



ESTADO DE MATO GROSSO
UNIVERSIDADE DO ESTADO DE MATO GROSSO
CAMPUS UNIVERSITÁRIO DE PONTES E LACERDA
FACULDADE DE CIÊNCIAS AGRÁRIAS E HUMANAS
BACHARELADO EM DIREITO



PAULO LINO DA SILVA

CRIMES DIGITAIS E SUA ADEQUAÇÃO AOS TIPOS PENAIIS

Pontes e Lacerda – MT
2018

PAULO LINO DA SILVA

CRIMES DIGITAIS E SUA ADEQUAÇÃO AOS TIPOS PENAIIS

Trabalho Conclusão de Curso apresentado como exigência parcial para obtenção do título de Bacharel em Direito à Universidade de Mato Grosso - UNEMAT, sob a orientação do Professor Esp. JOACIR MAURO DA SILVA JUNIOR.

Pontes e Lacerda – MT

2018

TERMO DE APROVAÇÃO

PAULO LINO DA SILVA

CRIMES DIGITAIS E SUA ADEQUAÇÃO AOS TIPOS PENAIS

Trabalho de conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Direito, no Curso de Bacharelado em Direito, da Universidade do Estado de Mato Grosso.

Em ____/____/____, a banca examinadora considera aprovado o Trabalho de Curso do Acadêmico PAULO LINO DA SIVA, para obtenção do Grau de Bacharel em Direito.

Orientador:

JOACIR MAURO DA SILVA JUNIOR
Universidade do Estado de Mato Grosso

Membros da banca:

CHRISLAYNE KERINA FERREIRA LOPES - 1º membro examinador
Universidade do Estado de Mato Grosso

FERNANDO HENRIQUE VIOLA DE ALMEIDA - 2º membro examinador
Universidade do Estado de Mato Grosso

Deus seja louvado.....

RESUMO

O referido trabalho discute aspectos do fenômeno dos crimes digitais, bem como as possíveis consequências jurídicas aplicadas atualmente na legislação vigente em nosso país segundo classificação doutrinária adotada. Para tal discussão foi feita uma pesquisa bibliográfica, para verificar como se adequa a legislação para amparar legalmente os crimes no ciberespaço. Será apresentado as dificuldades que os operadores do direito vem enfrentando pela falta de uma legislação específica para os crimes virtuais e para fazerem adequação à legislação para amparar legalmente os crimes no ciberespaço. E analisaremos a competência para processar e julgar os processos dos crimes no ciberespaço, e apresentaremos alguns julgados sobre os referidos assuntos.

Palavras chave: Ciberespaço, Tipos Penais, Legislação.

ABSTRACT

This paper discusses aspects of the phenomenon of digital crimes, as well as the possible legal consequences currently applied in the legislation in force in our country according to the adopted doctrinal classification. For such discussion a bibliographical research was done, to verify how the legislation is adapted to legally support crimes in cyberspace. It will present the difficulties that law enforcement has been facing due to the lack of specific legislation for cyber crimes and to adapt to legislation to legally protect crimes in cyberspace. And we will analyze the competence to process and prosecute crimes in cyberspace, and we will present some judgments on those matters.

Key words: Cyberspace, Penalty Types, Legislation.

SUMÁRIO

INTRODUÇÃO	8
1 HISTORIA DA INFORMATICA E CRIMES VIRTUAIS	9
1.1 Origem e Evolução da Internet.....	9
1.2 O Conceito de Crime Virtual	10
1.3 Fraudes Virtuais	11
1.3.1 Estelionato	11
1.3.2 Invasão de Privacidade	12
1.3.3 Crimes Contra a Honra	13
1.3.4 Crimes Contra a Propriedade Intelectual	14
2 A NECESSÁRIA ADEQUAÇÃO TÍPICA DOS CRIMES VIRTUAIS	16
2.1 Legislação Nacional de Uso dos Meios Eletrônicos.....	16
2.2 Marco Civil da Internet e a Lei 12.737/2012.....	17
2.3 Legislação Internacional em Relação aos Crimes Virtuais	18
2.3 Crimes Virtuais e sua Dificuldade de Instrução Probatória	20
2.4 Provedores de Acesso à Internet a Suas Responsabilidades.....	22
3 REFORMA DO CODIGO PENAL PARA ADEQUAÇÃO A TECNOLOGIA.....	24
3.1 Competência para Processar e Julgar	25
3.2 Julgados envolvendo a prática de crimes virtuais.	26
CONSIDERAÇÕES FINAIS	34
REFERÊNCIAS BIBLIOGRÁFICAS	35

INDRODUÇÃO

O presente trabalho tem o objetivo de apresentar os principais aspectos do fenômeno dos crimes digitais, bem como as possíveis consequências jurídicas aplicadas atualmente na legislação vigente em nosso país segundo classificação doutrinária adotada. Foi feito uma pesquisa bibliográfica, para verificar como se adequa a legislação para amparar legalmente os crimes no ciberespaço.

O trabalho está dividido em três capítulos. No primeiro capítulo abordaremos história da informática e crimes virtuais, neste capítulo faremos um panorama histórico desde o surgimento do computador, da internet bem como a evolução das tecnologias e como os crimes virtuais estão inseridos na legislação vigente.

No segundo capítulo será apresentado a adequação da legislação para amparar legalmente os crimes no ciberespaço. Neste capítulo será apresentado as dificuldades que os operadores de direito vem enfrentando pela falta de uma legislação específica para os crimes virtuais, o que os levam a fazer adequações na legislação para amparar legalmente os crimes no ciberespaço.

No terceiro capítulo analisaremos a competência para processar e julgar os processos referentes a crimes no ciberespaço. Vale lembrar que existem diversas formas de definir a competência de cada juízo, seja pela matéria, seja pelo território, ou até pela função. E apresentaremos alguns julgados sobre os referidos assuntos.

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

1 HISTORIA DA INFORMATICA E CRIMES VIRTUAIS

1.1 Origem e Evolução da Internet

O computador, máquina que nos últimos anos tem substituído vários afazeres humanos, tem sido um dos meios para se cometer crimes de informática, apesar de que os mesmos podem ser praticados também com o telefone, que são dotados de funcionalidades informatizadas, com cartões de crédito, celulares etc., porém é a ferramenta mais utilizada já que é utilizado por um número cada vez maior de pessoas, de todas as classes sociais.

Castro (2003, p. 1), trata da conceituação do computador:

Computador é conceituado como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle. Em um último sentido, pode ser considerado como uma máquina que manipula informações sob diversas formas, podendo receber, comunicar, arquivar e recuperar dados digitais ou analógicos, bem como efetuar operações sobre lei.

A internet surgiu no período da Guerra Fria e foi criada para que as forças armadas norte-americanas mantivessem informadas em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações. Nas décadas de 70 e 80, além de ser utilizada para fins militares, a Internet também foi um importante meio de comunicação acadêmico. Foi só na década de 90 que a Internet começou a alcançar a população em geral. Foi nesta época que a internet foi popularizando e passou a ser utilizada por vários segmentos sociais.

A partir de então fica difícil imaginar o mundo sem a Internet. Ela está presente nas escolas, faculdades, empresas e diversos locais, possibilitando acesso às informações e notícias do mundo em apenas um *click*.

A primeira rede social foi criada em 1995, com o nome o *ClassMates* criada pelo norte-americano Randy Conrads, tinha o objetivo de reunir amigos da escola e

faculdade. O serviço era pago, mas fez muito sucesso na época entre usuários dos Estados Unidos e Canadá e existe até hoje. No Brasil, a mania de ter amigos pela internet chegou com o Orkut (2004), que leva o nome do dono, o engenheiro turco Orkut Büyükkökten. No mesmo ano surgiu o *Facebook*, criado por Mark Zuckerberg e amigos da universidade. No começo, era apenas para alunos de algumas faculdades. Em 2006, foi liberado para qualquer pessoa (a partir de 13 anos). Hoje, o *Facebook* é a rede social mais popular no mundo, com mais de 1 bilhão de usuários; 67 milhões só no Brasil.

Já em 2010 um novo serviço se expandiu no mundo da Internet: os sites de compras coletivas. Tais sites realizam a intermediação entre consumidores e empresas. Estes sites conseguem negociar descontos para a venda de grande quantidade de produtos e serviços. Os consumidores compram cupons com 50% de desconto ou até mais.

A comunicação nos dias atuais está muito acelerada em questão de segundos o internauta fica sabendo o que está acontecendo do outro lado do mundo, nunca foi tão rápido se comunicar como nos dias de hoje. Especialistas da área estão confiantes quanto aos avanços da internet, muitos acreditam que futuramente os internautas poderão sentir cheiro e sabores ao navegar.

1.2 O Conceito de Crime Virtual

Ao definirmos o que é crime digital pode se dizer que estes são os crimes praticados através da internet ou computadores, geralmente o criminoso atinge a vítima ou computador dela. Alguns vão além e atingem uma rede de computadores completa, como as de empresas, organizações e órgãos públicos. À luz da doutrina, Ramalho Terceiro (2013, p.15) define crime digital com a seguinte ênfase:

[...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

Souza *et al* (2006 p. 25) define que, “O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual.” Já Rocha (2000 p 36) define o crime

de informática como: “Aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos”. Já Almeida, Mendonça e Carmo et al. (2015, p. 223) conceitua crime virtual como: “[...]crime virtual é qualquer conduta antijurídica e culpável, realizada a partir de um computador conectado à internet.”

Diante dos conceitos acima, podemos citar alguns exemplos de crime virtual, quais sejam: furto de informações, desvio de dinheiro de contas bancárias, sites falsos de compra eletrônica, crimes contra a honra (injúria, calúnia e difamação), ameaças, falsidade ideológica, entre outros.

1.3 Fraudes Virtuais

1.3.1 Estelionato

Segundo Greco (2010, p. 486) estelionato é “a concepção equivocada da realidade, é conhecimento falso do que ocorre no mundo real. Assim, aquele que atua movido pelo erro acredita numa coisa enquanto a realidade é outra”.

O crime de estelionato esta tipificado no Código Penal com a seguinte redação:

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

§ 2º - Nas mesmas penas incorre quem:

Disposição de coisa alheia como própria

I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;

Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;

Defraudação de penhor

III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;

Fraude na entrega de coisa

IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;

Fraude para recebimento de indenização ou valor de seguro

V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;

Fraude no pagamento por meio de cheque

VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Estelionato contra idoso

§ 4º Aplica-se a pena em dobro se o crime for cometido contra idoso.

Várias pessoas são enganadas, pensando que estão recebendo um “benefício” porém estão sendo fraudadas por telefone, internet, telefone, etc.

Com a entrega em domicílio, que nos tempos atuais estão em alta, sabendo que há muita compra pela internet e as entregas são realizadas em um tempo hábil. Desta forma tem satisfeito o “prazer” de muitos em realizar tal ação. Neste sentido, tem ocorrido com frequência várias condutas delituosas no ciberespaço, as quais podemos verificar a prática do estelionato. Isto porque pessoas são enganadas com propagandas enganosas em sites falsos ou são vítimas de clonagem de cartão de crédito.

1.3.2 Invasão de Privacidade

O direito à privacidade é elevado a condição de direito fundamental pela Constituição Federal, nos moldes do artigo 5º, inciso X, do Texto Maior. Lafer (pg. 108, 2001) o define como:

[...] o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada.

Assim o direito à privacidade não é estar só, mas exercer o mínimo de privacidade que lhe é permitido, o que nos últimos dias internautas, vem sofrendo serias invasões, pois a segurança digital é rompida a todo momento com pessoas mal intencionadas a lesionar ou infringir o direito de outrem, também o que ocorrera com a atriz Carolina Dieckmann, pois em razão desse acontecimento foi criada a Lei 2793/2011.

Para Dotti (1980, p.27), a vida privada abrange todos os aspectos que por qualquer razão não gostaríamos de ver cair no domínio público; é tudo aquilo que não deve ser objeto do direito à informação nem da curiosidade moderna que, para tanto, conta com aparelhos altamente sofisticados.

1.3.3 Crimes Contra a Honra

Os crimes contra a honra são tipificados no Capítulo V, do Título I (Crimes Contra a Pessoa), da Parte Especial do Código Penal, desde 1940. No entanto, é evidente sua desatualização ao contexto atual, onde as relações sociais estão cada vez mais virtualizadas e o próprio conceito de honra parece ter se alterado, na medida em que atos que constituíam ofensas gravíssimas no passado, hoje são aceitas como ordinárias pela coletividade.

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa [...]

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa [...]

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa. [...]

Deste modo, a calúnia pode ser descrita como imputação falsa de um fato criminoso a alguém, necessita de dolo específico, determinando a imputação de um fato, que deve ser qualificado como crime e que a imputação seja falsa. Damásio de Jesus (2007, p. 219) descreve que a calúnia se configura em:

Constitui crime formal, porque a definição legal descreve o comportamento e o resultado visado pelo sujeito, mas não exige sua produção para que exista crime, não é necessário que o sujeito consiga obter o resultado visado, que é o dano a honra objetiva do agente.

Uma vez que na calúnia existe imputação de fato definido como crime, na difamação o fato é meramente ofensivo a reputação do ofendido. Além do mais, o tipo de calúnia exige elemento normativo da falsidade da imputação, o que é irrelevante no delito da difamação. Enquanto na injúria o fato versa sobre qualidade negativa da

vítima, ofendendo-lhe a honra subjetiva, na difamação há ofensa à reputação do ofendido, versando sobre fato a ela ofensivo.

Crimes contra a honra pela Internet confrontam dois direitos fundamentais do cidadão. De um lado, a liberdade de expressão, que é, por preceito constitucional (art. 5º, IX), independente de censura ou licença. De outro, a honra, que é inviolável (art. 5º, X). Consequentemente, por ambos possuírem assento na Lei Fundamental, caberá ao juiz, no caso concreto, realizar a devida ponderação de qual interesse se sobrepõe, o que, sem dúvida, não é tarefa fácil para o juiz, visto que não é somente a linha de análise dos crimes, mas acarreta junto com os tais, vários quesitos como definir a competência, local do fato, etc.

1.3.4 Crimes Contra a Propriedade Intelectual

Nosso ordenamento jurídico brasileiro garante de forma efetiva e relevante punição a aqueles que praticam crime contra a propriedade intelectual, que compõe tudo aquilo que se oriunda da criatividade humana, esse tipo penal encontra-se mencionado no artigo 184, caput, do Código Penal.

Art. 184. Violar direitos de autor e os que lhe são conexos: (Redação dada pela Lei nº 10.695, de 1º.7.2003)

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente. (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização

expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003).
Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 10.695, de 1º.7.2003)

O legislador se preocupa com a propriedade intelectual de forma geral. Porém o enfoque aqui apresentado é exposição de obras literárias, musicas, etc, que diariamente estão expostas na rede de internet e raramente são penalizados os infratores por falta de uma especificidade legislativa e condições informatizáveis do judiciário de uma forma geral.

1.3.5 Crimes cibernéticos e autoria

Na atual sociedade, o ambiente cibernético é um ambiente frequentado por todo tipo de pessoas e não se restringe a uma comunidade. A presença física e o espaço geográfico não são mais fundamentais para a realização de atos ou fatos jurídicos. A sociedade cibernética traz a mudança no conceito de fronteira física com o surgimento de nova concepção de jurisdição. Porém, tais atos, vai além daquilo que imaginamos, quando digitamos uma frase ou publicamos algo em redes sociais. Neste contexto pensa-se, qual juiz seria apto para julgar uma lide ou um crime de tamanha extensão? Segundo Lima (2003, p. 70):

Delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.

Deste modo o conhecimento do julgador para com as tecnologias deveria ser extremamente amplo, pois o mesmo deveria conhecer o ambiente cibernético citado, ou sem medo de aplicação da lei colocasse tudo o que lê em pratica, pois a codificação para crimes digitais está caminhando e como Lima disse é uma área que está aberta, facilitando aos infratores e causando dificuldade aos que deveriam inibir tais condutas.

2 A NECESSÁRIA ADEQUAÇÃO TÍPICA DOS CRIMES VIRTUAIS

2.1 Legislação Nacional de Uso dos Meios Eletrônicos

O Direito Penal está totalmente ligado a Internet, visto que as relações que ali são firmadas são entre indivíduos, e estes devem ter suas condutas disciplinadas, sendo que cabe ao Direito disciplinar e regulamentar as condutas entre os membros desta sociedade digital. Neste ponto encontram-se relacionadas as leis, decretos, medidas provisórias, instituições normativas, resoluções e portarias que deram origem a diversos instrumentos de comunicação como:

A Internet é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos com o propósito de servir progressivamente usuários no mundo inteiro. A internet se tornou indispensável para grande parte da população mundial. Nessa rede é possível pesquisar, estudar, jogar, assistir vídeos, namorar, comprar, trabalhar e até praticar crimes.

A internet pode proporcionar muitos benefícios aos usuários, porém tem que ter muito cuidado ao usá-la, pois no mundo virtual existem muitos criminosos e o grande problema desses delitos praticados na internet é a ausência quase total de punibilidade pelo Estado. Isto porque a criminalidade digital avançou mais rapidamente do que legislação no Brasil e as técnicas para chegar ao autor do crime ainda estão em fase de aprimoramento.

Dessa maneira enquanto não temos uma legislação específica para os crimes virtuais, os operadores do direito fazem enquadramento da legislação para amparar legalmente os crimes no ciberespaço.

A Lei 9.296, de 24/07/1996, trata da interceptação telefônica e regulamenta o inciso XII, parte final do art. 5º da Constituição Federal. Essa lei tem gerado controvérsia quanto a sua aplicação na Internet, referindo-se a sua aplicação ou não aos e-mails. Entretanto, há uma corrente doutrinária favorável que garante a sua aplicação e proteção quanto ao sigilo das comunicações estabelecidas no mundo virtual, impondo limites à inviolabilidade e a privacidade na rede.

O delito de estupro, tipificado no artigo 213 do Código Penal (CP), reúne duas condutas distintas, a saber: a prática de conjunção carnal (primeira parte) ou de atos libidinosos (segunda parte), mediante constrangimento da vítima, exercido através de violência ou grave ameaça. Ato este que não está expresso, porém se enquadra nos

moldes da vida *online*, pois o mesmo não necessita de uma conjunção carnal, basta somente um constrangimento à vítima.

2.2 Marco Civil da Internet e a Lei 12.737/2012

A Lei nº 12.737, de 30 de novembro de 2012, foi denominada socialmente pela mídia como a Lei Carolina Dieckmann, tal apelido se deu em razão da repercussão do caso no qual a atriz teve seu computador invadido e seus arquivos pessoais subtraídos, inclusive com a publicação de fotos íntimas que rapidamente se espalharam pela internet através das redes sociais. A atriz vitimada então abraçou a causa e acabou ficando conhecida pelo nome da atriz, que extraoficialmente recebera o nome da atriz.

Esta lei foi considerada um avanço para o ordenamento pátrio, todavia não solucionou e nem teria como solucionar o problema legislativo concerte aos crimes virtuais. São considerados bons avanços na legislação brasileira no que concerne ao tratamento de informações e crimes ocorridos na internet.

Com a Lei Carolina Dieckmann o Código Penal Brasileiro incorporou-se os artigos 154A e 154-B no Capítulo IV, que trata dos crimes contra a liberdade individual, mais precisamente na seção dos crimes contra a inviolabilidade dos segredos.

A nova lei, no “caput” do artigo 154-A, dispõe que é crime:

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.

Com o texto da lei ora citada, incrimina a conduta do agente que invade, não levando em consideração os mecanismos de segurança, pois seu poderio de invasão é maior que a própria blindagem, e obtém, adultera ou destrói a privacidade digital alheia, bem como a instalação de vulnerabilidades para obtenção de vantagem ilícita. Observa-se, contudo, a necessidade da existência de um mecanismo de segurança no sistema do aparelho, uma vez que a lei condiciona a ocorrência do crime com a violação indevida deste. Assim, a invasão do dispositivo informático que se der sem a violação do mecanismo de segurança pela inexistência deste será conduta atípica. Por tal razão torna-se cada vez mais importante proteger os aparelhos com

antivírus, firewall, senhas e outras defesas digitais. Todavia se consegue uma segurança maior está como o cuidado do operador em ter um total domínio ao manusear os aplicativos, em clicar ou acessar itens que seja duvidosos ou propostas muito vantajosas, que já pode ser encarada como estelionato virtual.

Para os crimes previstos no “caput” do artigo, a pena prevista na lei é de detenção, de três meses a um ano, e multa. Se este delito causar prejuízo econômico para a vítima, o parágrafo 2º prevê um aumento de pena de um sexto a um terço.

Já no parágrafo 3º traz uma pena maior, de reclusão, de seis meses a dois anos, e multa, se a invasão se dá com a finalidade de obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas. O objetivo neste caso, é resguardar a privacidade e o sigilo inerentes às atividades comerciais e industriais, protegendo, assim, as empresas, indústrias e instituições bancárias, bem como toda clientela, principalmente dos bancos, pois em cadeia seria um prejuízo bem maior.

A ação penal nos casos dos crimes do “caput” será pública condicionada à representação da vítima. Ou seja, mesmo se tratando de cometimento do ilícito, o legislador atribuiu para a vítima o oferecimento da condição de procedibilidade, observando-se a legitimidade para tanto e a fluência do prazo decadencial que finda na extinção da punibilidade. Todavia, a ação penal será pública incondicionada quando o delito for praticado 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.

O dispositivo ora apresentado veio com certa demora, pois a sociedade reclamou a tutela penal da intimidade cibernética durante muito tempo. Muitas outras intimidades foram protegidas, tais como a inviolabilidade de domicílio, o sigilo epistolar, o sigilo das correspondências e das comunicações, sigilos das comunicações telefônicas, sigilo bancário e outros. E no mundo digitalizado há a mesma necessidade de se erguer muros protetores, para que não tenhamos nosso “patrimônio digital” afetado.

2.3 Legislação Internacional em Relação aos Crimes Virtuais

É notória a necessidade de possuir uma política internacional criminal comum, pois sabemos que não tem fronteiras para os criminosos virtuais. Para que isto

aconteça é necessária uma reunião entre países para adotar leis que protejam a sociedade contra criminalidade no ciberespaço. Já houve um pequeno avanço em se tratando deste tema, pois no dia 23 de novembro de 2001 foi realizada a convenção de Budapeste sobre o *Cibercrime*¹¹. Esta convenção de Direito Penal e Direito Processual Penal foi firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução. Ele trata de violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes.

De acordo com alguns estudiosos do direito este documento foi o precursor do intercâmbio entre os países, sendo o mais importante ícone no combate ao crime cibernético na atualidade. O tratado possui 04 capítulos e 48 artigos em uma linguagem de fácil compreensão.

Vejamos um breve resumo do que aborda a Convenção de Budapeste de 2001:

1) Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos

a) Acesso ilegal: é o acesso irregular e doloso a computadores e redes.

b) Interceptação ilegal: é a captura irregular e dolosa de dado.

c) Interferência de dados: é o ataque de “cracker”, com destruição ou captura.

d) Interferência em sistemas: é a captura, bombardeio ou negação de serviços.

e) Uso abusivo de dispositivos: é a venda ilegal de dados, códigos e senhas.

2) *Infrações relacionadas com computadores;*

a) Falsidade informática: é a falsificação de dados.

b) Burla informática: é o estelionato na versão cibernética.

3) *Infrações relacionadas com o conteúdo;*

a) Pornografia infantil: produção, armazenamento, oferta, divulgação, etc.

b) Racismo e xenofobia: difusão de imagens, ideias ou teorias racistas que incentivem a violência contra o indivíduo ou grupo de semelhantes, tendo em vista motivações racistas, religiosas, étnicas, nacionalistas, utilizando-se de expressões injuriosas e ameaçadoras com o objetivo intimidatório discriminatório ou que implique em xenofobia. Apologia ao genocídio ou outros crimes contra a humanidade.

¹¹ **Cibercrime** é o nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede. Essas práticas podem envolver invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros.

De acordo com THOMAS (2010, p.20) “Vários são as recomendações contidas na Convenção de Budapeste que já foram positivadas no ordenamento jurídico pátrio, isso é um avanço”. Mesmo não havendo legislação coesa para abordar tais crimes e reprimir de forma adequada os crimes cibernéticos em sua totalidade, este tratado internacional parte da premissa de que o combate ao *cibercrime* deve ser realizado através de um Regime Internacional. De acordo com CASTELLS, (2007, p. 203):

A prática do crime é tão antiga quanto a própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral.

Os criminosos evoluíram juntamente com as tecnologias, tornando uma ameaça para a sociedade e para o Estado. E, infelizmente, a legislação não conseguiu evoluir junto com as tecnologias. Ainda de acordo com (CASTELLS 2007, p. 205), falando sobre a internacionalização ele diz:

a internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização.

Nas palavras de CASTELLS os criminosos estão cada mais se organizando, fazendo aliança, ou seja, tornando-se mais forte para que o crime a cada dia prolifere e os mesmos ficam ilesos porque usam o mundo virtual como suporte para cometer seus crimes.

Esses perigos são reais, e percebemos a necessidade dos países se reunirem. Assim como os criminosos estão se organizando para realizar os crimes é necessário que os países se aderem a um acordo Internacional mais específico, que aborde o conjunto de normas, regras e procedimentos que regulam as relações estatais internacionais no combate ao *cibercrime* (nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede).

2.3 Crimes Virtuais e sua Dificuldade de Instrução Probatória

A atividade investigativa é um desafio em relação aos crimes virtuais, especialmente pela dificuldade em relação a coleta de provas, ante ao dinamismo da tecnologia de informações. Atualmente com os avanços da tecnologia, com o surgimento da internet, presenciamos fatos que acontece do outro lado do mundo em tempo real. O mundo está conectado, com apenas um click torna-se possível comunicar com qualquer pessoa independente onde ela esteja. Diante desta facilidade os criminosos utilizam os meios virtuais para praticar os mais diversos crimes.

Esses criminosos são conhecedores na área da informática. Então eles aproveitam seu conhecimento para lesar o cidadão e enganar os investigadores. De acordo com Dorigon e Soares (2018, p. 3):

A tecnologia da informática é detentora de grande complexidade e dinamismo sem igual, o que faz com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade e a cada uma de suas repentinas mudanças.

E um dos problemas que tem sido enfrentados na hora da investigação é a falta de profissional qualificado na área de informática, e vale ressaltar que para investigar esses criminosos é necessário que os agentes públicos tenham conhecimento sobre as tecnologias e das informações necessárias para uma melhor prestação da proteção estatal aos cidadãos nos órgãos responsáveis pela persecução penal.

Outra dificuldade para investigar o crime virtual é que os criminosos armazenam os dados na *cloud computing*², conhecida como computação nas nuvens. É um modelo computacional que armazena dados sem a necessidade de um espaço em *hardware*, mas sim de forma virtual, na internet. Permitindo o acesso de qualquer lugar do mundo por meio de um dispositivo eletrônico com conexão à internet. Isto dificulta a investigação visto que os dados não precisam estar no computador do usuário. De acordo com Cavalcante, (2013, p.54) A “nuvem”:

Estes computadores acessados remotamente, podem, inclusive, estar localizados em outros países, ou seja, o usuário pode estar utilizando do serviço disponibilizado por esses servidores no Brasil, enquanto o computador responsável por prestar o acesso pode estar localizado em outro país, como por exemplo o Japão.

² **cloud computing** - computação em nuvem

Como os arquivos podem estar em qualquer país do mundo, isto torna a investigação mais difícil. Sendo que cada nação possui a sua lei, essa é uma barreira que precisa ser enfrentada. Para a polícia brasileira investigar um caso em uma nuvem de um servidor de outro país, pode ser necessário acionar a polícia internacional. Dorigon e Soares (2018) salienta que o serviço da nuvem é muito útil mas dificulta as investigações, uma vez que dificilmente será possível apreender um computador que esteja em outro país, podendo vir a impossibilitar a obtenção da prova da materialidade do delito cometido.

2.4 Provedores de Acesso à Internet e Suas Responsabilidades

Para falarmos sobre responsabilidade dos provedores precisamos antes ter um breve entendimento a respeito de tal ferramenta. A lei 12965/12 trouxe a diferenciação entre os provedores para fins de responsabilidade, obedecendo às especificações e limites técnicos existentes para cada um. A jurisprudência já vinha fazendo as devidas diferenciações quanto aos provedores de conexão e de aplicações, o que se manteve no texto da Lei.

Os provedores, denominados de provedores de conexão ou provedores de serviços, são os responsáveis pela intermediação entre a operadora e o usuário do serviço contratado. Nesta modalidade de provedor, é oferecida a conexão com a Internet conforme especificidades e velocidades contratadas e o acesso pode ser feito através de uma identificação de usuário e senha, por exemplo. Os provedores de conexão são os responsáveis por alcançar ao usuário diretamente o acesso à rede. Este acesso é feito através de uma conexão adquirida de *backbone*³.

Segundo Marcel Leonardi, também podem ser inseridos ao conceito de provedores de conexão os cafés, *lan houses*, escolas ou qualquer outro local que forneça conexão à Internet aos seus usuários. O referido autor diz: “muitas instituições de ensino e empresas permitem o acesso de seus alunos e empregados à rede através de seus equipamentos; livrarias e cafés exploram o acesso como negócio, cobrando determinada quantia (...)”.

³ **backbone** é conhecido como a “espinha dorsal” da internet e tem a função de identificar a rede por onde passa os dados de cada usuário

O conceito trazido pelo Marco Civil da Internet é o dos provedores de aplicações. Também chamados de *middleware*, estes provedores, diferentemente dos provedores de conexão, disponibilizam um instrumento para a execução de aplicações. A subseção III da Lei 12.965/2014, prevê normas pertinentes a “Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações”, estando o seu conceito e delimitação expostos no artigo 5º, inciso VIII da mesma Lei, que especifica que “registros de acesso a aplicações de internet” são o “conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”.

O Superior Tribunal de Justiça vinha decidindo, desde antes do Marco Civil da Internet, que os provedores são obrigados a viabilizar a identificação de usuários, coibindo o anonimato. Segundo a decisão, visando evitar que terceiros fossem prejudicados com atitudes ilícitas de usuários, é dever do provedor e oferecer meios de identificação dos usuários, através do fornecimento do número do IP.

Em uma visão abrangente, o Marco Civil da Internet aponta um avanço na questão da responsabilidade dos provedores pois não atribui aos provedores de conexão uma responsabilidade por conteúdos aos quais não tem qualquer ingerência mas estabelece a responsabilidade dos provedores de aplicações nos casos em que restar comprovado que não agiu de forma diligente para retirada de conteúdos ilícitos.

3 REFORMA DO CODIGO PENAL PARA ADEQUAÇÃO A TECNOLOGIA

Com vários avanços tecnológicos, que cada dia se renova na sociedade, os crimes digitais vem se tornando algo comum entre a população, e-mails falsos, crimes contra a honra e outros são diariamente enfrentado por nossos juristas e o código não está preparado para punir ou lidar com tantas condutas que são novas em nosso ordenamento, por fim acabam decidindo por analogia, pois não se pode ficar sem decisão e como diz SOUZA, (2011, p. 185):

No Direito Penal a invocação mais imediata para a colmatação das lacunas é a analogia, consistente em aplicar uma hipótese não prevista na lei a caso semelhante. Não cria direito novo, mas descobre o existente, como forma de auto-integração da lei.

O delito mais comum hoje seria o de desviar valores usando a internet banking. Esta prática como se fosse o estelionatário, fazem analogia ao Código Penal Brasileiro com o artigo 171 que diz: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Isto é perfeitamente aplicável. Podem-se citar ainda várias outras práticas criminosas que são aplicáveis pela legislação do Código Penal: Ameaça na Internet pode ser analisada pelo Artigo 147 “Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave”. Difamar alguém, por exemplo, em uma rede de relacionamentos: Art. 139 “Difamar alguém, imputando-lhe fato ofensivo à sua reputação”, e assim por diante.

Antes da promulgação da Lei nº 12.737 de 30 de novembro de 2012, não havia uma legislação penal especial e autônoma para regulamentar os crimes cometidos na rede. O que ocorria, então, era uma adaptação da atual parte especial do Código Penal. Mas é importante salientar, conforme lembra Fabrizio Rosa, que:

Não se deve confundir um crime comum praticado pelo uso ou contra o computador de um ‘crime de informática’ propriamente dito. Daí a necessidade de uma legislação específica para esses delitos “ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si que, então, se torna objeto de aprofundada reflexão jurídica e técnica. (ROSA, 2002, p.30).

É de suma importância observar que a atividade legislativa deve ocorrer de forma precisa e conjunta, com estudos cuidadosos e com auxílio dos especialistas das áreas jurídica e informática, para evitar incoerência e dificuldades na aplicação da lei, evitando discussões nos tribunais, impunidades ou injustiças, além da análise da real necessidade da intervenção do Direito Penal. Saber estabelecer estratégias jurídicas eficientes no mundo cada vez mais digital e virtual é condição de sobrevivência do profissional do direito, uma vez que cada vez mais o tempo e a tecnologia atuam de modo a exigir celeridade e flexibilidade nas soluções jurídicas. A questão que se coloca é de eficácia. Portanto, é necessário antever os acontecimentos e criar soluções flexíveis, que sobrevivam ao tempo.

3.1 Competência para Processar e Julgar

Existem diversas formas de definir a competência de cada juízo, seja pela matéria, seja pelo território, ou até pela função. No direito penal brasileiro, adotou-se a teoria da Ubiquidade, onde se considera o lugar da infração aquele onde se consumou o crime, ou onde foi praticado a última ação ou omissão. Segundo Aury Lopes Jr 2011 p.423 “A competência é um conjunto de regras que asseguram a eficácia da garantia da jurisdição e, especialmente, do juiz natural. Delimitando a jurisdição, condiciona seu exercício.”

Em primeiro lugar, é importante abordar acerca do conceito de jurisdição, sendo o poder-dever do Estado-juiz de dizer o direito, é o poder que o Estado concedeu ao juiz de aplicar o direito ao caso concreto, é o poder que o magistrado tem de aplicação da lei a cada caso concreto. Segundo TAVORA (2013, p. 239) “É o poder-dever pertinente ao Estado-juiz de aplicar o direito ao caso concreto”.

No direito penal e em regra para vários crimes digitais usa-se o artigo 70 do código penal, que diz: “A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.” Sobre matéria e competência disse o Ministério Público Federal:

Nos limites dos reclamos deste Roteiro, tratar-se-á sobre a competência em razão da matéria e a competência em razão do local, a fim de se esclarecer em que casos os crimes de pornografia infanto-juvenil e crimes de racismo praticados por meio da *Internet* serão de

competência da justiça federal ou da justiça estadual, bem como em qual local deverá ser instaurado o processo, além de uma breve menção a outros tipos de crimes, como é o caso do furto mediante fraude por meio de *Internet*.

Este entendimento é em nível nacional, porem a Convenção de Budapeste Sobre Cibercrime 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.

3.2 Julgados envolvendo a prática de crimes virtuais.

Como narrado no subtítulo anterior o caso a ser exposto a seguir demonstra a dificuldade em se tratando de competência, pois as divergências sempre estão em foco pois como a internet está em todo lugar há sempre o que discutir como no caso concreto do julgamento do processo 00032703820168190011, julgado pelo Primeira Turma Recursal dos Juizados Especiais Criminais do Rio de Janeiro:

Apelação. Juizado Especial Criminal. Ação Penal Privada. Crime contra a honra. Difamação. Art. 139 do Código Penal. Em sendo o crime de menor potencial ofensivo, tem-se a regra do art. 63 da Lei nº 9.099/96 que dispõe que: "A competência do Juizado será determinada pelo lugar em que foi praticada a infração penal". Em sendo o crime praticado pela internet, impossível a aferição quanto ao exato local da infração, incidindo sobre a hipótese a regra do art. 72 do Código Processo Penal que estabelece que não sendo conhecido o lugar da infração, a competência regular-se-á pelo local do domicílio ou residência do Réu. Não provimento do Recurso. VOTO 1. Modalidade recente de crime, carece a norma que regula os crimes virtuais¹ - como identificamos em Legislações Especiais - de dispositivo legal definidor da competência territorial. Desafia a matéria extenso debate para se estabelecer os melhores critérios técnicos para a aferição da autoria da postagem. Silente a norma, precisamos nos recorrer às regras existentes na legislação vigente, não, sem antes observar que não se trata de matéria pacífica. Não se está a ignorar os termos do art. 63 da Lei nº 9.099/95 que estabelece que a competência será determinada pelo lugar da infração penal, mas, se está a questionar qual seria o exato lugar do aperfeiçoamento da conduta. Neste ponto é que nascem as divergências: Local da hospedagem do site. Posição sustentada no C.C. nº 97.201-RJ 2em que se entendeu que a competência seria do local onde está hospedado o provedor da página da internet, pois este seria o responsável pela divulgação da informação. "[...] 1. Não recepcionada a Lei n. 5.250/1967 pela nova ordem constitucional (ADPF n. 130/DF), às causas decorrentes das relações de imprensa devem ser aplicadas as normas da legislação comum, inclusive,

quanto à competência, o disposto no art. 70 do Código de Processo Penal. 2. O crime de calúnia (art. 138, caput, do Código Penal) consuma-se no momento em que os fatos "veiculados chegam ao conhecimento de terceiros" (CC n. 107.088/DF, Relatora Ministra Maria Thereza de Assis Moura, DJe de 4/6/2010). 3. Tratando-se de queixa-crime que imputa a prática do crime de calúnia em razão da divulgação de carta em blog, na 111 CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012 internet, o foro para processamento e julgamento da ação é o do lugar de onde partiu a publicação do texto tido por calunioso. 4. In casu, como o blog em questão está hospedado em servidor de internet sediado na cidade de São Paulo, é do Juízo da 13ª Vara Criminal dessa comarca a competência para atuar no feito. 5. Conflito conhecido para declarar competente o suscitado." Justifica o Ministro Arnaldo Esteves Lima como sendo o local mais adequado para a realização da coleta e obtenção das provas como mais inteireza. Posicionamento, contudo, que contraria a Legislação Processual que adota a teoria do resultado como regra. Local de residência do ofendido. Posição vencida do Ministro Napoleão Nunes Maia Filho, no julgamento CC nº 97.201- RJ. Deveras cômodo a vítima que se estabeleça no local por ela definido como nas causas cíveis..3 Local da residência do Autor do Fato. Posição dominante? Em sendo o crime cometido através da internet por ser acessível pelos mais variados meios e por conseguinte, em variados locais (notebook, tablets, celulares, lan house) a aferição quanto ao exato local da infração, torna-se impossível. Incidiria, neste entendimento, a regra do art. 72 do Código de Processo Penal que estabelece que: "Não sendo conhecido o lugar da infração, a competência regular-se-á pelo local do domicílio ou residência do Réu". Positivo desta posição a possibilidade de uma rápida busca e apreensão dos equipamentos utilizados pelo autor e a verificação se da citada máquina estariam sendo enviadas as mensagens ao servidor. Local do Resultado do Delito⁴ incidindo a regra do art. 70 do Código de Processo Penal, sendo este onde a vítima vem a sofrer os resultados da publicação.⁵ Superior Tribunal de Justiça 2. Crimes contra a honra praticados por meio de publicação em periódicos, para o Superior Tribunal de Justiça, são da competência do juízo do local onde ocorreu a impressão, em consonância com o que estabelece o art. 70 do Código de Processo Penal que estabelece que: "A competência será, de regra, determinada pelo lugar em que se consumir a infração". Entretanto, nos crimes praticados por veiculação na internet, o conteúdo e a sua recepção pode se dar em qualquer lugar, voltando-se o Superior Tribunal de Justiça pela determinação da competência no local onde se encontra o responsável pela divulgação. Orientação no Informativo de Jurisprudência nº: 0434. COMPETÊNCIA. INTERNET. CRIMES CONTRA HONRA. A Seção entendeu, lastreada em orientação do STF, que a Lei de Imprensa (Lei n. 5.250/1967) não foi recepcionada pela CF/1988. Assim, nos crimes contra a honra, aplicam-se, em princípio, as normas da legislação comum, quais sejam, o art. 138 e seguintes do CP e o art. 69 e seguintes do CPP. Logo, nos crimes contra a honra praticados por meio de publicação impressa em periódico de circulação nacional, deve-se fixar a competência do juízo pelo local onde ocorreu a impressão, uma vez que se trata do primeiro lugar onde as matérias produzidas chegaram ao

conhecimento de outrem, de acordo com o art. 70 do CPP. Quanto aos crimes contra a honra praticados por meio de reportagens veiculadas na Internet, a competência fixa-se em razão do local onde foi concluída a ação delituosa, ou seja, onde se encontra o responsável pela veiculação e divulgação das notícias, indiferente a localização do provedor de acesso à rede mundial de computadores ou sua efetiva visualização pelos usuários. Precedentes citados do STF: ADPF 130-DF, DJe 6/11/2009; do STJ: CC 29.886-SP, DJ 1º/2/2008. CC 106.625-DF, Rel. Min. Arnaldo Esteves Lima, julgado em 12/5/2010. CONFLITO DE COMPETÊNCIA. CRIMES CONTRA HONRA PRATICADOS PELA INTERNET. COMPETÊNCIA. VEICULAÇÃO DO CONTEÚDO OFENSIVO. FIXAÇÃO NO LOCAL DO TITULAR DO PRÓPRIO DOMÍNIO E QUE CRIOU A HOME PAGE ONDE É ABASTECIDO SEU CONTEÚDO. 1. Tratando-se de crimes contra a honra praticados pela internet, a competência deve ser fixada de acordo com a regra do art. 70 do Código de Processo Penal, segundo o qual "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Isso porque constituem-se crimes formais e, portanto, consumam-se no momento de sua prática, independentemente da ocorrência de resultado naturalístico. Assim, a simples divulgação do conteúdo supostamente ofensivo na internet já é suficiente para delimitação da competência. 2. Esse local deve ser aquele de onde efetivamente partiu a publicação do conteúdo, o que ocorre no próprio local do domínio em que se encontra a home page, porquanto é ali que o titular do domínio alimenta o seu conteúdo, independentemente do local onde se hospeda o sítio eletrônico (provedor). 3. No caso, a veiculação da reportagem que deu ensejo ao inquérito policial partiu de sítio eletrônico cujo domínio era de empresa situada no Mato Grosso, razão pela qual a competência é do Juízo Federal da 5ª Vara do Mato Grosso. (CC 136.700/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, TERCEIRA SEÇÃO, julgado em 23/09/2015, DJe 01/10/2015) REFLEXÕES 3. A verdade é que o Código de Processo Penal nunca fixou o domicílio da suposta vítima como critério de fixação da competência. Conhecido ou não o lugar da infração, a competência em ambas as hipóteses descarta o domicílio da vítima. Nem mesmo nas hipóteses de serem as ações de exclusiva iniciativa da vítima. Nestas, previu o Legislador, inclusive, que o Querelante optasse pelo local da ação, mas, apenas, lhe concedeu a faculdade de propor no domicílio do Réu - art. 73 do C.P.P6 - e não em seu próprio. Em outras palavras, estivessemos no Código de Processo Penal ou na Lei nº 9.099/95, não seria a residência da vítima o fator determinante na fixação da competência territorial, como pretende o Recorrente. E por quê? Porque o fim da ação penal não é a satisfação pessoal da vítima, esta suscetível, sim, de ser obtida na via cível. Nestas ações, o particular é legitimado, extraordinariamente, a postular em juízo, mas, o titular do direito de punir continua sendo o Estado e, pela ótica do Estado é que se tem que aferir o interesse de ser a ação proposta no domicílio da vítima ou não. Precisamos nos nortear, assim, pelo interesse público e não pelo privado, evidentemente, prejudicado pela onerosa ocorrência de eventual deslocamento para outra comarca para a propositura da ação e presença às audiências. Induvidoso que o ideal é que a ação se dê no local de onde efetivamente teriam partido as publicações e o conteúdo7, ou seja,

no local de domicílio do Réu, não apenas em razão da facilidade de arrecadação da prova, do reconhecimento do concurso formal, e, porque não dizer para eventual reunião de processos quando da execução da pena. Posição igualmente adotada quando eram praticados pela via dos impressos. Entendimento que orientou a RE 628624, em que reconheceu o STF a Repercussão Geral da matéria que trata da competência para o processamento e julgamento dos crimes de divulgação de imagens de crianças e adolescentes. In verbis a decisão: CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. APURAÇÃO DO DELITO DO ART. 241-A DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. SUPOSTA VEICULAÇÃO DE IMAGENS DE PORNOGRAFIA INFANTIL PELA INTERNET. COMPETÊNCIA FIRMADA PELO LUGAR DA INFRAÇÃO. ART. 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DE TERCEIRO JUÍZO, ESTRANHO AO CONFLITO. 1. A consumação do delito, que atualmente tem previsão no art. 241-A do Estatuto da Criança e do Adolescente, "ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários" (CC 29.886/SP, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, julgado em 12/12/2007, DJ 01/02/2008, p. 427). 2. A conduta delituosa a ser apurada, na hipótese, refere-se à veiculação de imagens de menores aliciadas para exposição em cenas obscenas, via webcam, por meio do MSN/ORKUT e TWITTER, além de hackeamento e utilização do perfil de uma delas, fazendo-se o agente passar por esta, para comunicar-se com terceiros. 3. Ausentes indícios de transnacionalidade do crime, a tanto não servindo o mero meio internet, competente é o juízo estadual do local de indicada residência do suspeito, em Londrina/PR, na forma do art. 70 do Código de Processo Penal. 4. Conflito conhecido para declarar competente o Juízo de Direito da Vara Criminal da Comarca de Londrina - TJ/PR, juízo estranho ao conflito. (STJ - CC: 136257 PR 2014/0251911-6, Relator: Ministro NEFI CORDEIRO, Data de Julgamento: 11/03/2015, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 20/03/2015) Ressalto, apenas, não ser o crime do decisum transcrito um crime contra a honra que desafia regra própria de interpretação, mas, incidir a mesma preocupação do Legislador na eleição da competência. DA LEI 9.099/95 4. Impossível a aferição do exato local em que o blog do Autor do Fato foi lido ou mesmo produzido - e em sendo o crime de difamação, crime que se consuma com o conhecimento do fato por terceiros e, não propriamente, pela vítima, como ocorre com a Injúria - incide a regra subsidiária do art. 72 do Código de Processo Penal - como previsto no art. 92 da Lei nº 9.099/95 - para entender que a competência é fixada no domicílio do Autor do Fato e não da vítima. CONCLUSÃO 5. Voto no sentido de conhecer do recurso, e, no mérito, negar-lhe provimento. Rio de Janeiro, 01 de setembro de 2.017. Cláudia Márcia Gonçalves Vidal Juíza de Direito 1 Lei nº 12.737/12 (Lei Carolina Dieckman que altera os arts 154, 266 e 298 do Código Penal e a Lei nº 12.965/14. 2 Divergências de voto também no CC nº 106.625 - DF 3 Trata-se de agravo cujo objeto é decisão que inadmitiu recurso extraordinário interposto contra acórdão da Turma Recursal Criminal do Tribunal de Justiça do Estado do Rio Grande do Sul, assim ementado: AÇÃO

PENAL PRIVADA. CRIME CONTRA A HONRA. DIFAMAÇÃO. ARTIGO 139 DO CÓDIGO PENAL. RECURSO EM SENTIDO ESTRITO CONHECIDO COMO APELAÇÃO PELO PRINCÍPIO DA FUNGIBILIDADE. REJEIÇÃO DA QUEIXA-CRIME. DECISÃO REFORMADA. 1. No âmbito do JECrim, é cabível apelação da decisão que rejeita a queixa (art. 82, caput, da Lei 9.099/95). 2. A competência no Direito Processual Penal tem como regra o lugar da infração (art. 70 do Código de Processo Penal). Em se tratando de crimes de menor potencial ofensivo, tem-se a regra do art. 63 da Lei nº 9.099/95, que dispõe: "A competência do Juizado será determinada pelo lugar em que foi praticada a infração penal." Tratando-se de crime cometido através da INTERNET, por ser acessível pelos mais variados meios (notebooks, tablets, celulares, lan houses), impossível a aferição quanto ao local da infração. Portanto, aplicável ao caso a regra do art. 72 do Código de Processo Penal: "Não sendo conhecido o lugar da infração, a competência regular-se-á pelo local do domicílio ou residência do réu". No caso específico dos autos, ambos (local da infração e domicílio do réu) remetem a competência ao juízo da comarca de Tapes. 3. Não se aplica, na espécie, o critério residual da prevenção, pois o caso em tela não se enquadra em nenhum dos casos elencados no art. 83, do CPP (arts. 70, § 3º, 71, 72, § 2º, e 78, II, c). RECURSO EM SENTIDO ESTRITO CONHECIDO COMO APELAÇÃO E PROVIDO. O recurso extraordinário busca fundamento no art. 102, III, a, da Constituição Federal. A parte recorrente alega violação ao art. 5º, XXVII e LIII, da Constituição. A decisão agravada não admitiu o recurso extraordinário sob os seguintes fundamentos: (i) incidem, no caso, as Súmulas 282 e 356/STF; (ii) eventual ofensa à Constituição seria reflexa. O recurso é inadmissível, tendo em vista que, para chegar a conclusão diversa do acórdão recorrido, imprescindíveis seriam a análise da legislação infraconstitucional pertinente e uma nova apreciação dos fatos e do material probatório constante dos autos, o que torna inviável o processamento do recurso extraordinário, nos termos da Súmula 279/STF. Nessa linha, vejam-se o RE 650.842, Rel. Min. Joaquim Barbosa; o RE 650.844, Rel.ª Min.ª Carmen Lúcia; e o AI 838.104 AgR, Rel.ª Min.ª Ellen Gracie. Diante do exposto, com base no art. 38 da Lei nº 8.038/1990 e no art. 21, § 1º, do RI/STF, nego seguimento ao recurso. Publique-se. Brasília, 19 de fevereiro de 2015. Ministro Luís Roberto Barroso Relator. STF - RECURSO EXTRAORDINÁRIO COM AGRAVO : ARE 864724 RS - RIO GRANDE DO SUL 4RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET. ANÁLISE SOBRE A COMPETÊNCIA PARA APRECIAR A MATÉRIA. APLICAÇÃO DA REGRA DO ART. 70 DO CÓDIGO DE PROCESSO PENAL TEORIA DO RESULTADO. LOCAL ONDE A VÍTIMA E TERCEIROS TOMARAM CONHECIMENTO DOS FATOS, EM TESE, OFENSIVOS, AINDA QUE AS PUBLICAÇÕES NO FACEBOOK TENHAM OCORRIDO EM LOCAL DIVERSO. RECURSO PARCIALMENTE CONHECIDO, E, NESSA PARTE, PROVIDO. Aplica-se a regra do art. 70 do Código de Processo Penal (lugar da consumação) nos crimes contra a honra, cometidos pela Internet (na rede social Facebook), tendo em vista que o conteúdo, em tese, ofensivo, pode ser publicado de qualquer lugar, contudo causam ofensas à honra da vítima na comunidade em que ela vive. I. (TJPR - 2ª C.Criminal - RSE - 1397104-5 - Maringá - Rel.: José

Mauricio Pinto de Almeida - Unânime - - J. 08.10.2015) TJ-PR - Recurso em Sentido Estrito RSE 13971045 PR 1397104-5 5 Adotado na decisão CC nº 29.886 - SP 6 Art. 73. Nos casos de exclusiva ação privada, o querelante poderá preferir o foro de domicílio ou da residência do réu, ainda quando conhecido o lugar da infração. 7PROCESSUAL PENAL. CONFLITO NEGATIVO DE COMPETÊNCIA. NOTÍCIA-CRIME PELA SUPOSTA PRÁTICA DOS DELITOS PREVISTOS NOS ARTS. 20 E 21 DA LEI 5.250/97 (LEI DE IMPRENSA). LEI NÃO RECEPCIONADA PELA CONSTITUIÇÃO FEDERAL. ADPF 130/DF. APLICAÇÃO DOS ARTS. 138 E 139 DO CP E ART. 70 DO CPP. DUAS SEQUÊNCIAS DE FATOS DISTINTOS. PUBLICAÇÃO DE REPORTAGENS VEICULADAS NA REVISTA ISTOÉ. COMPETÊNCIA DO JUÍZO DO LOCAL DA IMPRESSÃO DA REVISTA. MATÉRIAS DISPONIBILIZADAS NO BLOG "CONVERSA AFIADA". COMPETÊNCIA DO LOCAL EM QUE PRATICADOS OS ATOS DE PUBLICAÇÃO. CONFLITO CONHECIDO. COMPETÊNCIA DA JUSTIÇA FEDERAL PAULISTA. 1. Não recepcionada a Lei de Imprensa pela nova ordem Constitucional (ADPF 130/DF), quanto aos crimes contra a honra, aplicam-se, em princípio, as normas da legislação comum, quais sejam, art. 138 e seguintes do Código Penal e art. 69 e seguintes do Código de Processo Penal. 2. Na hipótese de crime contra a honra praticado por meio de publicação impressa de periódico, deve-se fixar a competência do Juízo onde ocorreu a impressão, tendo em vista ser o primeiro local onde as matérias produzidas chegaram ao conhecimento de outrem, nos moldes do art. 70 do Código de Processo Penal. Remanesce, na prática, o resultado processual obtido pela antiga aplicação da regra de competência prevista na não recepcionada Lei de Imprensa. 3. Crimes contra a honra praticados por meio de reportagens veiculadas pela internet ensejam a competência do Juízo do local onde foi concluída a ação delituosa, ou seja, onde se encontrava o responsável pela veiculação e divulgação de tais notícias. 4. Conheço do conflito para declarar competente o Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado de São Paulo. STJ - CONFLITO DE COMPETÊNCIA : CC 106625 DF 2009/0136422-1 8 Art. 72. Não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu. ----- 1 8 Recurso nº 0003270-38.2016.8.19.0011 - Voto Relator I Turma Recursal Criminal (TJ-RJ - APR: 00032703820168190011 RIO DE JANEIRO CABO FRIO J VIO E ESP ADJ CRIM, Relator: CLAUDIA MARCIA GONCALVES VIDAL, Data de Julgamento: 05/10/2017, CAPITAL 1a. TURMA RECURSAL DOS JUI ESP CRIMINAIS, Data de Publicação: 24/10/2017)

Enfim, não teremos uma regra definida para abarcar todos os casos de crimes virtuais, pois em cada um há divergência da maneira em que age o agente ou em que ocorre os fatos. Em suma será analisado a cada caso concreto a sua competência.

Estes crimes em regra dificultam a ação dos policiais em localizar o agente, pois mesmo estando preso ele consegue cometer delitos dentro da prisão e as normas

se confundem pois quando da criação das leis não haviam casos específicos como o que se segue:

PENAL. PROCESSUAL PENAL. HABEAS CORPUS. FURTO QUALIFICADO ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES. APELAÇÃO EM LIBERDADE. IMPOSSIBILIDADE. PACIENTE PRESO EM OUTRA AÇÃO PENAL E ENVOLVIDO MAIS DE UMA VEZ EM CRIMES VIRTUAIS. MUDANÇA DE ENDEREÇO NÃO INFORMADA AO JUÍZO COMPETENTE. PEDIDO DE TRANSFERÊNCIA PARA PRESÍDIO PRÓXIMO À RESIDÊNCIA DA FAMÍLIA. JUÍZO DE EXECUÇÕES PENAS. ORDEM DENEGADA. 1. Cuida-se de HABEAS CORPUS, com pedido liminar, impetrado em favor de RAUL BEZERRA DE ARRUDA JÚNIOR, apontando como autoridade coatora o Juiz Federal da 6ª Vara Federal da Seção Judiciária da Paraíba por ter indeferido o pedido de liberdade provisória, nos autos do processo n.º 0001537-02.2014.4.05.8201, face à sentença penal condenatória proferida nos autos da Ação Penal n.º 2006.82.01.001114-6, instaurada para apurar a prática dos delitos tipificados nos artigos 1º, VII, c/c parágrafo 2º, inc. I, da Lei n.º 9.613/98, e nos arts. 288 e 155, parágrafo 4º, inc. II e IV, do Código Penal. 2. Depreende-se dos autos que o paciente, juntamente com outros cinco acusados, em liame subjetivo permanente, formaram uma quadrilha visando ao furto sistemático de contas bancárias, mediante a utilização de programas preparados para invadir e subtrair contas bancárias pela internet, o que configuraria, em tese, os tipos penais previstos nos artigos 155, parágrafo 4º, inciso II e IV, e 288, ambos do Código Penal, no artigo 10 da Lei n. 9.296/96, no artigo 10 da Lei Complementar n. 105/2001 e no artigo 1º, inciso VII, c/c parágrafo 2º, inciso I, da Lei n. 9.613/98. 3. O impetrante sustenta, em síntese, que a decisão de indeferimento do pedido de liberdade provisória carece de fundamentos concretos e sem qualquer alicerce para a manutenção da segregação cautelar do paciente. Pugna, pois, pela concessão da ordem assegurando-lhe o direito de responder a todos os atos do processo em liberdade até o seu trânsito em julgado, ou, na remota impossibilidade, a imediata transferência do paciente para um presídio próximo à localidade da residência de sua família situada em Parnamirim/RN. 4. Afastada a alegação de nulidade do ato judicial de negativa do direito de apelar em liberdade, porquanto satisfatoriamente fundamentado pelo juízo a quo na parte dispositiva da sentença condenatória. Excerto da sentença transcrito. 5. Conforme se infere da parte dispositiva da sentença condenatória, o paciente não se inibiu de continuar a prática delitiva tendo sido preso novamente em cumprimento à determinação do Juízo da Comarca de Pombal-PB nos autos do Processo n.º 1921-53.2012.815.0301, além de ter-se envolvido mais de uma vez em crimes virtuais. Consta, ainda, o registro de que o paciente não foi localizado pela Polícia Federal nos endereços indicados em Campina Grande/PB. 6. A não comunicação de mudança de endereço ao juízo competente, bem como a reiteração das condutas delituosas, revela a inadequação e insuficiência das medidas cautelares alternativas à prisão previstas no art. 319 do CPP. 7. Considerando que inexistem elementos nos autos suficientes à análise do pedido de transferência do paciente para um

presídio próximo à localidade da residência de sua família (Parnamirim/RN), cabe ao Juízo de Execuções Penais do Rio Grande do Norte apreciar tal pretensão. Ordem de habeas corpus denegada em consonância com o parecer ministerial.

Portanto, há sim a necessidade de uma renovação e reenquadramento dos dispositivos penas para facilitação dos tribunais.

CONSIDERAÇÕES FINAIS

A evolução da internet e, as transformações de paradigmas sociais, em conjunto com o aumento desenfreado da informatização, envolvendo incidentes cibernéticos é matéria que nunca perde sua importância, de modo que se tornou necessária a elaboração de uma lei que dispunha acerca da tipificação criminal de delitos informáticos.

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

Assim, 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 muito importante a criação de uma legislação específica ou a adequação da existente a fim de resguardar o bem jurídico protegido e inibir a prática dos crimes virtuais.

Por fim, nota-se que algumas mudanças vieram para ficar, e muitas outras estão por vir, e, cada vez mais, uma visão global com uma atuação de estrategista será exigida dos profissionais do Direito, de modo a trazerem soluções para o âmbito de uma sociedade globalizada, convergente, digital e em constante mudança.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Jéssica de Jesus; MENDONÇA, Allana Barbosa e CARMO, Gilmar Passos do. Et al. **CRIMES CIBERNÉTICOS**. Ciências Humanas e Sociais Unit | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br. disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acessado dia 10 de jan. de 2018.

BRASIL. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988**, Brasília. Disponível em: <
http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 12 fev. 2018.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm Acessado em: 14 març. 2018.

BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acessado em 10 jan 2018.

BRASIL. **Lei 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponivem em: <
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acessado em 05 mai. 2018

BRASIL. **Superior Tribunal de Justiça**. Agravo Regimental no Agravo em Recurso Especial n.º 259482/MG, Relator Ministro Sidinei Beneti, Terceira Turma, julgado em 16.04.2013

Brasil. **Ministério Público Federal**. Câmara de Coordenação e Revisão, 2. Roteiro de atuação: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013.
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.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529. Acessado dia 25 de nov. de 2017.

CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Lumen Juris: Rio de Janeiro, 2003, p. 1.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <
http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf
>. Acesso em: 19 maio 2018.

JESUS, Damásio. **Direito Penal. Parte especial: dos crimes contra a pessoa e dos crimes contra o patrimônio**. 28 ed. rev. e atual. São Paulo: Saraiva 2007.

DORIGON, Alessandro e SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade**. Disponível em: <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/1>. Acessado dia 09 de abril de 2018.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: Ed. Revista dos Tribunais, 1980, p.27

LAFER, Celso apud AGUIAR JR., *Op. Cit.*, p. 108, 2001.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:
http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm. Acessado em 17 de março de 2018.

LIMA, María de la Luz apud FURLANETO NETO, Mário; GUIMARÃES, José A. Chaves, op. cit., mar. 2003. p. 70.

LOPES JR., Aury. **Direito Processual Penal** e sua conformidade constitucional. 8ª Edição. Vol. 1. Rio de Janeiro: Lumen Juris, 2011.

LUNARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. 1 ed. São Paulo: Juarez de Oliveira, 2005. pgs. 22-23.

RAMALHO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Jus Navigandi, Teresina, ago. 2013. Disponível em: . Acesso em: 10 de jan de 2018.

ROCHA, Manuel Lopes. **Crimes da informática – Remy Gama Filho** Editora: CopyMarket.com, 2000)

ROSA, Fabrício. **Crimes de Informática**. 2. ed. Campinas: Bookseller, 2006

SOUZA, Carlos Afonso Pereira de; CALIXTO, Marcelo; SAMPAIO, Patrícia Regina Pinheiro. **Os Direitos da Personalidade**. Breve Análise de sua Origem Histórica. Disponível em: http://www.puc-rio.br/direito/pet_jur/cafpatdp.html. Acessado dia 25 de nov. de 2017.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**: de acordo com a Lei nº 12.760/2012 que aumentou o rigor da “Lei Seca”. 8º Edição. Bahia: JusPodvm, 2013.

TJ-RJ - APR: 00032703820168190011 RIO DE JANEIRO CABO FRIO J VIO E ESP ADJ CRIM, Relator: CLAUDIA MARCIA GONCALVES VIDAL, Data de Julgamento: 05/10/2017, CAPITAL 1a. TURMA RECURSAL DOS JUI ESP CRIMINAIS, Data de Publicação: 24/10/2017, disponível em: <https://tj-rj.jusbrasil.com.br/jurisprudencia/514514776/apelacao-criminal-apr-32703820168190011-rio-de-janeiro-cabo-frio-j-vio-e-esp-adj-crim?ref=juris-tabs>. Acesado em : 10/05/2018.

TRF-5 - HC: 00093902720144050000 AL, Relator: Desembargador Federal José Maria Lucena, Data de Julgamento: 15/01/2015, Primeira Turma, Data de Publicação: 22/01/2015. Disponível em: <<https://trf-5.jusbrasil.com.br/jurisprudencia/178269147/habeas-corpus-hc-93902720144050000-al>> Acesado em 20 mai. 2018.