O DIREITO NA ERA DIGITAL:
O Cibercrime no Ordenamento Jurídico Brasileiro

Orientando: [1]CARDOSO, Lucas de Holanda M. (FEMA/IMESA)
Orientador: [2]Prof. Me. Carlos Ricardo Fracasso (FEMA/IMESA)
Coorientadora: [3]Profª. Me. Maria Angélica Lacerda Marin (FEMA/IMESA)
[1]email: lu.hmc@hotmail.com
[2]email: ricardofracasso@femanet.com.br
[3]email: adoromeusalunos@hotmail.com

RESUMO:
A praticidade e a conectividade, oferecidas pela internet, geraram uma série de benefícios à sociedade. Todavia, com a crescente adesão social à tecnologia, surgem novos meios que possibilitam a prática dos crimes cibernéticos. Nesse diapasão, o impacto do avanço tecnológico no ordenamento jurídico brasileiro faz repensar o papel do Direito frente à ocorrência dos crimes virtuais ocorridos e os desafios jurídicos em face à tipificação do cibercrime.

PALAVRAS-CHAVE: Internet; crimes virtuais; ordenamento jurídico Brasileiro; cibercrime.

ABSTRACT:
The practicality and connectivity offered by the Internet have generated a series of benefits to society. However, with the increasing social adherence to technology, new means emerge that allow the practice of cyber crimes. Within this context, the impact of the technological advance in the Brazilian legal system makes it possible to rethink the role of the Law in the face of the occurrence of virtual crimes and the legal challenges to the typification of cybercrime.

KEYWORDS: Internet; virtual crimes; Brazilian legal system; cybercrime.

1. Introdução

1.1 Evolução das Tecnologias de Informação

O ser humano sempre dispôs de suas habilidades para desenvolver técnicas e metodologias para uma finalidade específica, de acordo com a sua área de interesse, desse modo, tornou-se imprescindível desenvolver novos meios, formas, ou ferramentas que facilitassem a realização de suas atividades diárias. É possível observar isso desde as pinturas rupestres realizadas de forma arcaica pelo homem pré-histórico, até a criação de aparelhos eletrônicos que permitem a comunicação e facilitam a conectividade entre as pessoas em qualquer lugar do globo terrestre.

O século XX marcou o desenvolvimento e o surgimento de novas tecnologias que trouxeram um novo paradigma a sociedade: a era da informação ou era digital. Assim sendo, a consequência gerada pelo desenvolvimento da tecnologia computacional, gerou a terminologia Tecnologia da Informação (TI), isto é, um "conjunto de recursos tecnológicos e computacionais, desde os voltados à geração de dados, até as pertinentes e sofisticadas redes de comunicação, presentes nos processos de utilização da informação'' (VELLOSO, 2004, p. 263). Estes termos passaram a fazer parte do cotidiano das pessoas, e a serem utilizados para designar os avanços tecnológicos advindos da terceira revolução industrial, proporcionando o surgimento do computador, da informática, da internet e do ciberespaço[1].

Com o advento da internet e a popularização de seu uso, a *World Wide Web* – WWW, teia de amplitude mundial, ou em um sentido mais compreensível, rede mundial de computadores, corroborou para que milhares de pessoas interajam, bastando para isso, que elas se conectem à rede, sendo possível, desse modo, acessar às informações disponíveis referentes aos mais variados assuntos. Além disso, é possível elencar outras vantagens proporcionadas pela utilização da internet, dentre as quais podem se destacar: a comunicação, a informação, o entretenimento, a prestação de serviços como as transações bancárias on-line, o pagamento de contas, a procura por emprego, assistir a filmes, séries, documentários, ouvir músicas, realizar reservas em hotéis, comprar e vender produtos e mercadorias, dentre outras.

A internet possui tipos de ambientes diversificados, que são denominados *website*, ou somente *site*. Um *site* possui um endereçamento eletrônico virtual, a URL, *Uniform Resource Locator*, ou seja, é um caminho que indica onde está o que o usuário

[1] Termo idealizado por Willian Gibson e descrito em 1984 em seu livro Neuromancer, como um espaço virtual composto por cada computador e usuário conectados em uma rede mundial.

procura. Desse modo, o conjunto das informações que aparecem na mesma tela do monitor recebe a denominação de página, e as diversas páginas relacionadas ao mesmo assunto compõem um *site*. É por meio de um link, isto é, o endereço de uma página, que o usuário é direcionado ao conteúdo que procura na internet. Para que haja uma comunicação na rede entre as páginas, é utilizado um protocolo de comunicação na internet, HTTP (*Hypertext Transfer Protocol*), do mesmo modo para que seja possível a transferência de arquivos na rede utiliza-se o FTP (*File Transfer Protocol*).

Um site possui pontos que o conectam entre as partes que o compõe, e também o direcionam a outras informações de outros sites, por meio de um link, desse modo, navegar na internet significa percorrer as páginas de um ou de vários sites, por meio de links sucessivos. Hoje é possível localizar por meio de mecanismos de busca os mais variados assuntos, bem como tornar acessível um vasto conteúdo de dados e informações na rede, como esclarece (BROOKSEAR, 2013, p. 9):

> Para tornar a informação na Web acessível, sistemas de software, chamados de motores de busca, foram desenvolvidos para ‘’peneirar’’ a Web ‘’categorizar’’ seus achados e, então, usar os resultados para auxiliar os usuários que estejam pesquisando por tópicos em particular. As grandes empresas nessa área são a Google, a Yahoo! e a Microsoft.

Com o avanço da tecnologia, conectar-se à rede mundial de computadores ficou cada vez mais acessível, ainda mais com a popularização dos smartphones, aparelhos celulares, que possuem recursos que possibilitam tal acesso, ou seja, “o que há pouco era meramente um telefone evoluiu para um pequeno computador de propósito geral que cabe na palma da mão’’ (BROOKSHEAR, 2013, p. 10). Os celulares evoluíram a tal ponto que além de serem utilizados com a finalidade de possibilitarem a comunicação via telefonia móvel, eles equiparam-se a pequenos computares, repletos de aplicativos que possuem uma diversidade de funções, como destaca (BROOKSHEAR, 2013, p. 10):

> Esses “telefones’’ são equipados com um amplo conjunto de sensores e interfaces, incluindo câmeras, microfones, bússolas, telas sensíveis ao toque, acelerômetros (para detectar a orientação do telefone e seu movimento) e diversas tecnologias sem fio para se comunicarem com outros smartphones e computadores. O potencial é enorme.

Ainda sobre o assunto aduz o autor (BROOKSHEAR, p. 125):

> Na última década, a tecnologia de telefones móveis avançou de dispositivos portáteis simples e de propósito singular para computadores de mão complexos e de múltiplas funções. A primeira geração de redes de telefonia sem fio transmitia sinais de voz analógicos através do ar, de maneira parecida com os telefones tradicionais, mas sem os fios de cobre passando através das paredes. Em retrospecto, chamamos esses primeiros sistemas de redes de

> telefonia de “1G’’, ou primeira geração. A segunda geração usava sinais digitais para codificar voz, fornecendo um uso mais eficaz das ondas emitidas pelo ar e transmitindo outros tipos de dados digitais como mensagens de texto. A terceira geração (“3G’’) de redes de telefonia fornece taxas de transferência de dados mais altas, permitindo chamadas móveis de vídeo e outras atividades que consomem bastante largura de banda. Os objetivos das redes 4G incluem taxas de transferência de dados ainda mais altas e uma rede de troca de pacotes completa usando o protocolo IP, que fornecerá às novas gerações de smartphones capacidades atualmente disponíveis apenas para PCs com acesso à banda larga.

A tecnologia avançou exponencialmente de tal modo, que modificou as relações na sociedade como as noções de espaço e tempo. Se antes demorava para chegar informações de eventos distantes, hoje em dia é possível ter acesso de modo instantâneo a shows, palestras, aulas, conferências, seminários, cursos, jogos, lutas e afins. Com o advento da globalização, a sociedade é desafiada a adaptar-se a uma realidade nova, que conecta milhões de pessoas em uma velocidade cada vez maior, permitindo a rápida circulação de dados e informações, bastando para isso um dispositivo que possua recursos capazes de conectá-lo à internet.

2. Conflitos Jurídicos Gerados na Era Digital

São inúmeras as vantagens proporcionadas pela tecnologia e a utilização da internet, dentre as quais se destacam: a comunicação, a informação, o entretenimento, a prestação de serviços como as transações bancárias on-line, o pagamento de contas, a procura por emprego, assistir a filmes, séries, documentários, ouvir músicas, realizar reservas em hotéis, comprar e vender produtos e mercadorias, dentre outras. No entanto, o mesmo canal que pode ser utilizado para tais funcionalidades, infelizmente proporciona aos seus usuários a possibilidade do mau uso deste para a prática de vários atos caracterizados como crimes digitais.

O chamado *Cybercrime*, Crime Virtual, de acordo com (FERREIRA, 2005, p. 261), é classificado como sendo:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Já Moisés de Oliveira Cassanti, ao tratar do assunto, utiliza a seguinte definição: “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.” (CASSANTI, 2016, p. 51). Como a definição a respeito da

criminalidade informática é amplo, o conceito encontrado por parte da doutrina é que este recente fenômeno histórico e sociocultural corresponde a elevada incidência de atos ilícitos, que têm por objetivo lesar ou obter algum tipo de vantagem indevida de outrem.

Vale esclarecer que é comum a confusão no tocante a nomenclatura atribuída ao criminoso virtual entre cracker e hacker. Os crackers são conceituados como pessoas que possuem amplo conhecimento de informática, e utilizam deste para cometerem delitos, adquirirem informações privadas, ou mesmo causarem algum dano a terceiros, como elucida (ROSA, 2006, p.61):

> O mesmo que hacker, com a diferença de utilizar o seu conhecimento para o "mal". Destruir e roubar são suas palavras de ordem. Assim, o cracker usa os seus conhecimentos para ganhar algo; rouba informações sigilosas para fins próprios e destrói sistemas para se exibir.

Por conseguinte, os hackers também possuem um vasto conhecimento, mas eles não utilizam deste para lesar ou causar alguma forma de dano a outrem, visto que, em determinadas situações eles são contratados por empresas para identificarem possíveis falhas que possam comprometer informações sigilosas, e verificarem a eficácia de sistemas de segurança, assim como define (NOGUEIRA, 2008, p. 52):

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam desafiar entre si, para ver quem consegue invadir tal sistema ou página da internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.

Assim, em linhas gerais, é possível afirmar que com a difusão dos meios eletrônicos e com o advento da internet, é cada vez mais comum a prática de atos praticados com a finalidade de causar danos aos bens jurídicos de terceiros. Nesta esfera os agentes se valem de todos os recursos e meios possíveis que a web proporciona para cometerem este tipo de delito, principalmente os ocorridos nas zonas obscuras da rede mundial de computadores, a "*deep web*". Ela corresponde a camada da internet que é criptografada e que não é possível acessar por meio de sites de busca. Esta parcela da *web* é facilmente explicada por meio da analogia a um iceberg, ou seja, a internet que comumente utilizamos ao digitarmos no navegador um site corresponde a parte superficial, posto que, a parte inferior abrange a maior parte, isto é, a zona obscura.

A conexão que possibilita o acesso a esta esfera obscura não é ilegal, e não apresenta somente conteúdo ilícito, posto que, devido a sua discrição o fluxo dos dados que trafegam nesse ambiente representam 96% o tamanho da internet, o que equivale a

500 vezes mais o conteúdo da parte superior, de acordo com o levantamento dos dados realizados em 2015.

Destarte, como todo o conteúdo da *deep web* é sigiloso, é fácil imaginar um cenário que possibilite inúmeras oportunidades para quem esteja mal-intencionado em lesar outrem. É possível verificar não apenas nesse espaço, mas em toda forma de navegação na rede, eixos distintos de práticas delituosas, como os crimes contra a honra do indivíduo, e contra o patrimônio.

Dentre os que versam sobre a honra estão: a calúnia, a injúria, a difamação, insultos, divulgação de material confidencial, pedofilia, ato obsceno, apologia ao crime, preconceito ou discriminação. No tocante aos crimes contra o patrimônio, merecem destaque os contra a propriedade industrial, intelectual, o plágio o furto, a extorsão, a apropriação indébita, o estelionato, a pirataria e a comercialização ilegal de produtos, além da comercialização de armas e o tráfico de drogas.

Nos casos de venda de amamento e o tráfico de substâncias entorpecentes, a forma mais comum de pagamento é através da moeda digital utilizada de forma inovadora, os chamados “bitcoins”, que não dependem dos bancos centrais para circulação. Essas moedas são utilizadas de forma que não ficam registrados dados bancários, e são controladas por uma rede *peer-to-peer*, (ponto a ponto), isto é, uma rede onde cada ponto funciona tanto como cliente quanto como servidor, o que permite o compartilhamento de dados, sem ter a necessidade de utilizar um servidor central para desempenhar a tarefa.

3. Tipificação das Infrações Cibernéticas

Nos dias atuais é possível verificar um significativo avanço no que concerne ao acesso à internet, no entanto, essa eclosão nos leva a refletirmos sobre os benefícios e malefícios que sua utilização proporciona. Infelizmente, criminosos se valem desse meio para realizarem práticas delituosas com o intento de obter para si vantagens em proveito de outros usuários da internet.

Embora as ações infratoras sejam punidas, tendo como parâmetro o Código Penal brasileiro, vale destacar que ele foi reformulado em 1984, fato que o torna genérico e não eficaz para combater todas as condutas ilícitas, por ser anterior ao advento da internet. Como prevê o texto da lei sobre a aplicação da lei penal no art. 1º “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.”

Assim também destaca a Constituição Federal, no art. 5º, inc. XXXIX, e o Código Penal Militar, no art. 1º.

Certamente, um dos maiores desafios em combater o cibercrime, é a rapidez com que ele ocorre, pois, os meios utilizados são praticamente instantâneos e muitas vezes não deixam pistas. Por isso, é necessário que o Estado ofereça mais segurança ao ambiente da *word wide web* e maior rigor quanto à sua utilização.

A internet é considerada território livre, sem legislação específica e punição adequada, porém ainda que não estejam satisfatoriamente codificadas em lei, as condutas de crimes digitais são adequadas à legislação existente, e, diariamente, os meios de veiculação de informação noticiam a ação do Poder Judiciário coibindo e punindo a criminalidade cibernética.

3.1 Dispositivos Legais

Objetivando gerar maneiras para tornar a liberdade da navegação na internet mais restrita, e criminalizar as condutas de quem dispõe desse meio para cometer crimes, foi aprovado, em 04 de maio de 2016, o relatório final da CPI (Comissão Parlamentar de Inquérito) de Crimes Cibernéticos que contém uma série de propostas e Projetos de Lei (PLs), que passarão a tramitar com prioridade na Câmara dos Deputados, tal documento expressa, em seu texto, medidas que vão ao encontro do Marco Civil da internet e dos direitos dos usuários.

Um dos PLs prevê a possibilidade de um juiz bloquear funções de aplicativos de celulares, sites ou redes sociais, hospedados fora do Brasil ou que não possuam representação nacional, caso considere que o conteúdo apresentado seja voltado majoritariamente para a prática de alguma forma de crime, e sugere como pena a reclusão de, no mínimo, dois anos, excetuando-se os crimes contra a honra. É uma iniciativa interessante. Porém, o maior desafio será o de estabelecer que uma aplicação seja voltada à prática de crimes, bem como gerar parâmetros que permitam classificá-los como sendo um ato malicioso, ou criminoso.

Assim sendo, além dos Projetos de Lei, que tramitam na Câmara, referente à complexa tarefa de combater o cibercrime, é possível verificar, como alternativa, a adesão do Brasil, bem como sua assinatura à Convenção de Budapeste[2]. Vários países

[2] Criada em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004, após a ratificação de cinco países, a Convenção de Budapeste, ou Convenção sobre o Cibercrime, engloba mais de 20 países (EDERLY, 2008) e tipifica os principais crimes cometidos na Internet. A Convenção prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço,

da Europa tratam o cibercrime desde sua definição, até as normas procedimentais. Além de contarem com a cooperação mútua internacional, tanto na fase de investigação, quanto na produção probatória, por meio de documento oficial assinado pelos países participantes.

Atualmente os delitos cibernéticos são tipificados no Código Penal, nos seguintes artigos: furto (art. 155); crimes contra a honra (arts. 138,139 e 140 do CP); crime de ameaça (art. 147 do CP); extorsão (art. 158 do CP); extorsão Indireta (art. 160 do CP); escárnio por motivo de religião (art. 208 do CP); favorecimento da prostituição (art. 228 do CP); ato obsceno (art.233 do CP); escrito ou objeto obsceno (art. 234 do CP); incitação ao crime (art. 286 do CP); apologia de crime ou criminoso (art. 287 do CP); invasão de dispositivo informático (art. 154-A do CP); apropriação indébita (art. 168 do CP); estelionato (art. 171 do CP); violação de direito autoral (art. 184 do CP).

3.2 Leis Ordinárias Vigentes

Atinente a legislação existente, destacam-se as leis ordinárias que majoram o campo do enquadramento dessas condutas, como a lei referente à pedofilia (art. 241 da Lei 8.069/90 - ECA); a interceptação de comunicações de informática (art. 10 da Lei n° 9.296/96; os crimes contra a propriedade industrial (art. 195 da Lei n° 9.279/96); crime de divulgação do nazismo (art. 20º §2º. da Lei 7.716/89); crimes contra *software* "Pirataria" (art. 12 da Lei n° 9.609/98); preconceito ou discriminação (art. 20 da Lei 7.716/89) e a lei 12.735/2012, de combate à ação delituosa em redes, dispositivos de comunicação ou sistema informatizado, que ficou conhecida como lei Azeredo, por ter sido criada pelo deputado Federal Eduardo Azeredo (PSDB).

Na tentativa de tipificar novas condutas ilícitas praticadas por meio de recursos tecnológicos, e complementar os institutos jurídicos existentes, o legislador criou a lei 12.737/2012, que ficou conhecida nacionalmente como Lei Carolina Dieckmann, após 36 fotos íntimas da atriz terem sido publicadas na internet em maio de 2012. Foi um avanço ao combate dos crimes virtuais, pois este dispositivo legal criou novos tipos incriminadores, por meio da inclusão dos artigos 154-A e 154-B no Código Penal:

> **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

---

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".

> 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.
>
> **Art. 154-B.** Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Com fulcro no § 1º do artigo 154-A, incorre na mesma pena o agente que produz, oferece distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput* do artigo. Se a ação do invasor resultar prejuízo econômico à vítima, a pena será agravada, como aduz o § 2º:

> **§ 2º** Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Os parágrafos seguintes preveem a possibilidade de agravamento da pena nas seguintes situações:

> **§ 3°** 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.
>
> **§ 4°** 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.

O advento da Lei 12.737/2012, criou novos tipos incriminadores, contudo, o texto normativo não produziu grandes reformas no ordenamento jurídico, tampouco solucionou o problema que o Direito brasileiro enfrenta sobre o tema, todavia, este dispositivo legal trouxe significativos avanços ao tipificar condutas gravosas à sociedade, além disso, a referida lei foi a primeira a funcionar como instrumento normativo destinado especificamente à tutela do bem jurídico no mundo virtual.

3.2.1 Marco Civil da Internet

Outro avanço significativo do legislador foi a criação da Lei 12.965/2014, conhecida como Marco Civil da Internet, que regula a utilização da *web* no Brasil por meio de princípios, garantias, direitos e deveres, para os usuários da rede, e traça diretrizes para a atuação do Estado.

Este dispositivo legal ficou conhecido como "Constituição da Internet", pois, foi criado e debatido por cerca de aproximadamente duas mil pessoas, sobre três pilares norteadores: Liberdade, Privacidade e Neutralidade, que estabelecem princípios e garantias normativas do convívio civil, e responsabiliza os provedores de serviços.

O objetivo principal do marco civil, é prever práticas criminosas no ambiente online, prezar pela neutralidade da rede, pela liberdade de expressão, e pela privacidade dos seus usuários, evitando que suas informações pessoais sejam vendidas ou ofertadas à empresas sem sua prévia autorização, além de assegurar o sigilo em suas comunicações.

4. Considerações Finais

A praticidade e a conectividade, oferecidas pela internet, trouxeram significativos benefícios à sociedade. Todavia, com a crescente adesão social à tecnologia, surgem novos meios que possibilitam a prática dos crimes cibernéticos. Desse modo, a presente pesquisa teve por objetivo verificar o impacto gerado pela informatização nas relações sociais, bem como os delitos praticados por agentes que utilizam dos meios digitais para realizarem tal conduta.

Em título de hipótese, acredita-se que o impacto do avanço tecnológico gerou inúmeras vantagens à sociedade e que atrelado a elas surgiram novos meios que propiciam a prática de crimes virtuais. Assim o ordenamento jurídico brasileiro faz repensar o papel do Direito frente ao combate dos delitos ocorridos na área penal e a tipificação dos mesmos. Neste diapasão, foi abordada a forma com que o ordenamento jurídico brasileiro tipifica tais condutas, além de verificar os desafios jurídicos referentes a eficácia com que a legislação vigente penaliza tais crimes.

Constatou-se, portanto, confirmando a hipótese levantada, que apesar de existir punibilidade aos criminosos virtuais, algumas condutas próprias ainda não são regulamentadas pela legislação brasileira, o que permite que elas permaneçam impunes, portanto, embora haja um conjunto de normas esparsas que tipificam os crimes

cibernéticos, é necessário mais do que isso para uma efetiva tutela aos bens jurídicos da sociedade no mundo virtual, é imprescindível a materialização de reprimendas, para que a prática de ilícitos virtuais não ocorram, ou que sejam minimizados, partindo da elaboração de uma legislação específica que normatize situações atípicas, de modo que os anseios sociais e os litígios sejam solucionados de forma eficaz.

5. Referências Bibliográficas

ALCÂNTARA, Lucas. **Cibercrimes e a Tardia Legislação Brasileira.** Em: <https://www.profissionaisti.com.br/2014/01/cibercrimes-e-a-tardia-legislação-bsasileira/>. Acesso em 02 de outubro de 2017.

BARRETO, Erick Teixeira. **Crimes Cibernéticos Sob a Égide da Lei 12.737/2012.** Disponível em: <http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=18757>. Acesso em 06 novembro de 2017.

BORGES, Abimael. **Lei Carolina Dieckmann – Lei n° 12.737/12, art. 154-a do Código Penal.** Em: <https://www.abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-código-penal >. Acesso em 03 de outubro de 2017.

BROOKSHEAR, J. Glenn. **Ciência da Computação: Uma visão abrangente**. 11ª. ed. – Porto Alegre: Bookman, 2013.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes.** 2 ed. São Paulo: Quartier Latin, 2005.

PEREIRA, Leonardo. **Deep web: saiba o que acontece na parte obscura da internet**. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120>. Acesso em 10 novembro de 2017.

ROSA, Fabrízio. **Crimes de Informática.** 2. Ed. Campinas: Bookseller, 2006.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática.** São Paulo. BH Editora, 2008.

VELLOSO, Fernando de Castro. **Informática Conceitos Básicos**. 7ª. ed. rev. e atualizada – Rio de Janeiro: Elsevier, 2004.

VESCE, Gabriela E. Possolli. **Ciberespaço**. Em <http://www.infoescola.com/internet/ciberespaco/> Acesso em 25 outubro 2017.