CENTRO UNIVERSITÁRIO FAMETRO

Curso de Direito

SÂMYA PEREIRA MENESES

CRIMES VIRTUAIS: POSSIBILIDADES E LIMITES DA SUA REGULAMENTAÇÃO NO BRASIL

FORTALEZA

2019

SÂMYA PEREIRA MENESES

CRIMES VIRTUAIS: POSSIBILIDADES E LIMITES DA SUA REGULAMENTAÇÃO NO BRASIL

Artigo TCC apresentado ao curso de Bacharel em Direito do Centro Universitário Fametro – UNIFAMETRO – como requisito para a obtenção do grau de bacharel, sob a orientação do Prof. Me. Leonardo Jorge Sales Vieira.

FORTALEZA

2019

SÂMYA PEREIRA MENESES

CRIMES VIRTUAIS: POSSIBILIDADES E LIMITES DA SUA REGULAMENTAÇÃO NO BRASIL

Artigo TCC apresentado no dia 21 de junho de 2019 como requisito para a obtenção de grau de bacharel em Direito do Centro Universitário Fametro – UNIFAMETRO – tendo sido aprovado pela banca examinadora composta pelos professores abaixo:

BANCA EXAMINADORA

_____
Profº. Me. Leonardo Jorge Sales Vieira
Orientador - Centro Universitário Fametro

_____
Profª. Ma. Patricia Lacerda de Oliveira Costa
Membro - Centro Universitário Fametro

_____
Profº. Me. Francisco Gilney Bezerra de Carvalho Ferreira
Membro - Centro Universitário Fametro

CRIMES VIRTUAIS: Possibilidades e limites da sua regulamentação no Brasil

Sâmya Pereira Meneses[1]
Leonardo Jorge Sales Vieira[2]

RESUMO

Destaca-se que, juntamente com a importância da Internet e seu progresso para o desenvolvimento, surgiram usuários que se aproveitam desses sistemas para cometer crimes virtuais prejudicando os demais usuários na rede. Este artigo tem como objetivo principal, investigar tipos de crimes virtuais, possibilidades e limites da sua regulamentação no Brasil. O tipo de pesquisa para esta pesquisa foi bibliográfico, fundamentado na literatura jurídica, como doutrinas, revistas, publicações de artigos científicos, trabalhos monográficos, dissertações e teses. Observou-se que, por um lado a edição da Lei n. 12.737/2012 constituiu um importante avanço, ao tipificar expressamente o crime de "invadir dispositivo informático", criando um tipo penal que visou eminentemente proteger o sigilo de dado e informação pessoal ou profissional. Constatou-se também que, o desenvolvimento do Marco Civil da Internet, Lei 12.965/2014, mesmo sendo avaliado como um importante regulamentador da utilização dos meios digitais, ainda não é suficiente para combater os crimes virtuais. Percebe-se que, a decretação de uma lei especifica é imprescindível não somente para preencher as lacunas deixadas pelo Marco Civil da Internet e proteger melhor o cidadão, mas igualmente para uniformizar o significado dos conceitos essenciais para a proteção de dados.

Palavras Chave: Marco Civil. Crimes Virtuais. Proteção de Dados.

ABSTRACT

It is noteworthy that along with the importance of the Internet and its progress for development, users have emerged who take advantage of these systems to commit cyber crimes to the detriment of other users in the network. This article has as main objective, to investigate types of virtual crimes, possibilities and limits of its regulation in Brazil. The type of research for this research was bibliographical, based on legal literature, such as doctrines, journals, publications of scientific articles, monographic works, dissertations and theses. It was observed that, on the one hand, the edition of Law no. 12,737 / 2012 constituted an important step forward, by expressly typing the crime of "hacking into a computer device", creating a criminal offense that aimed eminently to protect the confidentiality of data and personal or professional information. It was also found that the development of the Civil Internet Framework, Law 12.965 / 2014, even though it is considered an important regulator of the use of digital media, is not yet sufficient to combat virtual crimes. It is perceived that the enactment of a specific law is indispensable not only to fill the gaps left by the Internet Civil Registry and to better protect the citizen, but also to standardize the meaning of the essential concepts for data protection.

Keywords: Civil Framework. Virtual Crimes. Data Protection.

[1] Graduanda do Curso de Direito pelo Centro Universitário Fametro – UNIFAMETRO.
[2] Professor Orientador do Curso de Direito do Centro Universitário Fametro – UNIFAMETRO.

1. INTRODUÇÃO

Pode-se dizer que, tratar sobre crime virtual envolve ações em pronto desenvolvimento, deste modo torna-se um tema bastante complicado. Em maioria, esses tipos de crimes são tratados, por pessoas com total habilidade técnica sobre o assunto. A cada dia são profundas as transformações que acontecem no meio da informática, igualmente como são profundas as modificações que acontecem na sociedade como todo.

Conforme visão de Roza (2016) torna-se importante destacar que, independente do nível social, cultural e de escolaridade, todos os usuários, estão passíveis de sofrer algum tipo de crime virtual. O problema é que, por muitas vezes quanto maior o nível de exposição de informações pessoais, maior o risco de sofrer algum golpe. Diante disso, surgem os seguintes questionamentos:

Qual a importância da Internet e seu progresso? Porque vem aumentando os tipos de crimes virtuais? As leis existentes vêm sendo competentes para combater efetivamente esses delitos?

O aumento que se percebe que ocorre na prática dos crimes virtuais está diretamente vinculado com o aumento do uso da internet entre as pessoas. Por isso, é fundamental para o bom desenvolvimento da “sociedade digital”, que esses criminosos sejam punidos com a reparação dos danos ocasionados; Para este pensamento tornar-se realidade é imprescindível lei mais severa.

Uma regulamentação eficaz contra os crimes virtuais se faz necessário nos levando a refletir sobre os meios de contingência que poderiam levar a sociedade a maior segurança.

Neste contexto, este artigo tem como objetivo principal, investigar tipos de crimes virtuais e possibilidades e limites da sua regulamentação no Brasil. Para complementar a pesquisa os objetivos específicos terão como base: demonstrar a importância e progresso da Internet na atualidade; Explicar sobre os tipos de crimes virtuais para compreensão do tema; Dissertar sobre leis existentes e as tipificações dos crimes virtuais, além de acompanharmos os projetos em discussão existentes a fim de melhorar o relacionamento dos usuários com a rede; E por último, comparar se os crimes cometidos aqui são igualmente executados e tipificados, ao realizados noutros países.

A presente pesquisa mostra-se importante para o estudante de direito que precisa compreender que, tratar sobre o crime virtual na atualidade é de grande importância para a sociedade. Entende-se necessário realizar ação conjunta, para assim expor sempre esses crimes, pois, nota-se que os crimes de informática necessitam ser combatidos urgentemente com atitudes amplas e globalizadas.

Vale destacar que a Internet oferece um ambiente, dinâmico, de alcance irrestrito, sem altos custos, sem a necessidade da utilização de papéis e impressão, auxilia a comunicação dos movimentos, tanto entre eles, como entre seus públicos. Partidos, sindicados, organizações não governamentais e até grupos guerrilheiros, ainda que eventualmente separados por estratégias e táticas de ação, descobrem no ciberespaço possibilidades de difundir suas reivindicações, de maneira irrestrita. As denúncias, pressões sociais, difusão de conceitos ocupam os sites institucionais, circulam entre os e-mails, entre os informativos eletrônicos e ganham ascensão (MIGUEL, 2007).

2. PROGRESSO E IMPORTÂNCIA DA INTERNET NA ATUALIDADE

Pode-se dizer que para o desenvolvimento da humanidade, destaca-se que á internet corresponde a um salto a uma mudança de paradigmas no pensar e agir da sociedade, portanto corresponde a uma revolução na história (KOLB; ESTERBAUER; RUCKENBAUER, 2001). Consequentemente, cada dia mais á virtualização da realidade se expande; pois, já existem salas de aula virtuais, igrejas virtuais e até religiões fundamentadas na virtualidade da Internet (FELINTO, 2005).

Com o crescimento e avanço das tecnologias, houve uma mudança na forma de estar junto sem a necessidade de estar perto, não se tem mais territórios fixados, as relações não são duradouras, tem-se assim uma geração plural com identidades fluidas e com um repertório que segue a rapidez das transformações tecnológicas. Para Castells (2013), as redes são a configuração lógica da organização da sociedade contemporânea, a geração que podemos chamar de geração conectada se caracteriza pela transmissão da informação como fontes fundamentais de produtividade e poder.

De acordo com Chiavenato (2010, p.313), a comunicação é essencial para o funcionamento coerente, integrado e sólido de qualquer organização. Instrumentos como *Facebook* e *Twitter* são detentores de grandes poderes, quando

as suas informações são usadas coerentemente, pois converter informações em conhecimento passou a ser o diferencial mais importante no contemporâneo cenário corporativo. Entretanto, é imprescindível utilizá-lo adequadamente para criar novos produtos, diversificar mercados e encantar clientes, conforme afirma o referido autor. A força dessas ferramentas comunicativas pode ser atribuída nas grandes transformações que acontecem no mundo todo.

A evolução tecnológica, meios de comunicação e novas interações impulsionaram a criação de um novo espaço público, onde a "internet coloca-se como um espaço que pressupõe uma subjetividade intersubjetivamente estabelecida, é processual e se põe em permanente tematização e questionamento. É, portanto, um espaço público" (SOUSA, 2006 p.67). Além do que, a cultura influencia diretamente na forma como interagimos na vida pessoal, e no mundo dos negócios, e essa regra não é diferente quando o assunto é cibercrime.

Pode-se dizer que, com a difusão da Internet e com o desenvolvimento da utilização dos sistemas computadorizados, tornam-se cada vez mais comuns os episódios em que as pessoas se aproveitam dessas ferramentas para fazer atos que trazem danos a bens jurídicos de terceiros. O desvalor feito por intermédio desses meios não tem fronteiras, pois de um computador localizado num país pode-se acessar um sistema e manusear suas informações, sendo que os efeitos dessa ação podem ser determinados em outro computador muito distante daquele em que ela foi originada, podendo, até mesmo, estar situado em um país bem distante (ROSA, 2005).

Ora, falar de Crimes Virtuais implica, necessariamente, trabalhar a complexidade da sua definição, pois envolve a tecnologia em constante evolução, culturas diferentes, atitudes que não conhecem fronteiras, em face de não existir limites predeterminados, gerando problemas de competência territorial.

Torna-se importante destacar de acordo com o que vem sendo exposto na literatura, cada dia mais vem crescendo os números de pessoas que acessam a internet existem mais de 800 mil websites na internet, e a cada dia são criadas mais de mil *homepages* por dia, e isso vem acontecendo, pois, na internet se encontra basicamente tudo, desde comprar um eletrônico qualquer, até mesmo concluir um curso universitário pela internet, o que acontece é que os usuários que ali se

encontram estão sujeitos aos mais variados crimes, estes, que não encontram barreiras para perpetuar-se por toda a rede, deixando estragos imensos na vida dos internautas de boa fé (PINHEIRO, 2010).

Por um lado, mesmo sendo avaliada como sendo uma revolução as novas tecnologias não trouxeram somente benefícios à população, pois destaca-se que, com a evolução do mundo digital cresce em todo o mundo crimes e criminosos que se qualificam em na execução destes por meio da informática.

2.1 Crimes virtuais

Os crimes virtuais são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, contudo todos são praticados contra ou com a utilização dos sistemas da informática.

Para muitos autores, tal como Castro (2003) os crimes virtuais são considerados como próprios e impróprios. Os primeiros são aqueles que só podem ser praticados através da informática. São os típicos crimes do mundo virtual, tendo em vista que existem única e exclusivamente em razão da informática. Aqueles realizados com a utilização do computador são denominados crimes virtuais impróprios, ou seja, por meio da máquina que é aproveitada como instrumento para prática de condutas ilícitas.

Quando tratamos sobre crimes digitais, estes podem ser conceituados como sendo, às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações aos direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros (PINHEIRO, 2010).

Martins (2012, p.78) leciona que:

> Destarte, o mundo cibernético tem sido alvo da atuação crescente de criminosos, que encontram na internet um meio fácil de cometer crimes, muitas vezes, aproveitando-se do anonimato, o que é vedado pela Constituição Federal, e da falsa impressão de que são impunes, ou pela falta de legislação específica, ou pela dificuldade na investigação criminal em encontrar os autores. É importante ressaltar que os usuários facilitam muito a prática destes ilícitos, tornando-se presas fáceis, pois ao acessar informações bancárias utilizando dados sigilosos, bem como a exposição da imagem, sem os devidos cuidados, acabam por favorecer a criminalidade cibernética.

2.2. Sujeitos ativo e passivo

O senso comum nos apresenta os Hackers como sendo os responsáveis por todos os crimes virtuais, e embora exista um leque de denominações para identificar os autores dos crimes virtuais, esse nome trata apenas de uma conceituação básica e genérica.

Os chamados Hackers são aqueles que normalmente modificam softwares, desenvolvendo novas aplicações, encontrando falhas em sistemas, ajudando a corrigi-las, etc. Por serem aqueles que utilizam todo o seu conhecimento para melhorar a segurança, de forma legal, foram intitulados como “White-hats” (chapéus brancos).

Já os Crackers, por outro lado, são os verdadeiros invasores de computadores e sistemas, inclusive comparados a terroristas. Utilizam o conhecimento da informática com propósitos ilícitos, são conhecidos como “Black-hats” (chapéus negros).

Quanto ao sujeito passivo do delito cibernético, há uma singularidade, uma vez que, figura o polo passivo dos crimes cibernéticos aquele a quem recaiu a ação ou omissão, seja a pessoa física ou jurídica, assim sendo a vítima, que podem ser prejudicadas de forma individual ou coletivamente.

2.3. Os crimes mais praticados

2.3.1 Invasão de Privacidade

A quantidade de informações que podem ser guardadas e transmitidas é de tal amplitude que se exige o estabelecimento de soluções para os problemas que podem derivar da relação entre informática e intimidade. O alcance cada ocasião maior das informações e o incremento das possibilidades e dos recursos tecnológicos fazem da Internet um espaço peculiar, com problemáticas e situações novas a serem enfrentadas pelo homem moderno, lançando, deste modo, expectativas desafiadoras para a ciência do Direito (CANOTILHO, 2012).

Conforme os dados e informações divulgados na Internet são de difícil controle, uma vez que a própria estrutura em que ela é fundamentada (interligação entre computadores em todas as partes do mundo) tem caráter fundamentalmente libertário. As informações circulam em grande velocidade e atingem um número vasto de pessoas, tornando-se, portanto, cada vez mais frequente a divulgação de dados e de fatos que necessitariam se manter circunscritos à intimidade das

pessoas. Quanto à matéria do direito à intimidade e à vida privada nos dias atuais, Eduardo Akira Azuma (2012, p.90) distingue:

> A importância de tais direitos vai crescendo na medida em que a autonomia da vida privada é ameaçada pelas novas modalidades de invasão científica e tecnológica. A intimidade e a privacidade ganham status de grande importância em razão da valorização e comercialização de dados pessoais, ação implacável da cultura de massas, algumas ações de cunho totalitário por parte dos Estados, uso nocivo dos meios tecnológicos entre outros.

Agravando a condição, de crimes virtuais um dos negócios promissores na economia consiste na negociação de dados particulares. Este ocorre em meio aos Estados e instituições privadas que produz uma exata rede de toca de informações, visando ações de *marketing* direcionado, ações contra crimes, preparação de perfis virtuais, entre outros.

Destarte, o direito necessita adequar-se às novas afrontas que a intimidade, a vida particular e as informações reservadas das pessoas suportam em consequência da Internet e das novas ferramentas que toleram a troca de informações. As inviolabilidades constitucionais à residência e ao domínio privado do indivíduo já não asseguram extensa tutela quando se trata, por exemplo, de autoridade sobre informações particulares (VIDAL, 2010).

A respeito de o assunto esclarecem Lucca; Simão Filho; Domingues, (2012, p.122):

> Sob este ponto de vista a Internet torna-se, especialmente, perigosa, pois se apresenta como um veículo de comunicação sem fronteiras, podendo as informações e publicidades que nela navegam atingir uma pessoa em qualquer parte do globo, ou mesmo à população de todo o mundo. Por isso, as disposições legais que possam ser aplicadas, analogicamente, a tudo que envolve a Internet, especialmente aquilo que se relacione à informação, à publicidade, assim deve ser, enquanto não houver adaptação legislativa, daquilo se fizer necessário, ou a criação de normas específicas.

O recolhimento de dados particulares através dos aparelhos automatizados, sem que ao menos o cidadão tenha ciência que suas informações estão sendo armazenadas e analisadas; o intercâmbio de dados por meio de órgãos públicos ou através de corporações, expandindo expressivamente o número de informações; a disposição de armazenamento de infinitos dados; a sucessiva redução dos gastos de geração, difusão, memorização e tratamento de informações; e, por fim, por mais modestos que possam parecer particularmente determinadas informações, os saldos cada vez mais intricados dos tratamentos informatizados,

com real risco de invasão da privacidade e da intimidade das pessoas, tornam imperativa a consagração, no Brasil e no mundo, desse original direito (GUERRA, 2004).

A popularização da Internet; a expansão das comunicações e a era das informações; proporcionaram vantagem ao aparecimento de originais métodos de abuso ao direito à privacidade. Deste modo, é necessária uma reestruturação, até mesmo uma nova concepção acerca deste direito.

2.3.2 Estelionato

O crime de estelionato encontrou na internet um campo abundante para prática de delitos, uma vez que é possível cometer crimes dos mais diversos tipos sem mostrar o rosto, ou correr o risco da prisão em flagrante.

Criminosos engenhosos se aproveitam do suposto anonimato, para ludibriar vitimas, auferindo dinheiro, patrimônio e até vantagens pessoais facilmente.

Uma das formas mais recorrentes do estelionato no ciberespaço é a invasão do correio eletrônico da vítima, em particular o daquelas pessoas que possuem o costume de consultar seus saldos e extratos bancários pelo computador. Nesta situação, o estelionatário (*cracker)* encontra alguma maneira de clonar a página legítima do internet banking do usuário e fazer com que ele tente fazer o acesso, sem saber que os dados que estão sendo inseridos serão interceptados por um terceiro de má-fé que irá usá-los indevidamente (INELLAS, 2009).

No ano de 2011, uma nova modalidade de crime de estelionato virtual foi identificada pela Policia Federal do Estado de São Paulo. Na operação chamada de “tentáculos”, a polícia prendeu 11 pessoas, que por meio de maquinetas de cartão de crédito e débito devidamente adulterados, instalados em estabelecimentos comerciais obtinha as senhas dos clientes, situação esta realizada com a colaboração dos próprios lojistas. Ocorria que os clientes logo que digitavam suas senhas nas maquinas fraudadas, tinham suas senhas clonadas sem que soubessem, visto que havia um *lap top* conectado a rede de por meio de tecnologia *weriless,* em poder dos criminosos, que em sequência utilizavam as informações bancárias obtidas, para efetuarem saques e compras.[3]

---

*FOLHA.COM. Disponível em: <http//:www1.folha.uol.com.br/cotidiano>. Acesso em:19 de abr. 2011.

Desse modo, os hackers, podem em minutos subtrair altos valores, sem saírem de casa, apenas invadindo um dispositivo ou clonando dados bancários das vitimas.

Vale destacar, para que seja configurado estelionato é preciso o emprego do artifício ardil, induzir a vítima em erro, obtenção da vantagem ilícita, prejuízo alheio. Assim se faz que com duplo resultado, vantagem ilícita e prejuízo alheio, conexo com a fraude e o erro que provocou (DELMANTO, 2016).

2.3.3 Crimes Contra a Honra

Os crimes contra a honra (difamação, injuria, calúnia) praticados na internet, mesmo que em páginas internacionais a exemplo do *Twitter* e *Facebook.* Em regra, trata-se de competência da justiça estadual. Contudo para divulgação de fotos e vídeos pornográficos de crianças e adolescentes, a competência é da justiça federal. Conforme o disposto no Estatuto da Criança e do Adolescente:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa (ANGHER, 2015, p.1064).

Uma reportagem publicada no site Jus Brasil mostra que as mulheres são a maioria entre as vítimas de crimes contra a honra, em uma faixa etária de 25 a 45 anos, e a maioria com formação superior. Em pesquisa feita pelo jornal O Dia, Alves e Capelli (2014), mostra que entre os adolescentes de 11 a 17 anos, os crimes contra a honra aparecem em destaque. Segundo Drechsel (2016), de maneira geral, crianças e jovens são as principais vítimas de crimes cibernéticos.[*]

A Carta Magna, em seu art. 5º, X, proclama a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Afere-se, por conseguinte, que o direito à intimidade é preceito constitucional fundamental, e carece ser protegido, ressaltamos assim, a missão do Estado de promover a proteção e promoção de uma vida com dignidade a todos.

2.3.4 Pedofilia

[*] ATHENIENSE, Alexandre. Mulheres são maiores vítimas de crimes contra a honra na internet. Disponível em: ,https://alexandre-atheniense.jusbrasil.com.br/noticias/2103190/mulheres-sao-maiores-vitimas-de-crimes-contra-a-honra-na-internet>

A pedofilia é considerada um crime que sempre da origem a muita comoção social, entretanto não é difícil se deparar na internet, com imagens que apresentam conteúdos pornográficos envolvendo menores e por muitas vezes crianças, diante disso, um dos poucos crimes que apresenta sua ação na internet tipificada é a pedofilia pelo meio do artigo 241, inciso II, do ECA que assim "assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo" (VELOSO, 2014 p.44).

De acordo com a visão de Batista (2004 apud MORAIS, 2018), que é fundador do site *Censura* que combate a pedofilia e abuso sexual na internet, os computadores das vítimas podem em muitos casos estar interligadas com redes de pedofilias, que muitas das vezes, as crianças enviam fotos para amigos ou colegas de classe e essa imagem acaba caindo na rede dos pedófilos. Ou porque alguém ligado ao colega que recebeu a foto está em uma rede de pedofilia, ou porque a imagem foi colocada em algum blog e, com isso, se tornou pública.

Santos; Andrade; Morais (2009) destacam que, quando o problema está na dificuldade de identificação dos infratores (ciberpedófilos), diante do anonimato oferecido pela internet, é importante salientar que esse anonimato que impede a identificação não é absoluto. Identificar o infrator que se esconde atrás da tela de um computador não é uma tarefa impossível. Uma das possibilidades seria através do número IP (*Internet Protocol*) que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc.), sabendo esse número é possível chegar ao computador de onde se originou a atitude delituosa, identificando assim o criminoso.

Ocorrer que muitas vezes, crimes como esses, e outros já citados acima ficam impunes, e isso cada vez mais vêm se tornando um grande problema na vida de muitas pessoas. Indivíduos e famílias que se sentem violadas, pois pode-se dizer que sem uma legislação e fiscalização mais severas, o surgimento de comunidades criminosas agindo neste sentido tem sido facilitado. E graças ao anonimato, os criminosos se vangloriam de delitos por eles exercidos na internet.

3. LEGISLAÇÕES VIGENTES E PROJETOS EM DISCUSSÃO

3.1. Lei dos Crimes Cibernéticos (Lei 12.737/2012) conhecida como Carolina Dieckmann

A lei 12.737/12 ficou popularmente conhecida como “lei Carolina Dieckmann” em virtude do episódio com a atriz, que em maio de 2012, teve seu computador invadido por criminosos que divulgaram 36 fotos íntimas da mesma, causando um grande transtorno e constrangimento à vítima. A pena para esse tipo de crime prevê de seis meses a dois anos de reclusão, conforme o art. 154-A do código penal: “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” (OLIVEIRA, et. al. 2017 p.119).

A lei 12.737/2012 pela primeira vez no direito brasileiro dispõe sobre a tipificação criminal de delitos informáticos, permitindo a responsabilização penal dos infratores, vez que até então o Código Penal não possuía artigos que tratassem especificamente de crimes eletrônicos. Foram acrescentados ao Código Penal, por meio da lei em questão, os artigos 154-A e 154-B, e foram alterados os artigos 266 e 298. O artigo 154-A tipifica o crime de invasão de dispositivo informático, seja este conectado ou não à rede de computadores, através de violação de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo (PIOLI, 2015).

Outro ponto importante a ser destacado é que, por um lado o caput do dispositivo (art. 154-A do CP) desde seu desenvolvimento vem sendo considerado o maior avanço proporcionado por essa norma. Lembrando que, os novos artigos inseridos no Código Penal brasileiro pela Lei 12.737/2012 têm como objetivo principal ser possível combater a invasão de dispositivos informáticos alheios, conectados ou não à rede de computador. Importante salientar que se entende por dispositivos informáticos: computador de mesa, *notebook, laptop, ultrabook, tablete, ipad, smartphone* etc.

Uma questão relevante a ser mencionada é que ambos os artigos acima citados buscam proteger de quaisquer violações os dispositivos informáticos, senão vejamos:

> 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.

Apesar de a Lei n° 12.737/2012 ter ingressado no ordenamento jurídico, tem-se infelizmente assistido ataques cada vez mais complexos, trazendo resultados desastrosos em diversos países, sem a devida identificação e punição desses cibercriminosos.

3.2. Marco Civil da Internet (Lei 12.965/2014)

Com o passar dos tempos foi sendo constatada a importância da Internet e com isso veio também à necessidade da preservação do direito fundamental de liberdade de expressão, juntamente com a influência que o caso *Snowden*[*] proporcionou o Estado Brasileiro optou em aprovar a normatização da Internet em território brasileiro, concedendo direitos aos usuários e estabelecendo deveres a todos os envolvidos, por meio da Lei nº 12.965, de 23 de abril de 2014, denominada de Marco Civil da Internet (BRASIL, 2014).

[*] **Edward Joseph Snowden** é um analista de sistemas, ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global do Sistema de Segurança dos EUA. A revelação deu-se através dos jornais The Guardian e The Washington Post, dando detalhes da Vigilância Global de comunicações e tráfego de informações executada através de vários programas. Em reação às revelações, o Governo dos EUA acusou-o de roubo de propriedade do governo, comunicação não autorizada de informações de defesa nacional e comunicação intencional de informações classificadas como de inteligência para pessoa não autorizada.

A lei acima mencionada surgiu com perspectivas de promover um movimento considerável na relação dos usuários com a rede, com o Estado e com os atores privados que ocupam posições relevantes nesse cenário. Além do conteúdo, o aspecto do processo de construção é particularmente enaltecido no caso do Marco Civil. Lemos (apud LUCCA; SIMÃO FILHO; LIMA, 2015, p.75) exalta a importância democrática da iniciativa, justamente devido a seu processo de criação. Nas palavras de Lemos (apud LUCCA; SIMÃO FILHO; LIMA, 2015, p.75), o Marco Civil da Internet é "um dos principais exemplos globais de lei redigida por meio de procedimentos abertos e colaborativos".

Pode-se dizer um dos assuntos mais polêmicos entre os doutrinadores de Direito Penal que trata da Informática é a conceituação, pois essa vem, muitas vezes, em forma limitativa ou então abrangente demais, não conjecturando as muitas circunstâncias em que se condizem os crimes de informática (PINTO FERREIRA, 2007).

O Marco Civil da Internet, assim como no caso dos dados pessoais, não colocou de forma expressa o que seria os dados sensíveis e o que são englobados por eles, apesar de determinar em sua redação a necessidade de uma maior proteção. Essa situação acontece devido a dificuldade em se determinar o que seriam os dados sensíveis, levando em consideração que o momento e a finalidade de cada dado pode ou não violar a intimidade de seu titular.

Na pesquisa realizada por Rodriguez (2009, p.45) conclui-se que:

> (...) juristas vêm se apresentando relutantes em definirem um conjunto de informações que possam ser declaradas, per se, sensíveis, sem considerar todo o contexto de sua utilização, publicização ou outras formas de tratamento. Nesta mesma linha, podemos verificar a Declaração Internacional sobre Dados Genéticos Humanos da UNESCO (DIDGH), salientando que tais dados serão especialmente protegidos em função de seu contexto. Em contrapartida, no entanto, a maioria dos Estados membros da União Europeia já apresentam um arraigado pensamento de que existiriam certas categorias de dados que sempre seriam capazes de lesar a esfera íntima da pessoa.

Em relação às condutas que são consideradas como sendo não tipificadas Gouveia (2007) menciona as invasões, os vírus de computador e a destruição de informações e assevera que esses e outros delitos habituais ou antigos, como pornografia infantil, racismo e violência moral, que vêm sendo exercidos no ciberespaço, estão trazendo danos reais à vida das pessoas.

Destaca-se que, em sua obra “Direito Penal Informático”, Britto (2013, p. 153) em um de seus escritos destaca que:

> Cabe aos cientistas do Direito a continuação das incursões doutrinárias, principalmente no Direito comparado, a fim de atingirmos um maior grau de eficácia na aplicação da lei penal sem perder o respeito aos princípios e fundamentos do atual Estado Democrático e Social de Direito.

Portanto, ressalta-se que, decretar uma lei específica torna-se imprescindível não somente para preencher as lacunas deixadas pelo Marco Civil da Internet e proteger melhor o cidadão, mas igualmente deve apresentar como objetivo principal uniformizar o significado dos conceitos essenciais para a proteção de dados e coordenar as políticas internas e externas do Brasil.

3.3. PROJETOS DE LEI EM TRAMITAÇÃO

3.3.1. PL Nº 5555/2013 – Autor: Deputado João Arruda - PMDB/PR[*]

Aborda sobre disseminação não consensual de imagens íntimas, conhecida como “revenge porn”, ou “pornografia de vingança”. Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha - criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação.

*NOVA EMENTA: Inclui a comunicação no rol de direitos assegurados à mulher pela Lei Maria da Penha, bem como reconhece que a violação da sua intimidade consiste em uma das formas de violência doméstica e familiar; tipifica a exposição pública da intimidade sexual; e altera a Lei n° 11.340 de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal).

3.3.2. PL Nº 6.989/2017 – Autor: Deputado Odorico Monteiro – PROS/CE[*]

Propõe mudar lei, retirando do ar, sites, vídeos e outros mecanismos que sugiram ou fomentem indivíduos a atentarem contra a própria vida.

---

[*] BRASIL. **Projeto de Lei nº 5.555/2013.** Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha - criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=576366>. Acesso em 01. jun. de 2019.

[*] BRASIL. **Projeto de Lei nº 6989/2017**. Altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, para incluir procedimento de retirada de conteúdos que induzam, instiguem ou auxiliem a suicídio de aplicações de internet. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2124329>. Acesso em 01. jun. de 2019.

*EMENTA: Altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, incluindo procedimento de retirada de conteúdos que induzam, instiguem ou auxiliem a suicídio de aplicações de internet.

3.3.3 PL N.º 9.744, DE 2018 – Autor: Deputado Sr. Sandro Alex - PSD/PR[*]

*EMENTA: Obriga a criação de mecanismos de identificação em anúncios publicitários na internet e responsabiliza aquele que administra, intermedia ou gerencia tais anúncios em sítio ou aplicação de internet que disponibilize e/ou distribua conteúdo que abarque ilícitos penais.

3.3.4 Projeto de Lei 154/19 – Autor: José Nelto - PODE/GO[*]

Muda o Código Penal (Decreto-Lei 2.848/40) para agravar a pena aplicada a quem comente crimes cibernéticos – praticados por meio eletrônico. Pelo texto, a agravante será aplicada quando o crime for praticado por meio de computador ou outro dispositivo de comunicação conectado ou não à internet.

Hoje em dia, o Código Penal estabelece entre as agravantes o crime por motivo fútil ou torpe, contra pais, filhos, irmãos e cônjuge, com abuso de autoridade.

*EMENTA: Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, para estabelecer uma agravante genérica para os crimes cibernéticos.

4. CIBERCRIME NO BRASIL E NO MUNDO

4.1 No Brasil

Com o surgimento dos ataques informáticos aumentou-se a necessidade de controle do Estado, bem como a de utilizar tecnologia da informação que esteja em profunda e constante modernização.

Possuímos no Brasil uma associação de direito privado com atuação nacional, pouco difundida nas mídias chamada SaferNet Brasil. Fundada em 2015

---

* BRASIL. **Projeto de Lei nº 9744/2018**. Obriga a criação de mecanismos de identificação em anúncios publicitários na internet e responsabiliza aquele que administra, intermedia ou gerencia tais anúncios em sítio ou aplicação de internet que disponibilize e/ou distribua conteúdo que abarque ilícitos penais. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169062 >. Acesso em 01. Jun. de 2019.

* BRASIL. **Projeto de Lei nº 154/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, para estabelecer uma agravante genérica para os crimes cibernéticos. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190632>. Acesso em 01. Jun. de 2019.

por professores e pesquisadores com a finalidade primária de desenvolver projetos voltados ao combate à pornografia infantil. Consolidou-se como entidade de referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, conquistando assim espaço e respeito inclusive no plano internacional, firmando inclusive acordos de cooperação com instituições governamentais, a exemplo do MPF - Ministério Público Federal.

A associação SaferNet possui alguns projetos, dentre eles o INHOPE, que representa a resposta brasileira a um esforço internacional, que reúne atualmente 22 países empenhados em coibir o uso indevido da Internet para a prática de crimes contra os Direitos Humanos.

Contudo, o seu primeiro projeto foi a criação da "Central Nacional de Denúncias de Crimes Cibernéticos", que é única na América Latina e Caribe, e recebe uma média de 2.500 denúncias (totais) por dia envolvendo páginas contendo evidências dos crimes de Pornografia Infantil ou Pedofilia, Racismo, Neonazismo, Intolerância Religiosa, Apologia e Incitação a crimes contra a vida, Homofobia e maus tratos contra os animais.

O último relatório da Central Nacional de Denúncias de Crimes Cibernéticos aponta um crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na internet suspeitas de tráfico de pessoas, e os gastos de US$ 15,3 bilhões para combater crimes cibernéticos no Brasil em 2010.

4.2 CPI de crimes cibernéticos e seu relatório final

Em de 2015, criou-se a CPI de Crimes Cibernéticos, que investigou a prática destes crimes e seus efeitos perante a economia e a sociedade no país. Com a função de investigar quadrilhas suspeitas de desviar dinheiro de bancos e abordar crimes e violações dos direitos humanos na internet, a operação desarticulou um bando suspeito de desviar pela internet mais de R$ 2 milhões de correntistas de bancos variados, e ainda usava parte do dinheiro desviado para comprar armas e drogas.

A mesma CPICIBER[*], encerrou suas atividades divulgando relatório final, fruto de discussões que ocorreram durante dezenas de audiências públicas realizadas no âmbito da CPI. A seguir os oito projetos propostos:

1. Projeto de Lei que estabelece a perda dos instrumentos do crime doloso, em qualquer hipótese, como efeito da condenação;

2. Projeto de Lei que altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático;

3. Projeto de Lei que altera a Lei no 5.070, de 7 de julho de 1966, autorizando o uso dos recursos do Fistel por órgãos da polícia judiciária;

4. Projeto de Lei que inclui os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme;

5. Projeto de Lei que altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, determinando procedimento específico para a retirada de conteúdos que atentem contra a honra e outras providências;

6. Projeto de Lei que altera a Lei das Organizações Criminosas, a Lei da Lavagem de Dinheiro e o Marco Civil da Internet para incluir no rol das informações cadastrais de usuários o endereço de IP;

7. Projeto de Lei que altera o Marco Civil da Internet para possibilitar o bloqueio de aplicações de internet por ordem judicial;

8. Projeto de Lei que adiciona a Educação Digital entre as Diretrizes do Plano Nacional de Educação – PNE;

O relatório indica também ao Poder Executivo para a “adoção de medidas para melhorar a segurança da infraestrutura de tecnologia da informação da Administração Pública”; ao Banco Central, por intermédio do Ministério da Fazenda,

[*] AUGUSTO, ANTONIO. **Comissão Parlamentar de Inquéritos dos Crimes Cibernéticos aprova relatório final**. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/noticias/conheca-as-propostas-do-relatorio-final-da-cpiciber>. Acesso em 02 de jun.2019.

ao próprio Ministério da Fazenda e ao Ministério da Justiça, sugerindo a "adoção de medidas de combate aos crimes cibernéticos"; ao Poder Judiciário, sugerindo a "criação de Varas Especializadas em Crimes Cibernéticos nos Tribunais brasileiros"; e ao Ministro de Estado das Comunicações "sugerindo à Agência Nacional de Telecomunicações a adoção das medidas necessárias para a implantação do IPV6 no país".

4.3. Competência dos delitos virtuais, em âmbito internacional e sua repercussão mundial.

Há situações em que o agente pode estar em diversos espaços virtuais, além de poder ter várias identidades ao mesmo tempo.

Importante dizer que a competência para legislar é soberana em todos os países. Então como submeter um cidadão de um país às leis de outro país, quando os dois se dizem competentes para julga-lo?

Para tratarmos da competência dos delitos virtuais, em âmbito internacional, devemos conhecer os conceitos de crime à distância, que são aqueles que têm a ação ou omissão e consumação fora do território nacional e vice-versa, conforme dispõe o artigo 6º do Código Penal Brasileiro[*], qual seja a da teoria da ubiquidade.

Podemos citar a exemplo de ações realizadas além das fronteiras brasileiras, a "Convenção de Budapeste" (ETS 185), que é um tratado internacional que em seu bojo aborda o direito penal e direito processual penal, firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução. Trata-se basicamente de violações de direito autoral, fraudes relacionadas com computadores, pornografia infantil e violações de segurança de redes. Até de 2 de setembro de 2006, 15 países haviam assinado, ratificado ou aderido à Convenção, enquanto outros 28 apenas assinaram. O Brasil, assim como os demais países da América do Sul, ainda não é signatário da Convenção de Budapeste.

---

[*] "*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"*

Pesquisas realizadas no sentido de averiguar como os demais países atuam, quantificam e qualificam os cibercrimes, são divulgadas constantemente nas mídias digitais, a fim de atualizar os usuários.

Recentemente, duas multinacionais e bastante conhecidas empresa de softwares, a McAfee e a CSIS, divulgaram um estudo anunciando que o cibercrime gera anualmente um prejuízo de quase US$ 600 bilhões para as empresas no mundo todo, número esse que expressa cerca de 0,8% do PIB mundial. É sabido, porém, que grande parte dos ataques cibernéticos não são oficialmente registrados, sendo a assim na realidade, esses números podem ser muito maiores que os informados.

Em entrevista concedida ao site "IT WEB"*, o executivo Raphael Labaca, especialista em educação e pesquisa do laboratório de segurança "*Eset*" na América Latina, explicou os aspectos regionais dos ataques ou ameaças cibernéticas. Afirma que no caso da América Latina, uma das principais dificuldades é a punição dos sujeitos que praticam estes crimes, pois não existe no código penal a tipificação de cibercrime, como crime. Através de estudos elaborados pela "*Eset*", empresa líder em detecção proativa de ameaças, foi possível em relação aos países alvo de cibercrimes, retirar as seguintes conclusões:

Na Rússia, dos crimes mais comuns a invasão de computador alheio está 1º colocado no *ranking*. Ou seja, o sujeito invade o computador e apropria-se do seu domínio, e para que o proprietário possa voltar a usá-lo e o infrator exige um pagamento em dinheiro, cometendo assim um estelionato, sendo necessária a vítima pagar, para voltar acessar seu computador normalmente.

A China é uma das maiores fabricantes de "*malware*", porém descobriu-se que os ataques originados do país não são, normalmente, direcionados para os usuários chineses.

Já na Europa, os crimes virtuais em sua maioria estão voltados para os falsos antivírus que são conhecidos como "Rogues", que são janelas que aparecem no navegador durante alertando o usuário que o seu computador está infectado,

* O IT Forum 365 é uma plataforma social B2B que entrega Conteúdo, Relacionamento e Negócios aos profissionais decisores de TI das maiores empresas. (É uma propriedade da International Data Group, Inc, licenciado pela IT MIDIA.).

pedindo verificação, sugerindo correção, contudo a vitima é cobrada por um serviço que não existe.

Nos Estados Unidos da América, em função da sua extensa dimensão territorial e população, foram identificados os mais diversos tipos de crimes virtuais, desde os ataques ao sistema bancário, como “cavalos de Tróia”, “*botnets*” e outros.

E por último, a América Latina é alvo principalmente de ataques ao setor bancário. As maiorias dos bancos usam a língua oficial espanhola nos seus sistemas, tornando mais fácil os ataques. Por outro lado à criação de “*botnets*”, criados a partir de pendrives infectados são ações muito praticadas em países como o Peru, Chile e Argentina.

Importante salientar que, estes foram os ataques mais comuns identificados na pesquisa realizada pela empresa, o que não atesta que outros tipos de crimes não sejam cometidos diariamente.

5. CONSIDERAÇÕES FINAIS

Este artigo tem como objetivo principal, investigar tipos de crimes virtuais, suas possibilidades e os limites da sua regulamentação no Brasil.

O grande segredo da internet é a capacidade de colocar em conexão diferentes redes de computadores, fazendo com que haja uma interação global. Essa conectividade só é possível graças à existência de um protocolo global de informações, o que torna possível diferentes redes e sistemas se comunicarem mutuamente.

Notou-se que, o crescimento da Internet e do uso de redes sociais chegam revolucionando os relacionamentos pessoais e provocando sérias implicações de ordem moral, social, política, econômica e, consequentemente, jurídica. O crescimento da internet trouxe muitos benefícios, mas na mesma dimensão a quantidade dos crimes virtuais aumentou significativamente.

Observou-se que entre os crimes virtuais, a pedofilia domina as práticas criminosas e constitui uma das principais violações de direitos na internet, sendo a pornografia infantil, prática ligada à pedofilia, a violação que mais recebeu denúncias nos últimos anos.

A edição da Lei n. 12.737/2012 constituiu um importante avanço, ao tipificar expressamente o crime de “invadir dispositivo informático”, criando um tipo penal que visou eminentemente proteger o sigilo de dado e informação pessoal ou profissional. Constatou-se também que, o desenvolvimento do Marco Civil da Internet, Lei 12.965/2014, mesmo sendo avaliado como um importante mecanismo para tentar regular e dar mais controle à utilização dos meios digitais, ainda não é suficiente para combater os crimes virtuais.

É praticamente impossível construir um sistema exauriente para a questão da determinação do lugar do crime, pois a internet não conhece barreiras físicas. Não há controle prévio, tampouco centralizado dos dados que circulam, assim sendo quase impossível monitorar o trânsito de tais dados na internet.

A sociedade se encontra em constante evolução, e junto com ela devem caminhar as leis que regem o Estado, sendo alteradas e modificadas sempre que necessário para que o país continue se desenvolvendo de forma justa e igualitária, preservando o bem-estar de seus habitantes.

Compreendemos, porém, que apesar do Brasil ter competência para julgar e processar os cibercrimes, fica muito difícil localizar os autores destes delitos, tendo em mente a facilidade que a internet proporciona de se manter o anonimato.

É válido ressaltar que os recursos tecnológicos, ainda, chegam ao Brasil muito tardiamente, assentando, na maioria das vezes, uma carência de recursos e de profissionais especializados. Além de existirem possíveis conflitos de competência o que pode ter como consequência a certeza da não punição dos delitos.

Fica evidente a necessidade do Brasil, tornar-se um Estado signatário da Convenção de Budapeste, sendo possível acelerarmos questões cibernéticas com os instrumentos jurídicos adequados. Pois o caráter da convenção internacional, sendo multilateral, viabiliza ações efetivas de forma a proteger a sociedade brasileira de riscos globais.

Percebe-se, por fim, que diante do contexto atual que apresenta crescente índice de crimes virtuais, bem como as falhas ainda existentes na legislação, faz-se essencial o desenvolvimento de uma lei especifica e severa contra esses tipos de crimes virtuais.

REFERÊNCIAS

AUGUSTO, ANTONIO. **Comissão Parlamentar de Inquéritos dos Crimes Cibernéticos aprova relatório final**. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/noticias/conheca-as-propostas-do-relatorio-final-da-cpiciber>. Acesso em 02 de jun.2019.

ALVES, Francisco Edson. CAPPELLI, Paulo. **Jovens são vítimas de crimes contra a honra nas redes sociais**. 2014. Disponível em: odia.ig.com.br/odiaestado/2014-05-10/jovens-sao-vitimas-de-crimes-contraa-honra-nas-redes-sociais.html> Acesso em: 19/04/2019.

ANGHER, Anne Joyce. **VADE MECUM**. 20 ed. São Paulo: Rideel, 2015.

AZUMA, Eduardo Akira. **A intimidade e a vida privada frente às novas tecnologias da informação.** Artigo disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=6168. Acesso em: 19/04/2019.

BRASIL. **Lei nº 12.965**. Presidência da República. Nota Oficial. Disponível em: /www2.planalto.gov.br/acompanheo-planalto/notas-oficiais/notasoficiais/comunicado-oficial>Acesso em: 19/04/2019

BRASIL. **Projeto de Lei nº 5.555/2013**. Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha - criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=576366>. Acesso em 01. jun. de 2019.

BRASIL. **Projeto de Lei nº 6989/2017**. Altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, para incluir procedimento de retirada de conteúdos que induzam, instiguem ou auxiliem a suicídio de aplicações de internet. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2124329>. Acesso em 01. jun. de 2019.

BRASIL. **Projeto de Lei nº 9744/2018**. Obriga a criação de mecanismos de identificação em anúncios publicitários na internet e responsabiliza aquele que administra, intermedia ou gerencia tais anúncios em sítio ou aplicação de internet que disponibilize e/ou distribua conteúdo que abarque ilícitos penais. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169062 >. Acesso em 01. Jun. de 2019.

BRASIL. **Projeto de Lei nº 154/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, para estabelecer uma agravante genérica para os crimes cibernéticos. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190632>. Acesso em 01. Jun. de 2019.

BRITO, A. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição**. Imprenta: Coimbra, Almedina, 2012.

CASTELLS, Manuel. **Redes de indignação e esperança**: movimentos sociais na era da internet. 1 ed. Rio de Janeiro: Zahar, 2013.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática**: e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumem Júris, 2003. 236 p.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 9. ed. rev. e ampl. São Paulo: Atlas, 2010.

CHIAVENATO, Idalberto. **Comportamento Organizacional.** Rio de Janeiro: Editora Campus, 2010.

DELMANTO, Celso et. al. **Código penal comentado**. 9. ed. Rio de Janeiro: Renovar, 2016.

DRECHSEL, Denise. **Crianças e jovens são as principais vítimas dos crimes cibernéticos.** 2016. Disponível em: http://periodicos.pucminas.br/index.php/sinapsemultipla/article/viewFile/16488/12745 Acesso em: 19/04/2019.

FELINTO, Erick. **A religião das máquinas**: ensaios sobre o imaginário da cibercultura. Porto Alegre: Sulina, 2005.

GOUVEIA, Flávia. **Tecnologia a serviço do crime**. BR – Notícias do Brasil 2007. Disponível em: <http://www.cienciaecultura.bvs.br/pdf/cic/v59n1/aobv59n1.pdf>. Acesso em:19/04/2019

GUERRA, Sidney. **O direito à privacidade na internet:** uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet**. 2. ed., atual. e ampliada. São Paulo: Juarez de Oliveira, 2009.

KOLB, Anton; ESTERBAUER, Reinhold; RUCKENBAUER, Hans-Walter (Org.). **Cibernética**: responsabilidade em um mundo interligado pela rede digital. São Paulo: Loyola, 2001. p. 57-64. p. 58

LUCCA, Newton de; SIMÃO FILHO, Adalberto; DOMINGUES, Alessandra de Azevedo; FINKELSTEIN, Maria Eugênia. **Direito & internet**: aspectos jurídicos relevantes. [S.l: s.n.], 2008.

LUCCA, Newton De; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira De. **Direito & Internet III**: Marco Civil da Internet Lei no. 12.965/2014. São Paulo: Quartier Latin, 2015. p. 79–100.

MACIEL, Camila. **Cresce número de denúncias de crimes na internet em 2014**. 2015. Disponível em: <http://www.ebc.com.br/noticias/2015/02/cresce-numero-de-denuncias-de-crimes-na-internet-em-2014>. Acesso em: 17 jun. /2017.

MARTINS, Sandra Carla Castro Marques. **Estelionato Eletrônico**: a (des) necessidade de uma tipificação legal 2012. Disponível em: https://repositorio.ucb.br/jspui/bitstream/10869/2819/2/Luis%20Guilherme%20de%20Matos%20Feitoza.pdf Acesso em: 19/04/2019

MIGUEL, Katarini Giroldo. **A expressão dos movimentos ambientais na atualidade**: mídia, diversidade e igualdade. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação XXX Congresso Brasileiro de Ciências da Comunicação – Santos – 29 de agosto a 2 de setembro de 2007.

MORAIS, Lucas Andrade de. **Ciberpedofilia**: os crimes de pedofília praticados através da internet. Conteúdo Jurídico, Brasília-DF: 27 abr. 2018.

Nucci. Guilherme de Souza. 2014. Manu**al de direito penal: parte geral e parte especial**. 10ª ed. Rio de Janeiro. Forense: Revista atualizada e ampliada.

OLIVEIRA, et. al. **Crimes Virtuais e a legislação brasileira**. (RE) Pensando direito. Revista do Curso em Graduação em Direito do Instituto Cenecista de Ensino Superior de Santo Ângelo. EDIESA Ano 7 n. 13 jan./jun. 2017 p. 119 – 130.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.65

PINTO FERREIRA, Lóren Formiga. **A Eficácia da Lei Penal Brasileira Frente aos Crimes Praticados Por Intermédio dos Sites de Relacionamento**. Bagé: URCAMP, 2007.Monografia, Faculdade de Direito, Universidade da Região da Campanha, 2007.

PIOLI, Roberta Raphaelli. **Delitos Informáticos**: Lei Carolina Dieckmann traz inovações necessárias Revista Consultor Jurídico, abril 2013.

RODRIGUEZ, Daniel Piñeiro. **A proteção de dados pessoais sensíveis no contexto do estado democrático de direito**. 2009. Disponível em: < http://www.pucrs.br/edipucrs/IVmostra/IV_mostra_pdf/direito/72217daniel_pineiro_rodriguez.pdf >. Acesso em: 19/04/2019

ROSA, Fabrízio. **Crimes de informática**. 2. ed. Campinas: Bookseller, 2005.

ROZA, Anderson Figueira Da. **As redes sociais no mundo do crime**. 2016. Disponível em: canalcienciascriminais.com.br/as-redes-sociais-no-mundo-do-crime> Acesso em: 01/04/2019

SANTOS, Gustavo de Oliveira; ANDRADE, Izabella Lucena Medeiros de; MORAIS, Lucas Andrade de. A Responsabilidade Civil dos Estabelecimentos Fornecedores de Serviço de Acesso à Internet nos "Cybercrimes". **Unieducar**, Fortaleza, ano XI, n. 4880, 2009.

SOUSA, M. W. (org). **Recepção mediática e espaço público**: novos olhares. São Paulo: Paulinas, 2006.

Valin, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela Internet.** In Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 115.

VELOSO, Fernando de castro, **informática: conceitos básicos**. 9 ed.Rio de Janeiro, Elsevier 2014.

VIDAL, Gabriel Rigoldi. **O direito à privacidade, os bancos de dados e as novas tecnologias.** Jus Navigandi, Teresina, ano 15, n. 2626, 9 set. 2010