente do critério territorial.

Ainda existem discussões se a competência para julgar os crimes virtuais seria apenas da Justiça Federal, já que alguns artigos científicos remetem ao fato do art.109 da Constituição de 1988[16] incisos IV e V, principalmente no inciso IV que diz ‘’ os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União”, pelo fato da internet ser um serviço de caráter nacional, isso traria o interesse da União levando a entender que a competência seria exclusiva.

Não vamos esgotar a presente discussão, mas ao nosso leigo ver, a questão de atribuição ou não da competência da justiça federal ou até das justiças especializadas no que concerne os cybercrimes, deve atender as regras do caso concreto e até as diretrizes comuns de competência, já que como dissemos, 95%

[15] https://lfg.jusbrasil.com.br/noticias/2659329/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site

[16] http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

dos crimes virtuais são crimes comuns em que o ambiente virtual é apenas o meio, logo, se determinado crime, ou agente que praticou o cibercrime, preencher requisitos para figurar na Justiça Federal ou em Justiça Especializada, que vá o processo para essa, do contrário utiliza-se a residualidade da Justiça Comum Estadual.

3 CONCLUSÃO

A primeira conclusão que pudemos chegar é que os cybercrimes apresentam-se como um perigo ao mundo todo, e que ainda é escasso no mercado profissionais aptos a combater e investigar esses crimes.

Também foi possível compreender que os crimes cibernéticos podem ser divididos em próprios (crimes exclusivos do meio virtual), ou impróprios, que constituem a maioria desses crimes, já que o ambiente virtual se projeta como um meio para esse delito.

Foram demonstrados os principais casos e vimos que no Brasil mais de 70% dos usuários acabam sendo vítimas de práticas criminosas todos os anos, dentro da ótica nacional de análise foi possível compreender que a legislação sobre o tema ainda é muito escassa.

No entanto tal escassez não significa baderna, já que como a maioria dos crimes cibernéticos são impróprios, é possível a utilização da própria regulação dos crimes em sua forma comum, adequando ao caso. A Lei 12.737/12 trouxe grande contribuição para o cenário brasileiro, já que auxiliou na tipificação dos “sequestros de dados” e das invasões a e-mails e bancos de dados.

Por fim, foi possível ter um panorama geral da questão da competência nos crimes cibernéticos, foi possível entender por exemplo que a grande discussão se situa no âmbito da competência territorial, já que muitos provedores ficam localizados no exterior e também pela questão de que na maioria das vezes os crimes cibernéticos são plurilocais, envolvendo mais de uma base territorial, nesse sentido alguns julgados vem trazendo a aplicação da regra do artigo 70 do CPP, sendo competente o foro do local onde se situa o provedor. Em alguns casos, no

entanto de extraterritorialidade a jurisprudência ainda não tem caráter pacífico, parecendo razoável a aplicação das outras regras disciplinadas no art.70 do CPP bem como as regras do art.88.

Por fim, no campo da competência, vimos que há um certo pensamento, de que os crimes virtuais seriam sempre de competência da Justiça Federal, pois, a internet seria um serviço que interessaria a coletiva e à união, se enquadrando nas disposições do 109. Nesse sentido, em opinião própria descordamos um pouco de tal posição, já que cada caso deve ser analisado de forma específica, pois, a maioria dos crimes cibernéticos o meio virtual é apenas um meio (cibernéticos impróprios), então se o caso couber foro específico, que se aplique, do contrário deveria ser suscitada a competência residual da justiça estadual.

REFERÊNCIAS BIBLIOGRÁFICAS

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

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diario Oficial Rio de Janeiro:

BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Diário Oficial da União, Brasília.

<http://brasilescola.uol.com.br/informatica/internet-no-brasil.htm> Acesso em 27 de agosto de 2017

<http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html> Acesso em 27 de agosto de 2017

<http://g1.globo.com/tecnologia/noticia/2013/07/hackers-sao-acusados-em-maior-cibercrime-da-historia-nos-eua.html> Acesso em 27 de agosto de 2017

<http://revistagalileu.globo.com/Revista/Common/0,,EMI320627-17770,00CYBERCRIME+FAZ+MILHOES+DE+VITIMAS+NO+BRASIL+TODOS+OS+ANOS.htl> Acesso em 27 de agosto de 2017

<http://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos> Acesso em 27 de agosto de 2017

<http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html> Acesso em 27 de agosto de 2017

<http://www.egov.ufsc.br/portal/sites/default/files/a_internet_e_o_direito_uma_abordagem_sobre_cibercrimes.pdf>Acesso em 27 de agosto de 2017

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em 27 de agosto de 2017

<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em 27 de agosto de 2017

<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm.> Acesso em 27 de agosto de 2017

<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm> Acesso em 27 de agosto de 2017

<https://canaltech.com.br/seguranca/O-que-e-cibercrime/> Acesso em 27 de agosto de 2017

<https://lfg.jusbrasil.com.br/noticias/2659329/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site> Acesso em 27 de agosto de 2017

<https://lfg.jusbrasil.com.br/noticias/2659329/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site> Acesso em 27 de agosto de 2017

<https://noticias.bol.uol.com.br/bol-listas/10-famosos-hackers-do-mal-do-mundo.htm> Acesso em 27 de agosto de 2017

<https://olhardigital.com.br/fique_seguro/noticia/faculdade-paulista-ministra-curso-para-hackers/8493> Acesso em 27 de agosto de 2017

<https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual> Acesso em 27 de agosto de 2017

>https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual> Acesso em 27 de agosto de 2017

Lei 12.737/2012, sancionada em 30 de novembro de 2012 **Lei Carolina Dieckmann**

Masson, Cleber. Direito Penal Esquematizado, p.331, 2016.

Masson, Cleber. Direito Penal Esquematizado, p.331-334, 2016.

CENTRO UNIVERSITÁRIO “ANTONIO EUFRÁSIO DE TOLEDO” de Presidente Prudente. **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.