

Crimes Virtuais

Rodrigo de Mello Vidal

Rio de Janeiro
2015

CRIMES VIRTUAIS

Rodrigo de Mello Vidal

Pós-Graduado em Direito Público pela
Universidade Candido Mendes – Centro – Rio
de Janeiro

Resumo: O direito evolui junto com a sociedade, e com o avanço tecnológico e sua inserção no cotidiano dos indivíduos surgem diversas consequências para a sociedade, cabendo ao direito regular essas novas relações. Diversos usuários utilizam-se da tecnologia para cometer atos ilícitos, os chamados crimes virtuais, ou seja, aqueles crimes praticados no ambiente virtual. A legislação nem sempre consegue acompanhar a tecnologia, os aplicadores do Direito tentam enquadrar, na medida do possível, esses atos lesivos aos tipos penais previstos no Código Penal e na legislação penal esparsa, mas se faz necessário legislação específica para regular o tema. A essência desse trabalho é analisar os crimes virtuais, verificando os principais aspectos envolvidos na prática de tais crimes, demonstrando suas peculiaridades e como o ordenamento jurídico pátrio vem regulando esses crimes.

Palavras-chave: Crimes Virtuais. Direito da Informática. Internet. Tecnologia.

Sumário: Introdução. 1. A tecnologia e o surgimento dos crimes virtuais. 2. Crimes Virtuais. 3. Legislação aplicável nos crimes virtuais. Conclusão. Referências.

INTRODUÇÃO

O referido artigo científico dissertará sobre crimes virtuais que são atos ilícitos praticados por intermédio de dispositivos tecnológicos (computadores, smartphones, tablets e etc), com objetivo de demonstrar a realidade jurídica dos crimes virtuais no ordenamento jurídico brasileiro, analisando os principais aspectos envolvidos na prática de tais crimes, costumeiro na sociedade atual.

O primeiro capítulo deste artigo científico se propõe a analisar a tecnologia e o surgimento dos crimes virtuais, visando demonstrar como as novas tecnologias contribuíram no processo de globalização, aumentando a comunicação e troca de informações entre os indivíduos, interferindo diretamente na problemática dos crimes virtuais.

A segunda parte visa analisar os crimes virtuais, passando pelo conceito, os principais aspectos e peculiaridades do crime, formas de classificação, demonstrando ainda os crimes virtuais mais comuns.

No terceiro capítulo, o trabalho trata da legislação e da interpretação da jurisprudência sobre o tema, abordando as leis já editadas e modificações trazidas, além das inovações jurídicas sendo discutidas e o posicionamento adotado pela jurisprudência sobre os crimes virtuais.

O presente artigo científico busca analisar os crimes virtuais, dissertando sobre o seu surgimento, legislação aplicável e interpretação da doutrina e jurisprudência sobre o tema.

1. A TECNOLOGIA E O SURGIMENTO DOS CRIMES VIRTUAIS

O desenvolvimento das novas tecnologias facilitou a globalização econômica, social e cultural fazendo com que as distancias se encurtassem, aumentando a comunicação entre as pessoas.

A relação entre as pessoas cada dia mais se dá através de dispositivos tecnológicos; as tarefas que eram realizadas em longos espaços de tempo, agora podem ser realizadas de forma instantânea, tornando esses dispositivos indispensáveis, e passando a fazer parte do dia a dia das pessoas, das empresas e dos governos.

A internet, conhecida como rede mundial de computadores, foi o alicerce principal dessa expansão permitindo a comunicação simultânea entre indivíduos de qualquer lugar do mundo.

Num breve histórico, a origem da internet se deu na década de 1960 com o Governo dos Estados Unidos no combate a guerra fria, a fim de evitar que informações fossem perdidas num possível ataque sofrido a um de seus departamentos. Surge assim a internet para ajudar a troca de informações de maneira rápida entre seus órgãos.

O uso da internet seguiu restrito aos centros de pesquisas até a década de 1980, quando, finalmente, teve seu uso comercial liberado, atingindo diversos usuários e praticamente todos os meios de comunicação, trazendo inúmeros benefícios para a população mundial.

O desenvolvimento de novas tecnologias, interfaces de comunicação sem fios, e o uso integrado de dispositivos portáteis como notebooks, smartphones, tablets, dentre outros facilitou ainda mais esse processo de globalização, permitindo o acesso à internet e a troca imediata de informações.

No entanto, ao separar as pessoas por uma interface e proporcionar o anonimato, a internet e o mundo virtual aumentaram a sensação de liberdade do ser humano. Essas mudanças, impulsionadas pelos avanços tecnológicos e pelas mídias digitais, fizeram surgir novos paradigmas para a sociedade pós-moderna e para os sistemas que a organizam e regulam, como o Direito.

Hoje milhares de pessoas permanecem por vezes mais tempo navegando na internet do que vivendo o mundo real, e a rede mundial de computadores é acima de tudo uma rede mundial de indivíduos, onde existem relações jurídicas fluindo.

O direito deve trazer soluções para os litígios que venham a ocorrer dentro deste ambiente virtual. Ele é a solução prática de planejamento e estratégia que só pode ser feita em equipe, num contato direto com as demandas e a própria evolução da sociedade. O direito deve adaptar-se as demandas, aos anseios da sociedade, onde as transformações são cada vez mais rápidas.

Com essas tecnologias e a internet disponibiliza na rede, uma quantidade enorme de informações pessoais, ficando à disposição de milhares de pessoas que possuem acesso à internet. Essa facilidade de acesso à informação fez surgir também novas formas de violação de bens jurídicos protegidos pelo ordenamento, os quais passaram a ser realizados não só no plano físico, mas, também no plano virtual, através de usuários que cometem crimes na rede que são os denominados Crimes Virtuais.

O crime virtual, numa breve definição, é aquele praticado no ambiente virtual, a internet pode ser tanto ambiente propício para a consumação de crimes, quanto para a realização de seus atos preparatórios.

No intuito de compreender e, conseqüentemente, encontrar meios de reprimir estes novos delitos, surge um novo ramo jurídico especializado nesses crimes virtuais, já que Código Penal é de 1940, época em não havia essas tecnologias, o que torna claro a deficiência em combater tais crimes, devendo-se utilizar além dos princípios gerais do direito penal a legislação especial para combater tais condutas.

Novas relações sociais passaram a surgir nesta era digital, razão pela qual o direito deve se adaptar a esta nova realidade, visando combater essas infrações penais praticadas no ambiente virtual.

2. CRIMES VIRTUAIS

Para Capez crime pode ser conceituado sob três aspectos diversos, quais sejam: a) material – sob esse enfoque crime é “todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social”; b) - formal – sob esse enfoque “o crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo”; e c) analítico – nesse enfoque que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime, o conceito é: “todo fato típico ilícito”¹

De acordo com a doutrina majoritária, o conceito analítico de crime o define como um fato típico, antijurídico e culpável, e da noção de que a tipicidade, a conduta, o resultado e o nexos causal, formam o fato típico, excluído qualquer desses elementos não se há de falar em crime.

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia. Os crimes virtuais têm outras nomenclaturas, como por exemplo, crime digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática,

¹ CAPEZ, Fernando. Curso de direito penal: parte geral. 18ª edição. São Paulo: Saraiva, 2014.

delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. Sendo assim é difícil determinar o crime virtual, tendo em vista que existem muitas situações complexas no ambiente virtual.

Através do conceito analítico finalista de crime, pode se chegar à conclusão de que crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática.

A Organização para a Cooperação Econômica e de Desenvolvimento (OECD) propôs uma definição ampla, conceituando esse tipo de crime como sendo “qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados.”²

Já Sérgio Marcos Roque conceitua crimes cibernéticos como sendo "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material."³

Para melhor compreender os crimes virtuais faz-se necessário entender um pouco mais a fundo esse ambiente virtual. Na informática existe usuários chamados “crackers” que visando diminuir a segurança dos computadores e, por consequência, da própria internet, observa-se a utilização de diversos mecanismos que se dispõem, sobretudo, ao compartilhamento de dados sem o consentimento do seu legítimo detentor, ou seja, invade os computadores com a finalidade de causar danos, de cometer ilícitos, de se aproveitar das falhas existentes no sistema para obter vantagem indevida.

Nesse aspecto, merecem destaque os métodos usados para a invasão nos computadores ou sistemas de informática: a) Spamming – conduta de mensagens publicitárias por correio eletrônico para uma pequena parcela de usuários; b) Cookies – são arquivos de texto que são gravados no computador de forma a identificá-lo. Assim, o site obtém algumas informações, tais como quem está acessando o site, com que periodicidade o usuário retorna à página da web e outras informações almejadas pelo portal; c) Spywares – são programas espões que enviam informações do computador do usuário para desconhecidos na rede; d) Hoaxes – são e-mails, na maioria das vezes com remetente de empresas importantes ou de órgãos governamentais, contendo mensagens falsas, induzindo o leitor a tomar atitudes prejudiciais a ele próprio; e) Sniffers – são programas espões semelhantes ao spywares que são introduzidos

² ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002. p.53.

³ ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. p. 25.

no disco rígido e têm capacidade de interceptar e registrar o tráfego de pacotes na rede; f) Trojan horse ou cavalos de Troia – quando instalado no computador, o trojan libera uma porta de acesso ao computador para uma possível invasão. O cracker pode obter informações de arquivos, descobrir senhas, introduzir novos programas, formatar o disco rígido, ver a tela e até ouvir a voz, caso o computador tenha um microfone instalado. Como boa parte dos micros é dotada de microfones ou câmeras de áudio e vídeo, o trojan permite fazer escuta clandestina, o que é bastante utilizado entre os criminosos que visam à captura de segredos industriais; e g) Keyloggers é uma forma de spyware que registra cada batida no teclado ou outra atividade num sistema. Esses programas podem coletar números de cartão de crédito, senhas e outros dados delicados e transmiti-los a terceiros.

Através desses mecanismos alguns usuários mal-intencionados utilizam-se desses dispositivos tecnológicos para a prática de infrações penais.

E um dos grandes problemas do crime virtual é exatamente identificar esse indivíduo autor da prática do ato lesivo, ou seja, determinar a autoria do crime. Por si só o mundo virtual facilita no anonimato dos usuários, além disso, muitas vezes utilizando de recursos o indivíduo se passa por outra pessoa através de dados roubados, o que dificulta muito na descoberta do autor do crime.

Outro problema é comprovar a materialidade do crime, pois as evidências dos crimes virtuais são extremamente voláteis, podendo ser apagadas em segundos ou perdidas facilmente. Além disso, possuem formato complexo e costumam estar misturadas a uma grande quantidade de dados legítimos, demandando uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Destacamos ainda, o problema da competência, como a internet não possui fronteiras, qualquer conteúdo pode ser acessado de qualquer lugar do mundo. O Brasil pode proibir determinado ato, entretanto, somente poderá cumprir a proibição entre os provedores e usuários do território brasileiro. Temos um conflito de competência entre o foro do local de onde partiu a ofensa, do domicílio do ofendido e do infrator e ainda, do local onde o ofendido tomou ciência da ofensa.

A Convenção Sobre Cibercrime⁴ em seu artigo 22, deixa a critério das partes a jurisdição mais apropriada para o procedimento legal, não havendo um entendimento internacional uniforme a respeito da competência dos crimes virtuais.

⁴ CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME. Disponível em: < http://www.acidi.gov.pt/_cfn/529350b642306/live/+Conven%C3%A7%C3%A3o+sobre+o+Cibercrime++> acesso em 02 de junho de 2015.

No ordenamento jurídico Brasileiro, aplicam-se os artigos 5º e 6º do Código Penal Brasileiro, no que tange a competência para processar e julgar os crimes praticados na internet, sejam eles:

Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.⁵

O ordenamento jurídico pátrio adotou a teoria da ubiquidade, conforme versa o art. 6º do CP, sendo que os delitos que são praticados por brasileiro, tanto no país quanto fora, ainda que transnacionais, será aplicado à lei brasileira, tendo em vista ainda o que dispõe o art. 7º do Código Penal, o qual sujeita a lei brasileira a alguns crimes praticados no estrangeiro.

Em relação à classificação destes delitos a doutrina majoritária divide em: a) puros (ou próprios), ou seja, aqueles praticados por computador e se realizem ou se consumem também em meio eletrônico, na qual a informática é o objeto jurídico tutelado; e b) impuros (ou impróprios), aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens diversos da informática.

Os principais crimes virtuais próprios são: a) acesso e uso não-autorizados, ou seja, a utilização do sistema sem ser autorizado; b) Alteração e destruição de dados, ou seja, uso intencional de programas ilegais e destrutivos para alterar ou destruir dados. Os exemplos mais comuns desse tipo de programas são os vírus que, quando carregados em um computador, podem destruir dados, interromper ou provocar erros no processamento. Também é conhecido como fraude virtual, pois o agente pratica uma conduta de invasão, alteração ou modificação, pagamento ou supressão de dados eletrônicos ou programas, ou qualquer outra adulteração em um sistema de processamento de dados.

Os principais crimes virtuais impróprios são: a) estelionato: a conduta do agente será de induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem. Uma das condutas típicas do estelionato pela Internet consiste na conduta do agente encaminhar e-mails com conteúdo falso ao usuário, induzindo o mesmo a clicar em links disponíveis no corpo do e-mail, em que muitas das vezes direciona o usuário para um site falso

⁵ BRASIL. Código Penal. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União. Publicado em 7 de dezembro de 1940.

onde o mesmo digita informações pessoais ao agente que formulou a página falsa, estas informações são enviadas ao agente por meio da internet, que após apropriar-se dos seus dados bancários, transfere valores disponíveis em conta corrente para o seu domínio; b) insultos: falar mal ou insultar alguém que pode gerar processo com base no Artigo 140 do Código Penal, que pune “a injúria que ofende a dignidade ou decoro”; c) calúnia: inventar histórias falsas sobre alguém pode ser enquadrado no Artigo 138 do Código Penal; d) difamação: associar uma pessoa a um fato que ofende sua reputação. Artigo 139 do Código Penal; e) divulgação de segredo: revelar segredos de terceiros na internet ou divulgar material confidencial de documentos/correspondências que possam causar danos, pode levar a processo com base no Artigo 153 do Código Penal; f) escárnio por motivo de religião: criar comunidade online que menospreze ou zombe de pessoas religiosas e religiões. Artigo 208 do Código Penal; g) favorecimento da prostituição: Artigo 228 do Código Penal; h) ato obsceno: Artigo 233 do Código Penal; i) escrito ou objeto obsceno: Artigo 234 do Código Penal; j) incitação ao crime: Artigo 286 do Código Penal; l) apologia de crime: criar comunidades virtuais (fóruns, blogs, etc) para ensinar como burlar a legislação ou divulgar ações ilícitas realizadas no passado, que estão sendo realizadas no presente ou serão realizadas no futuro: Artigo 287 do Código Penal; m) falsa identidade: criar um perfil falso pode levar a processo judicial com base no Artigo 307 do Código Penal; n) preconceito ou discriminação: comentar em chats, e-mails blogs e outros, de forma negativa sobre raças, religiões, etnias, etc. Artigo 20 da Lei 7.716/89; o) pedofilia: troca de informações ou imagens envolvendo crianças ou adolescentes. Artigo 241-A, 241-B, 241-C, 241-D e 241-E da Lei no 8.069/90 ECA; p) Privacidade: trata, basicamente, da coleta e mau uso de dados. Dados sobre as pessoas são constantemente coletados, armazenados e distribuídos por redes facilmente acessíveis, sem o conhecimento ou o consentimento da pessoa a quem eles se referem ou a quem eles pertençam; e q) pirataria de software: é tratada como propriedade intelectual e, como tal, é considerada um bem jurídico tutelado pelo Direito. Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é entendido como pirataria de acordo com a Lei 9.610/98.

Como podemos ver os chamados crimes virtuais englobam os mais diversos tipos de crimes. A seguir veremos como a legislação trata o tema.

3. LEGISLAÇÃO APLICÁVEL AOS CRIMES VIRTUAIS

A Constituição Federal versa em seu art. 5º, XXXIX que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, ou seja, para que se venha a punir os crimes que são praticados no meio digital, é necessário que o tipo penal venha a se adequar nas normas já existentes, e as lacunas que por ventura ainda existem, devem ser preenchidas, sendo que hoje é extremamente necessária a incorporação dos conceitos de informática à legislação vigente.

O ordenamento é formado por vários ramos jurídicos, cada qual com sua legislação específica, ocorrendo o mesmo com os crimes informáticos.

No Brasil, o ordenamento jurídico demorou a criar normas para combater os crimes virtuais de forma direta. Até 2012 o ordenamento pátrio esteve sem cobertura legal específica, pois a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Nesse sentido, podemos citar, dentre outros, o Código Penal (CP), o Estatuto da Criança e do Adolescente (Lei n. 8.069/90) e Lei dos Crimes de Software (ou Lei Antipirataria, Lei n. 9.609/98) e a Lei de Segurança Nacional (Lei nº 7.170/83).

Em 2012, o ordenamento jurídico pátrio deu um grande passo para combater os crimes virtuais promulgando duas leis que atualmente norteiam o direito informático, quais sejam, a Lei n.º 12.735/12 e a Lei n.º 12.737/12 (Lei Carolina Dieckmann).

A Lei n.º 12.735/2012 tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. É um verdadeiro suporte para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como determinar o regulamento específico. Com esta determinação legal, todos os setores da polícia judiciária brasileira deverão organizar setores especializados em crimes cometidos na esfera virtual, criando no sistema jurídico brasileiro o suporte necessário para a edição de legislações dedicadas ao assunto.

Na Lei n.º 12.737/2012, o legislador foi além, editando a tipificação criminal dos principais delitos informáticos, relacionados com a invasão de dispositivos informáticos e a divulgação indevida de dados computacionais.

O seu artigo 2º alterou o Código Penal Brasileiro, incluindo os artigos 154-A e 154-B ao diploma legal referido. Estes artigos dispõem sobre as condutas combatidas na esfera

virtual, a respectiva sanção legal a ser aplicada aos futuros infratores e a forma de procedimento da respectiva ação penal.

O artigo 154-A inclui no ordenamento o crime de invasão de dispositivo informático, punindo “quem invadir dispositivo informático, mediante violação dos mecanismos de segurança, visando a obtenção, alteração ou destruição de dados computacionais sem a devida autorização de seu proprietário, ou, ainda, para instalar vulnerabilidades nos dispositivos a fim de obter vantagem ilícita”⁶

O artigo 154-B estabelece que as ações penais que versem sobre delitos informáticos só poderão ser processadas mediante representação, exceto se o crime for cometido contra a administração direta ou indireta federal, estadual, distrital ou municipal, ou, ainda, contra empresas concessionárias de serviços públicos.

Ainda sobre a Lei n.º 12.737/2012 seu artigo 3º, acrescentou parágrafos aos artigos 266 e 298 do Código Penal Brasileiro.

O artigo 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, e ao incluir os parágrafos, o ordenamento expande o alcance da norma para os serviços telemáticos ou de utilidade pública, abarcando, assim, os ilícitos cometidos não só contra o interesse público, mas, também, contra dados informáticos.

Já o parágrafo incluído no artigo 298, que tipifica o crime de falsificação de documento particular, estende os efeitos da norma aos cartões de crédito e de débito, os quais receberam do legislador a qualidade de documento particular devidamente reconhecido, e protegido, pelo ordenamento.

O legislador pátrio buscando acompanhar esses crimes, em projeto de lei do novo código penal propõe a criação de um título específico para crimes cibernéticos com intuito de a lei abranger condutas que se tornaram comuns com a disseminação de sistemas informatizados. As mudanças, previstas no PLS 236/2014, que tramita na Comissão de Constituição e Justiça (CCJ), são mais amplas que as inovações trazidas pela Lei 12.735/2012 e 12.737/2012. A nova parte introduz conceitos de informática, como provedor de serviços e dados de tráfego, e tipifica crimes no mundo virtual, como a ação de hackers que invadem sistemas digitais.

CONCLUSÃO

⁶ BRASIL. Lei n.º 12.737 de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União. Publicado em 30 de novembro de 2012.

A tecnologia e a globalização trouxeram novos caminhos para a sociedade, e o direito tem a obrigação de acompanhar essas modificações, visando proteger os indivíduos.

A internet ensejou uma revolução na vida das pessoas, das empresas e dos Estados, trazendo inúmeros benefícios a nossa sociedade. No entanto, o efeito colateral foi o surgimento de uma nova criminalidade, que se utiliza do espaço virtual para a prática de crimes.

O rápido avanço tecnológico é assimilado rapidamente por toda sociedade, inclusive pelos criminosos, de forma que o legislador penal não consegue acompanhar esta evolução.

O Código Penal Brasileiro foi elaborado em 1940, quando o legislador daquela época visou o bem a ser protegido, na definição de cada crime. Desse período para os dias atuais inúmeras mudanças ocorreram na sociedade, principalmente quanto ao desenvolvimento tecnológico, devendo o ordenamento pátrio estar sempre em atualização visando proteger o bem jurídico.

O legislador vem tentando qualificar esses crimes, no entanto a legislação ainda se mostra insuficiente a combater esses crimes virtuais, cabendo aos estudiosos do Direito o trabalho para a evolução da dogmática penal segundo uma nova realidade mundial para que o mundo virtual não se transforme em um universo paralelo onde as regras do direito não tenham alcance.

Desta forma, verifica-se que a falta de um enquadramento da conduta lesiva aos tipos penais existentes no ordenamento jurídico brasileiro pode levar à impunidade de seus agentes. Por isso, torna-se imperioso a criação de legislação específica ou a adequação da existente a fim de resguardar o bem jurídico protegido e inibir a prática dos crimes virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Código Penal. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União. Publicado em 7 de dezembro de 1940.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Diário Oficial da União. Publicado em 5 de outubro de 1988.

BRASIL. Lei n.º 12.735 de 30 de novembro de 2012, que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Diário Oficial da União. Publicado em 30 de novembro de 2012.

BRASIL. Lei n.º 12.737 de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União. Publicado em 30 de novembro de 2012.

INELLAS, Gabriel Cesar Zaccaria. Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004.

LOPES JR, Aury. Direito Processual Penal. 12ª edição. São Paulo: Saraiva, 2015.

PINHEIRO, Emeline Piva. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. Porto Alegre: PUCRS, 2006. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf>. Acesso em: 28 de maio de 2015.

VIANNA, Túlio Lima. Fundamentos de Direito Penal Informático. Rio de Janeiro: Forense, 2003.