UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS – UNIPAC
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS DE BARBACENA- FADI
CURSO DE GRADUAÇÃO EM DIREITO

CAROLINA GARCIA COSTA

CRIMES NA INTERNET E A INEFICÁCIA DA LEI

BARBACENA
2014

CAROLINA GARCIA COSTA

CRIMES NA INTERNET E A INEFICÁCIA DA LEI

Monografia apresentada ao curso de Direito da Faculdade de Ciências Jurídicas e Sociais de Barbacena, da Universidade Presidente Antônio Carlos - UNIPAC, como requisito parcial, para obtenção do título de bacharel em Direito.

Orientador: Prof.ª Me. Delma Gomes Messias

BARBACENA
2014

Carolina Garcia Costa

CRIMES NA INTERNET E A INEFICÁCIA DA LEI

Monografia apresentada ao curso de Direito da Faculdade de Ciências Jurídicas e Sociais de Barbacena, da Universidade Presidente Antônio Carlos - UNIPAC, como requisito parcial, para obtenção do título de bacharel em Direito.

Aprovada em: 02/12/14

Banca Examinadora

Prof.ª Me. Delma Gomes Messias
Universidade Presidente Antônio Carlos- UNIPAC

Prof.ª Esp. Odete de Araújo Coelho
Universidade Presidente Antônio Carlos- UNIPAC

Prof. Esp. Nelton José Araújo Ferreira
Universidade Presidente Antônio Carlos- UNIPAC

Dedico este trabalho ao meu pai Silvio e à minha mãe Rosana que foram fundamentais para a conclusão de mais essa etapa de minha vida.

Agradecimentos

À Professora Delma Gomes Messias

“Há homens que lutam um dia e são bons. Há outros que lutam um ano e são melhores. Há aqueles que lutam muitos anos e são muito bons. Mas há os que lutam por toda a vida. Estes são os imprescindíveis”.

Bertol Brecht

Resumo

A internet é um meio de comunicação de extrema importância para as relações humanas na sociedade atual, todavia não se pode ignorar o fato de que com os benefícios, também vieram os problemas, bem como os crimes virtuais cometidos em um espaço frágil e inseguro, que passou a fomentar discussões em relação à necessidade de uma tipificação específica prevista no código penal para tais crimes.
O presente estudo tem por objetivo analisar os principais aspectos da importância da internet na sociedade atual, os prós e os contras do seu uso, bem como o aumento dos crimes praticados através deste meio e a ineficácia da lei no tocante à penalização.

Palavras-Chave: Internet. Crimes virtuais. Cibercrimes Lei 12.737/12. Lei Carolina Dieckmann.

Abstract

The internet is a medium of extreme importance to human relations in modern society, however one can not ignore the fact that the benefits also came the problems, as well as virtual crimes committed in a fragile and insecure space, which began to encourage discussions regarding the need for a specific classification under the criminal code for such crimes.
The present study aims to analyze the main aspects of the role of the Internet in today's society, the pros and cons of its use, as well as the increase of crimes through this medium and the ineffectiveness of the law regarding the penalty.

Keywords: Internet. Cybercrime. Law 12.737/12. Law Carolina Dieckmann.

Sumário

1 Introdução

A tecnologia da informação nas últimas décadas proporcionou um avanço no comportamento das pessoas, mudando a forma como as mesmas se comunicam, criando possibilidades virtuais, onde em qualquer local do planeta pode-se encontrar algum computador conectado à *Internet*, levando as informações instantaneamente a qualquer parte, para todo tipo de público.

As câmeras propiciam a comunicação integrando áudio e vídeo em tempo real, interligando pessoas de diversas partes do mundo. A troca de *e-mails* tornou-se comum, tanto para a prática profissional quanto para atividades pessoais.

De igual importância é o uso da internet nas atividades ligadas ao comércio, onde facilmente pode-se comprar toda sorte de produtos e serviços, através da utilização da rede mundial de computadores, sendo denominado tal comércio de comércio eletrônico.

A internet é um meio de comunicação de extrema importância para as relações humanas na sociedade atual, todavia não se pode ignorar o fato de que com os benefícios, também vieram os problemas, bem como os crimes virtuais cometidos em um espaço frágil e inseguro, que passou a fomentar discussões em relação à necessidade de uma tipificação específica prevista no código penal para tais crimes.

O presente estudo tem por objetivo analisar os principais aspectos da importância da internet na sociedade atual, os prós e os contras do seu uso, bem como o aumento dos crimes praticados através deste meio e a ineficácia da lei no tocante à penalização. A pesquisa se inicia com comentários acerca das vantagens, desvantagens e consequências do uso da internet, seguida da definição e análise acerca dos principais crimes praticados por meio desta. Após, será apreciado em um breve relato o estudo acerca da Lei n 12.737/2012 (Lei Carolina Dieckmann) assim como a análise da recente Lei 12.965, de 23 de Abril de 2014(Marco Civil) que regulamenta o uso da internet no Brasil, bem como as críticas em relação a esse dispositivo legal. Por fim será delineada a necessidade de adaptação jurídico social de acordo com a nova “Era Digital”.

2 Internet e crimes virtuais

Segundo Furlaneto Neto *et al.* (2012) a rede mundial de computadores apresenta várias características, entre as quais: a instantaneidade, eliminando as barreiras do tempo e espaço; a isonomia entre os que a utilizam, ressalvando-se questões tecnológicas e de conhecimento pessoal; o dinamismo, pontuado pelo armazenamento e acesso a uma infinidade de textos, imagens e sons, isoladamente ou em um mesmo documento; da sensação de anonimato àqueles que não querem se identificar etc.

Com tais aspectos, traz consigo uma grande abertura que tem seu lado positivo com a liberdade que proporciona, e por outro lado, em face da falta de controle, tem aspectos negativos, entre eles a invasão da privacidade. Tais observações, nos dias atuais, ganharam outras perspectivas, percebendo-se que o anonimato é uma sensação falsa, pois em muitos casos se pode identificar o usuário, sendo possível algum tipo de rastreamento.

Se, por um lado incontestáveis são os avanços e os benefícios que o uso ético da internet trouxe para a propagação da informação, por outro se tem riscos inerentes da tecnologia da informatização, notadamente os crimes virtuais.

A título de exemplo de condutas criminosas, podemos citar sites de pornografia infantil e de racismo, ofensas à honra das pessoas, disseminação de vírus, tráfico de entorpecentes, comércio eletrônico como meio de golpes, ciberterrorismo, em que ações podem levar a atingir um grupo, organização ou governo, financeira ou politicamente. Nesse diapasão, os fraudadores digitais acompanham o avanço tecnológico e por meio de engenharia social continuam a vitimar cada vez mais internautas.

A presença da internet no dia a dia mundial se tornou uma constante, não existindo mais possibilidade de volta ao passado, de forma que deve ser aceita e compreendida da melhor maneira possível, exigindo-se, para tanto, o estudo e a pesquisa dos fenômenos que lhes são afetos, tais como os crimes virtuais.

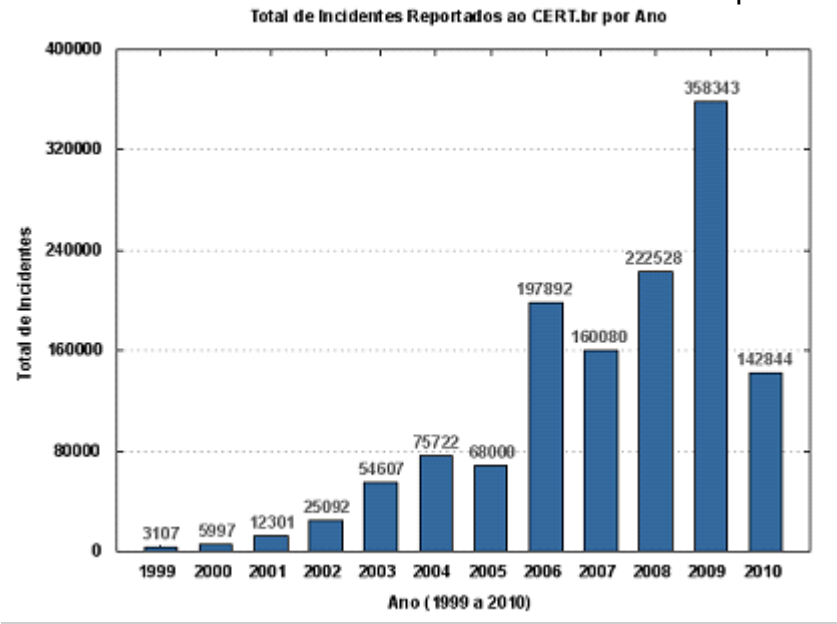
3 Dos crimes praticados por meio da internet

Como ressalta Lima (2006) a doutrina aborda a temática sobre o título de crimes virtuais, crimes digitais, crimes informáticos, crimes de informática, crimes eletrônicos, delitos computacionais etc. Sieber *apud* Rosa (2002, p. 53) conceitua crimes virtuais como sendo “qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados”.

Já Roque (2007, p. 25) conceitua como sendo “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. Importa ressaltar, no entanto que a doutrina não chegou a um consenso quanto ao nome jurídico do crime, tão pouco quanto o conceito dos crimes em espécie.

De acordo com Azeredo (2011), os crimes cibernéticos tomaram vulto nas últimas décadas, principalmente no ano de 2009, conforme demonstra gráfico abaixo:

GRÁFICO 01: Total de incidentes cibernéticos por ano



Fonte: CERT.br, 2010.

Para o autor, com as acirradas discussões e debates ocorridos em detrimento de tal acontecimento, no ano de 2010 observou-se uma queda significativa na prática destes crimes. O autor chama a atenção para o fato de que tais crimes ocorreram em todo o tipo de ambiente digital, seja ele empresarial, doméstico, financeiro ou comercial. Azeredo (2011) salienta o fato de o governo

brasileiro utilizar a tecnologia da informação para vários tipos de serviços públicos, bem como o Poder Judiciário, o qual passou do processo judicial do papel ao processo judicial eletrônico, necessário se fez a busca de uma solução para que tais crimes não ficassem impunes.

Segundo o autor, este tipo de crime, não só no Brasil, mas em todo o mundo, tem características particulares e diversas dos crimes comuns, surgindo à necessidade de uma maior preocupação com a segurança cibernética. Não importa as diferentes posições para tipificar o crime, o meio será sempre o mesmo, onde o computador é o instrumento e o ato em si é praticado utilizando a internet.

De acordo com Castro (2003) os crimes de internet possuem várias classificações, sendo que uma delas dá ao mesmo duas divisões: próprios e impróprios.

> Os primeiros são aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios. [...] impróprios admitem a prática por diversos meios, inclusive os meios informáticos (CASTRO, 2003, p. 23).

O autor também atenta para a classificação tripartida, que segundo ele se divide em:

> a) os crimes de informática puros, onde o agente objetiva atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; b) os crimes de informática mistos, onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa e c) os crimes de informática comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação (CASTRO, 2003, p. 24).

No entanto, classificar tais crimes não resolve o problema dos mesmos, sendo este tipo de classificação utilizado apenas como forma didática, uma vez que o *modus operandi* e a forma delitiva evoluem dia após dia.

Colli (2010, p. 32), classifica os crimes informáticos em virtuais puros, mistos e comuns, assim tem-se:

> Crime virtual puro - compreende em qualquer conduta ilícita, a qual atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a parte virtual do microcomputador. Crime virtual misto - seria o que utiliza a Internet para realizar a conduta ilícita, e o objetivo é diferente do

> citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes. Crime virtual comum - é utilizar a Internet apenas como forma de instrumento para realizar um delito que enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, como messengers, e-mail, torrent ou qualquer outra forma de compartilhamento de dados (COLLI, 2010, p. 32).

Como se pode ver, os crimes virtuais podem utilizar diferentes ferramentas para que se cometa o ato ilícito. A pessoa que o comete, segundo Colli (2010) é denominado *hacker*, sendo este classificado em interno ou externo. Interno são os indivíduos que acessam informações sigilosas, normalmente são funcionários de empresas ou servidores públicos e externos são os que não possuem nenhum tipo de ligação com a organização que atacam.

Para garantir a segurança, Colli (2010) cita alguns aspectos, como autenticação, confidencialidade e integridade. No que diz respeito à autenticação o autor ressalta que este é um aspecto fundamental da segurança, onde a entidade de um utilizador é validade. Já a confidencialidade prevê que apenas as pessoas que necessitam de determinadas informações tenham acesso às mesmas e finalmente a integridade a qual garante que a informação a ser processada é autêntica.

Em que pese às inúmeras abordagens doutrinárias quanto ao conceito da criminalidade informática e virtual é importante dizer que a caracterização do delito praticado por meio da internet dependerá da análise do caso concreto, devendo a conduta do delinquente se subsumir em norma prevista na legislação em vigor do país onde o delito for cometido. A exemplificação dos crimes apresentada não tem o condão de ser taxativa, pois existem vários crimes virtuais dos quais se escolheu os mais comuns para dar ênfase neste trabalho.

3.1 A internet e os crimes contra a honra

Segundo Furlaneto Neto *et al.* (2012), todos os delitos abaixo são compatíveis com suas práticas por meio da internet, a qual, nos casos citados, funciona apenas como um novo *modus operandi* para que se possa ter a ofensa da honra, quer na sua forma objetiva, quer na forma subjetiva.

Para o autor, nenhuma alteração legislativa é necessária ocorrer para tipificação da calúnia, difamação ou injúria praticadas por meio da rede mundial de computadores.

3.1.1 Calúnia

Segundo Furlaneto Neto (2012), caluniar, de acordo com o art. 138 do CP significa acusar falsamente alguém da prática de fato definido como crime, colocando em dúvida a sua credibilidade no meio social, atingindo, de tal forma, sua honra objetiva, isto é, o conceito externo que os outros têm da pessoa caluniada.

Ainda para o autor, o que se tutela no presente tipo penal é a honra objetiva à imagem da pessoal, constituindo os objetos material e jurídico do ilícito, não se exigindo a presença da vítima para a consumação do mesmo, uma vez que este ocorre quando o conhecimento da imputação falsa atinge terceiras pessoas.

Diante de tais constatações classifica-se a calúnia como sendo um crime comum, formal, de forma livre, comissivo, unisubjetivo, unisubsistente ou plurisubsistente, caso em que se admite tentativa.

3.1.2 Difamação

Para Furlaneto Neto *et al.* (2012), difamar significa atacar a reputação de alguém, desacreditando-o perante a sociedade, isso através de fato ofensivo à reputação, e não apenas negativo ou inconveniente, de acordo com o art. 139 do CP, mais uma vez tratando esse dispositivo legal da honra objetiva, da imagem social da vítima, que se constituem em seus objetos jurídico e material.

Ainda para o autor, sujeitos da difamação, assim como na calúnia, tanto o ativo como o passivo podem ser qualquer pessoa, neste último caso incluindo-se os inimputáveis. Por se referir o tipo penal a alguém, fica a pessoa jurídica excluída do polo passivo, podendo seus sócios ser vítimas do crime. O consentimento da vítima, também aqui, é admitido.

Segundo Furlaneto Neto *et al*. (2012), de forma diversa do delito de calúnia, o fato imputado não pode ser previsto em lei como crime, podendo ser tipificado como contravenção penal, no entanto deve ser descrito ao máximo possível, a fim de não ocorrer mero insulto, o que pode consistir injúria, devendo individualizar seu autor.

3.1.3 Injúria

Para Furlaneto Neto *et al*. (2012), nos termos do art. 140 do CP, injuriar é ofender atingindo a dignidade ou o decoro de alguém, sua honra subjetiva, o conceito que cada um tem de si próprio, sendo o objeto jurídico e material do ilícito em comento.

Ainda de acordo com o autor, no mesmo sentido dos outros dois delitos contra a honra, pode ser sujeito ativo e passivo qualquer pessoal, ficando de lado neste último caso, a pessoa jurídica por não possuir honra subjetiva. A denominada injúria real consiste na ofensa a honra subjetiva, uso de violência ou vias de fato, sendo indispensável que tal agressão considerada aviltante, humilhante, desprezível, quer com respeito ao utilizado quer pela sua própria natureza.

3.2 Crimes de fraude

No que diz respeito a estelionato ou fraude, Silva (2009, p. 8) utiliza o art. 171 do Código Penal, completando apenas que em casos de fraudes virtuais “esta seria a lesão ao patrimônio por meio enganoso, consumando-se, também, com o alcance da vantagem ilícita, em prejuízo alheio”.

Assim, de acordo com o autor:

> É utilizada em muitos casos de crimes econômicos, como manipulação de saldos de contas, balancetes em bancos, etc., alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. A fraude informática é o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido. Não requer conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador. Tradicionalmente a fraude envolve o uso de cartões de bancos roubados ou furtados. Usando software específico, podem-se codificar amplamente as informações eletrônicas contidas nas tarjas magnéticas dos cartões de bancos e nos de crédito (SILVA, 2009, p. 8).

Observa-se, porém, que para haver o estelionato nos crimes acima descritos necessário se faz que haja prejuízo alheio.

3.3 Dano

De acordo com Silva (2009), os crimes de dano são aqueles que incluem apagar, modificar, destruir, inutilizar, parcial ou completamente dados ou programas de computador. Já os crimes de veiculação de pornografia na internet possuem dois tipos de conduta, que seria a de oferecer serviço e/ou informação de caráter pornográfico utilizando-se para tal a internet.

Segundo Furlaneto Neto *et al*. (2012), o tipo penal encontra-se prescrito no art. 163 do CP. Com este, busca-se tutelar o patrimônio, no que tange tanto à propriedade quanto à posse, de bens móveis ou imóveis, de agressões perpetradas por outrem e que visem a anular ou diminuir sua utilidade ou valor.

Para o autor, o crime de dano somente será punível a título de dolo, exigindo-se portanto, que o agente haja impelido da consciência de destruir, inutilizar ou deteriorar coisa alheia. Nesse sentido, o erro quanto à propriedade do bem, ocorrido quando o agente danifica o bem alheio acreditando tratar-se de bem próprio, caracterizará erro de tipo. Pouco importa a motivação do agente, se por vingança, raiva ou a finalidade específica de causar prejuízo econômico à vítima, pois o tipo penal não exige cabimento subjetivo especial do tipo.

3.4 Estelionato

Segundo Furlaneto Neto et al (2012) previsto no art. 171 do CP, é conceituado pela conduta de o agente obter, para si ou para outrem, vantagem para si com prejuízo alheio, mediante artifício, ardil ou qualquer meio fraudulento.

Para Costa Júnior (2008, p. 437) “a vantagem ilícita é obtida como emprego da fraude visando à cooperação da própria vítima”, ou seja, o artifício se caracteriza pelo emprego de aparato material, encenação. Diversamente do furto, o que se visa não é especificamente a coisa alheia móvel, mas sim a vantagem ilícita, a qual deve ter caráter econômico, pois se encontra inserido entre os delitos contra bem jurídico, tratando-se de qualquer tipo de lucro, vantagem, ganho, devendo ser ilícito.

A consumação do estelionato se opera com a obtenção da vantagem indevida por parte do sujeito ativo, em face da fraude empregada, causando prejuízo a outrem.

3.5 Crimes contra a criança e o adolescente

Silva (2009) descreve uma alteração ocorrida no Estatuto da Criança e do Adolescente, pela Lei 11.829/08, a qual em seu art. 247 regulamenta a respeito de imagens de crianças ou adolescentes que possuem relacionamento com pornografia no meio cibernético.

Os art. 247-A até E, acrescentados pela Lei n° 11.829/08, tipificam as condutas “oferecer, trocar, disponibilizar, transmitir, distribuir, publicar divulgar, adquirir, possuir ou armazenar”, por quaisquer meios, vídeos ou imagem pornográficas que envolvam crianças ou adolescentes.

De acordo com Furlaneto Neto et al (2012), para a caracterização de cena de sexo explícito há a necessidade de reprodução de conjunção carnal ou ato libidinoso diverso da conjunção carnal, especificada pelo legislador como “atividades sexuais explícitas, reais ou simuladas”. Isso implica que se insere no contexto da definição legal a reprodução de cenas de sexo explícito por meio de desenhos e caricaturas. Por sua vez, a cena pornográfica reporta-se ao nu infanto-juvenil, com a exibição de órgãos genitais para fins primordialmente sexuais.

Caso o agente venha a fotografar criança e ou adolescente em cena de sexo explícito ou pornográfica e posteriormente vender ou expor a venda o objeto material do crime, responderá pelos crimes previstos nos arts. 240 e 241 do ECA em concurso material de crime.

3.6 Espionagem e sabotagem informática

Com relação à espionagem e sabotagem informática, Silva (2009) alega que tais crimes ocorrem quando programas são modificados, facilitando o acesso a dados, bem como quando existe a invasão e subtração de dados. Já a sabotagem é a destruição ou danificação que causem danos físicos e lógicos ao computador, envolvendo este ato os tais vírus de computador, os quais são programas feitos unicamente com a finalidade de gerar danos a outros computadores, podendo os mesmos se autocopiar para outros programas.

3.7 Crime contra a privacidade

Silva (2009) descreve o crime contra a privacidade como sendo um dos mais praticados, principalmente contra celebridades e personalidades públicas. A privacidade é um direito amparado pelo art. 5º., inciso X da CF/88, o qual diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação”.

O art. 20 do Código Civil dispõe o seguinte:

> Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais (BRASIL, 2002).

Segundo Brígido (2012), um exemplo foi o caso da atriz Carolina Dieckmann, a qual além de ter sua privacidade violada teve sua imagem denegrida, surgindo assim a Lei n. 12.737/12 ou Lei Carolina Dieckmann, como ficou conhecida e a qual será tratada mais adiante.

Um desdobramento da exposição da intimidade na internet são os casos da chamada “pornografia de vingança”, cada vez mais frequentes no Brasil, em que a intimidade de pessoas são expostas através de fotos e vídeos compartilhadas pelo ex-companheiro (a), que geralmente não aceita o fim do relacionamento e age dessa forma para denegrir a imagem da pessoa como uma forma de vingança. Podemos citar como exemplo o recente caso de uma adolescente de 16 anos do interior do Rio Grande do Sul que se matou após descobrir que o ex-namorado divulgou imagens íntimas dela na internet. E de uma outra adolescente do Piauí que teve um vídeo íntimo divulgado no W*hatsApp* e se suicidou. As mortes dessas duas meninas após a divulgação das imagens íntimas delas na internet trazem à tona a discussão sobre a penalização, e segundo Barros (2013) a necessidade de se criar uma tipificação criminal específica para esse tipo de conduta. O tema preocupa e já reverbera no Congresso Nacional, onde quatro projetos de lei sobre o tema foram apresentados neste ano, na tentativa de tornar mais dura a punição aos responsáveis pela prática.

Apresentado em maio, o Projeto de Lei 5555/2013, do deputado João Arruda (PMDB/PR) é conhecido como “Lei Maria da Penha virtual”. Ele propõe alterações nesta lei para que violação da intimidade da mulher na internet seja considerada violência doméstica e familiar.

A deputada Rosane Ferreira (PV/PR) também apresentou o PL 5822/2013 com finalidade semelhante. A matéria foi apensada ao PL do deputado Arruda, que teve outros dois projetos de lei anexados: o PL 6630/2013 e o PL 6713/2013.

O primeiro, proposto em outubro de 2013 pelo deputado Romário (PSB/RJ), pede que seja acrescentado “ao Código Penal, tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima.” A pena prevista é de detenção, de um a três anos, além de multa.

Sugere ainda que a pena seja aumentada de um terço se o crime é cometido “com o fim de vingança ou humilhação” e por “cônjuge, companheiro, noivo, namorado ou alguém que manteve relacionamento amoroso" com a pessoa que foi lesada.

De acordo com a matéria, o autor “fica sujeito a indenizar a vítima por todas as despesas decorrentes de mudança de domicílio, de instituição de ensino, tratamentos médicos e psicológicos e perda de emprego”.

Na mesma toada, o PL 6713/2013, de autoria da deputada Eliene Lima (PSD/MT), dispõe sobre punição a quem praticar vingança pornográfica. Para a parlamentar, o autor deve ser penalizado com um ano de reclusão mais multa de 20 salários mínimos. As postagens podem se referir tanto a mulheres quanto a homens.

Por tratarem do mesmo tema, todos os projetos passaram a tramitar juntos.

3.7.1 Invasão da Privacidade e o Aplicativo *Secret*

Ainda podemos citar o aplicativo para celular chamado *Secret* que tem provocado polêmica nas redes sociais nos últimos meses. Foi criado em fevereiro deste ano por *Chrys Bader* e *David Byttow,* ex-funcionários do *Google*. De acordo com o site G1 (2014) permite ao usuário contar segredos dele próprio ou de amigos anonimamente. Pessoas comentam frases que leram e fotos íntimas que viram, sem ter seu nome ou foto divulgados. Os usuários se sentem livre para compartilhar segredos e fotos. Ao instalar o *App,* é necessário conectá-lo com sua conta do *Facebook,* permitindo que ele acesse a lista de amigos para acessar suas

mensagens publicadas no *Secret*. Os desenvolvedores, dois ex-funcionários do *Google,* afirmam que é impossível identificar quem contou o segredo, já que não há nenhum dado ou foto do usuário. Eles também afirmam que não há risco de o segredo vazar no *Facebook.*

Em meio a tanta polêmica, e a exposição da intimidade de várias pessoas por meio deste aplicativo, em Agosto a Justiça do Espírito Santo determinou, em decisão liminar, a retirada do *Secret* das lojas de aplicativo de *Google* e *Apple*. A Justiça acolheu o pedido do Ministério Público do Espírito Santo, que protocolou uma ação civil pública. Além de determinar a suspensão do aplicativo, a Justiça decidiu ainda que as empresas devem também remover remotamente os aplicativos dos smartphones das pessoas que já os instalaram. Esse também era um pedido do Ministério Público do Espírito Santo, em ação assinada pelo promotor Marcelo Zenkner. A Justiça fixou multa de R$ 20 mil para cada dia de descumprimento.

Para o juiz Paulo Cesar de Carvalho, da 5ª Vara Cível de Vitória, o *Secret* infringe princípios constitucionais, por permitir que seus usuários usufruam do direito à liberdade de expressão sob a condição de anonimato. Escreveu o juiz na sua decisão o seguinte:

> A liberdade de expressão não constitui um direito absoluto, sendo inúmeras as hipóteses em que o seu exercício entra em conflito com outros direitos fundamentais ou bens jurídicos coletivos constitucionalmente tutelados, que serão equacionados mediante uma ponderação de interesses, de modo a garantir o direito à honra, privacidade, igualdade e dignidade humana e, até mesmo, proteção da infância e adolescência, já que não há qualquer restrição à utilização dos aplicativos indicados na inicial.

O Google recorreu da decisão liminar por meio do Agravo de Instrumento nº 0030918-28.2014.8.08.0024. Já a Microsoft recorreu por meio do Agravo de Instrumento nº 0031238-78.2014.8.08.0024 e em Setembro a Justiça do Espírito Santo voltou atrás e o aplicativo *Secret*, que permite publicar qualquer mensagem, inclusive ofensas diretas à pessoas, sem ser identificado, voltou a ser distribuído gratuitamente nas lojas online de *Apps* do Google e da Apple. O recurso em segunda instância teve vitória do Google. A suspensão foi determinada pelo desembargador Jorge Henrique Valle dos Santos, da terceira câmara cível do Tribunal de Justiça do Espírito Santo que analisou em sede liminar. O desembargador baseou sua decisão no fato de que ele acredita que o anonimato prometido pelo *Secret* não é totalmente verdadeiro, já que é possível rastrear seus

usuários pelo IP do computador. Além disso, caso as empresas tentassem remover os aplicativos já instalados nos smartphones, elas iriam contra as leis brasileiras.

"Na concretude do caso, é preciso ponderar que, não obstante o anonimato que figura como a própria razão de ser do aplicativo, não me parece haver dúvidas quanto à possibilidade de identificação do usuário por meio de seu IP (internet protocol)", disse, e ainda frisou que:

> "Há de ser ponderado, ainda, que determinações contidas na decisão recorrida revelam-se tecnicamente inviáveis, a ensejar, até mesmo, diante de uma análise perfunctória, violação do direito à privacidade dos usuários, na medida em que impõe à empresa que estabeleça um acesso remoto aos aparelhos de todos os cidadãos que já instalaram o aplicativo em seus respectivos smartphones a fim de que se remova o programa dos aparelhos, ato este de viabilidade técnica duvidosa e de juridicidade discutível, ainda mais considerado o prazo de dez dias ofertados, sob pena de multa diária".

Outro exemplo de exposição da intimidade segundo Brígido (2012), foi o caso da atriz Carolina Dieckmann, a qual além de ter sua privacidade violada teve sua imagem denegrida, surgindo assim a Lei n. 12.737/12 ou Lei Carolina Dieckmann, como ficou conhecida mas que ainda não é suficiente para amparar as vítimas desse tipo de crime, o que será tratado no próximo capítulo.

4 Lei n. 12.737/2012 Lei Carolina Dieckmann e Lei do Marco Civil

A Lei 12.737/2012 ou Lei Carolina Dieckmann, segundo Paulino (2013), promoveu alterações no Código Penal Brasileiro, tipificando os delitos ou crimes informáticos.

A legislação é proveniente do Projeto de Lei n. 2793/2011, o qual tramitou no Congresso Nacional em regime de urgência, uma vez que a atriz Carolina Dieckmann teve copiadas de seu computador pessoal trinta e seis fotos íntimas, as quais terminaram expostas na internet (PAULINO, 2013).

Ainda segundo o autor, apesar da aprovação da Lei a mesma gera discussões, devido a seu aspecto confuso, onde por vezes gera dupla interpretação, ou até mesmo interpretações subjetivas que podem enquadrar o ato ilícito em condutas triviais, sendo tal lei tida por alguns como ineficaz.

A Lei acresceu os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal. Os delitos previstos na Lei 12.737/2012 são:

> Art. 154-A - Invasão de 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. Art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa. Art. 298 - Falsificação de documento particular/cartão - Pena - reclusão, de um a cinco anos, e multa (BRASIL, 2012).

De acordo com Azeredo (2012), a Lei 12.737/12 considera os crimes cibernéticos dentro da realidade material. A Lei engloba os crimes informáticos e cibernéticos, que de acordo com Colli (2010, p. 44):

> A ligação entre cibernética, ciberespaço e crimes informáticos permite que se compreenda o instituto do *cibercrime* como sendo aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados por um mais indivíduos, no cometimento de uma ou mais, conduta(s), criminalizada(s), ou são alvo(s) desta(s).

O texto legal de acordo com Oliveira Júnior (2012) tem a finalidade de incriminar os indivíduos que driblam os mecanismos de segurança digital e invadem a privacidade alheia. No entanto, necessário se faz que o usuário tenha instalado em

seu equipamento antivírus, *firewall*, senhas e todo tipo de defesa digital que possa utilizar.

Segundo o autor, o legislador prevê uma pena de três meses a um ano e multa, no entanto caso o delito resulte em prejuízo econômico à vítima a pena é aumentada de um sexto a um terço.

Há também uma previsão maior de pena, no parágrafo 3º., onde prevê uma reclusão de seis meses a dois anos e multa caso a invasão tenha como objetivo obter conteúdos privados, segredos comerciais ou industriais ou até mesmo informações sigilosas. Deste modo o legislador protege as atividades comerciais e industriais, bem como as instituições bancárias (OLIVEIRA JÚNIOR, 2012).

Afirma Oliveira Júnior (2012) que:

> A ação penal nos casos dos crimes do "*caput*" será pública condicionada à representação da vítima. Quer dizer, mesmo em se tratando de cometimento do ilícito, o legislador outorgou para a vítima o oferecimento da condição de procedibilidade, observando-se a legitimidade para tanto e a fluência do prazo decadencial que deságua 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.*

Para o autor, houve certa demora em se instituir esta lei, uma vez que a sociedade brasileira já, há bastante tempo, estava sendo vítima deste tipo de invasão de privacidade.

4.1 Equiparação do cartão de crédito/débito a documento particular

Segundo Oliveira Júnior (2012), com o advento da nova lei há uma equiparação entre o cartão de crédito ou débito com documento particular, assim caso haja fraude utilizando os mesmos, vale lembrar que são objetos materiais do crime de falsidade documental. Para a configuração do crime basta que exista a inserção de dados impregnados na tarja magnética (parte juridicamente relevante do documento), que permite o acesso a sistemas bancários ou de crédito pertencentes à determinado correntista, não emitidos pela instituição correspondente.

De acordo com o autor, todavia, somente a conduta de falsificar no todo ou em parte o cartão será considerada crime, o que não ocorre com a simples posse de um cartão clonado por quem não foi responsável pela falsificação. Se utilizado o cartão e

alcançado o dano patrimonial, em regra, tratar-se-á de crime de furto qualificado pela fraude e a falsidade será absorvida.

4.2 Lei do Marco Civil da Internet

O Marco Civil da Internet, Lei 12.965/14, estabelece princípios, garantias, direitos e deveres dos usuários da Internet no Brasil, sendo a primeira lei construída de forma colaborativa entre Governo e sociedade utilizando a internet como plataforma de debate.

O Marco Civil da Internet começou a ser elaborado em 2009, pelo Ministério da Justiça em colaboração com o Centro de Tecnologia e Sociedade, da Fundação Getúlio Vargas, bem como com a participação direta da sociedade civil, comunidade empresarial e representantes das áreas técnica e acadêmica, por meio de colaboração on-line direta e aberta.

Após extenso debate público, com mais de 2.300 contribuições, o Projeto foi encaminhado ao Congresso Nacional em 2011, como o PL 2126/2011, e o deputado Alessandro Molon foi designado seu relator no ano seguinte. Durante o período da relatoria, foram realizadas sete audiências públicas, que contaram com a presença de representantes de 60 instituições dos mais diversos setores, como empreendedores, acadêmicos, operadoras telefônicas, ativistas, órgãos de governo, artistas e empresas de tecnologia, dentre outros.

O Marco Civil da Internet foi colocado em novo debate público por meio do portal e-Democracia da Câmara dos Deputados, onde o texto teve 45 mil visitas, 2.215 comentários e 374 propostas. Foi a primeira vez na Câmara dos Deputados que um relatório utilizou sugestões enviadas pela internet, até mesmo via *Twitter.*

De acordo com Bissoli (2014), a Lei n. 12.965/14 ou Lei do Marco Civil da Internet busca inovar, no entanto tira um pouco da liberdade do usuário da internet. Tal lei tem por pretensão promover a igualdade e a inclusão digital.

Segundo Bissoli (2014), destaca-se a preocupação com a liberdade de expressão dos usuários, proteção de dados pessoais, neutralidade e funcionalidade da rede, acesso às informações.

Afirma o autor que o Marco Civil define como responsabilidade do provedor de conexão a guarda e sigilo dos registros de conexão à internet por um prazo de um ano, no entanto, até a presente data não há qualquer dispositivo legal que

estabeleça esta conduta. Entretanto, deixou uma lacuna no que diz respeito aos provedores de aplicativos, os quais estão isentos de qualquer responsabilidade sobre danos decorrentes do uso por terceiros.

De acordo com Pereira (2014) O Marco Civil considera a internet uma ferramenta fundamental para a liberdade de expressão e diz que ela deve ajudar o brasileiro a se comunicar e se manifestar como bem entender, nos termos da Constituição.

O texto chega a apontar que "o acesso à internet é essencial ao exercício da cidadania". O internauta tem garantia de que sua vida privada não será violada, a qualidade da conexão estará em linha com o contratado e que seus dados só serão repassados a terceiros se ele aceitar - ou em casos judiciais, chegaremos a este tópico.

4.2.1 Neutralidade

Um dos pontos essenciais do Marco Civil é o estabelecimento da neutralidade da rede. O governo até pode fazer essa discriminação, mas só em duas situações: se ela for indispensável para a prestação dos serviços; ou se serviços de emergência precisar ser priorizados. Mesmo assim, o presidente que estiver no comando não tem como simplesmente mandar tirar internet de um lugar e botar no outro. Ele precisará consultar o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações.

4.2.2 Guarda de informações

Os provedores de internet e de serviços só serão obrigados a fornecer informações dos usuários se receberem ordem judicial. No caso dos registros de conexão, os dados precisam ser mantidos pelo menos por um ano, já os registros de acesso a aplicações têm um prazo menor: seis meses.

Qualquer empresa que opere no Brasil, mesmo sendo estrangeira precisa respeitar a legislação do país e entregar informações requeridas pela Justiça. Caso contrário, enfrentarão sanções entre advertência, multa de até 10% de seu faturamento, suspensão das atividades ou proibição de atuação.

Foi derrubada a obrigatoriedade de empresas operarem com data centers no Brasil ainda na Câmara.

4.2.3 Responsabilização pelo conteúdo

Pereira (2014) afirma que a empresa que fornece conexão nunca poderá ser responsabilizada pelo conteúdo postado por seus clientes. Já quem oferece serviços como redes sociais, blogs, vídeos etc. corre o risco de ser culpado, caso não tire o material do ar depois de avisado judicialmente. Por exemplo: se a Justiça mandar o *Google* tirar um vídeo racista do *YouTube* e isso não for feito, o *Google* se torna responsável por aquele material.

Haverá um prazo para que o conteúdo considerado ofensivo saia de circulação, mas o juiz que cuidar do caso pode antecipar isso se houver “prova inequívoca”, levando em conta a repercussão e os danos que o material estiver causando à pessoa prejudicada.

4.2.4 Obrigações do governo

Administrações federal, estaduais e municipais terão uma série de determinações a cumprir, caso o Marco Civil se torne realidade. Entre eles estabelecer “mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica”.

Os governos serão obrigados a estimular a expansão e o uso da rede, ensinando as pessoas a mexer com a tecnologia para “reduzir as desigualdades” e “fomentar a produção e circulação de conteúdo nacional”.

Os serviços de governo eletrônico precisarão ser integrados para agilizar processos, inclusive com setores da sociedade, e a internet ainda será usada para “publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada”.

Por fim, há ainda a preferência por tecnologias, padrões e formatos abertos e livres, e a de se estimular a implantação de centros de armazenamento, gerenciamento e disseminação de dados no Brasil, “promovendo a qualidade

técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa".

Desta forma, o anonimato é favorecido no que diz respeito ao uso das aplicações, o que gera risco às atividades empresariais por falta de identificação do usuário. Com isso, não se buscará mais o responsável por um IP, mas sim o próprio registro de conexão junto à aplicação.

Portando, podemos perceber que a regulamentação e penalização do uso da internet no Brasil ainda é matéria controvertida na doutrina e jurisprudência, sendo necessária a criação de uma legislação mais abrangente e concisa no que tange aos crimes virtuais.

5 Aplicabilidade da analogia

Preceitua Furlaneto Neto *et al.* (2012) sobre a importância da discussão que se produz em volta da analogia sempre que se debate sobre o fato de um tipo penal englobar ou não determinada ação ou omissão, não prevista de modo literal ou expressa na legislação existente, mas semelhante ao que foi legalmente previsto, ou seja, onde existe uma lacuna.

Antes de mais nada, necessário se torna distinguir a analogia da interpretação analógica, sendo a última uma forma de interpretação prevista na própria lei, estando nesta contida à intenção de abranger os casos semelhantes. Já a analogia, como se sabe, não é forma de interpretação, mas sim de integração da lei, prevista inicialmente da lei de introdução às normas do direito brasileiro, em seu artigo 4: “quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito”. Tal norma é de aplicação ao Direito em geral. Percebe-se da leitura deste artigo que a analogia é o primeiro recurso de que se vale o juiz diante da lacuna da lei, daí sua grande importância.

Maria Helena Diniz (1994, p.108), socorrendo-se em Tércio Sampaio Ferraz, afirma ser “a analogia um procedimento quase lógico, que envolve duas fases: a constatação, por comprovação, de que há uma semelhança entre fatos-tipos diferentes e um juízo de valor que mostra a relevância das semelhantes sobre as diferenças, tendo em vista uma decisão jurídica procurada”. Para tal autora, analogia encontra seu fundamento na igualdade jurídica, exigindo uma semelhança entre o previsto em lei e o não regulado por ela, para que ocorra uma decisão igual.

Nesse mesmo sentido, podem ser citadas as lições de Fragoso (1990), ao observar que, em face do princípio da reserva legal, não se pode criar novas figuras penais, agravar a posição do réu (analogia *in malam partem)* ou ainda se aplicar penas ou medidas de segurança que não estejam legalmente previstas, pois, segundo ele, “a analogia é somente admissível, em princípio, nos casos em que beneficia o réu (analogia *in bonam partem)*, mas não pode ser acolhida em relação às normas excepcionais” (FRAGOSO, 1990, p.86).

Este posicionamento se mostra como o mais acertado, posto que com ele se alcança segurança jurídica, a qual, no Direito Penal, é por demais necessária, pois de outra forma correr-se-ia o risco de punir condutas não previstas legalmente como

delituosas, pelo mero entendimento jurídico ao aplicar-se a analogia, desfigurando-se o Estado Democrático de Direito.

Assim existe consenso quanto à impossibilidade de se aplicar a analogia para criar figura delitiva ou sanção penal não prevista legalmente de modo expresso, mesmo porque, em face das garantias constitucionais previstas no artigo 5, do Texto Maior, não é permitido tal tipo de integração da norma.

Ainda de acordo com Furlaneto Neto et al (2012) é justamente sob esse aspecto que o estudo da analogia traz importante subsídios ao tema objeto deste trabalho, pois caso venha a se considerar que os delitos praticados via internet não precisam de uma legislação específica, estando compreendidos nas normas já existentes, deve-se ter muito cuidado para não estar aplicando-se indevidamente aquele instituto, vedado que é seu emprego, como se viu, para criar novas figuras penais.

6 Considerações finais

Por ser um ser social, o homem necessita comunicar-se, sendo assim cria tecnologias que lhes permite praticidade e conforto. Com o surgimento da internet, a mesma se tornou uma ferramenta de extrema necessidade para todos. No entanto, essa mesma tecnologia é usada para cometer atos ilícitos, e lesar pessoas, seja de que forma for, surgindo assim os crimes virtuais.

Com o intuito de coibir os vários crimes virtuais enquadrando-os no Código Penal é que se destaca a Lei 12.737/12, (Lei Carolina Dieckmann), a qual foi publicada em 2012, mas somente entrou em vigor em 02 de abril de 2013.

Tal lei tipifica vários crimes virtuais, como clonagem de cartão de crédito ou débito, invasão de dispositivos de informática, perturbação ou indisposição de serviços telemáticos. Porém nota-se, que as tecnologias avançam em progressão geométrica, surgindo a cada dia um novo programa ou modelo de computador, os quais por consequência fazem surgir novas práticas de delitos cibernéticos, os quais estão muito além da legislação vigente. Desta forma, necessário se faz que sejam criadas normas específicas para cada tipo de crime que surge.

No que diz respeito à Lei 12.965/14 (Lei do Marco Civil da Internet) observa-se que a mesma apesar de ter contribuído para o regulamento do uso da internet ainda não é o suficiente para coibir o crescimento dos crimes virtuais, pois a responsabilidade e a penalização desses crimes ainda são difíceis de serem definidas.

Assim, observou-se que apesar de existir uma legislação específica para o caso de crimes virtuais, devido ao grande avanço tecnológico, ainda há lacunas que devem ser preenchidas pelo legislador, a fim de coibir os novos crimes que surgem a cada dia.

Referências

AZEREDO, E. **Segurança na internet.** Disponível em: <www.edemocracia.camara.gov.br>. Acesso em: 08 jun. 2014.

BARROS, Ana Cláudia. **Intimidade na internet:** casos de *sexting* aumentam e Congresso discute quatro projetos. Disponível em: < www.noticias.r7.com>. Acesso em: 14 nov. 2014

BISSOLI, L. **Marco civil da internet:** o retrocesso no registro e guarda de dados. Disponível em: <www.revistavisaojuridica.uol.com.br>. Acesso em: 10 jun. 2014.

BRIGIDO, E. H. **Carolina Dieckmann nua, além de ter sua privacidade violada teve sua imagem denegrida.** Disponível em: <www.trabalhistaribeirao.com.br>. Acesso em: 09 jun. 2014.

CAMPOS, A. L. N. **Sistema de segurança da informação:** controlando riscos. Visual Books. Florianópolis, 2006.

CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2 ed. Rio de Janeiro : Lumen Juris, 2003.

COLLI, M. **Cibercrimes:** limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

DINIZ, Maria Helena**. Curso de Direito Civil Brasileiro - 1º volume**, 10ª edição, São Paulo, Editora Saraiva, 1994.

EBIT. Disponível em: <http://www.ebit.com.br>. Acesso em: 08 jun. 2014.

FRAGOSO, Heleno Cláudio. **Lições de direito penal. Parte especial**. 6 ed, Rio de Janeiro: Forense, 1990.

FURLANETO NETO, M.; SANTOS, J. E. L.; GIMENES, E. V. **Crimes na internet e inquérito policial eletrônico.** São Paulo: Edipro, 2012.

G1. **Justiça libera o aplicativo Secret no Brasil a pedido do Google**. Disponível em: < http://www.g1.globo.com>. Acesso em 14 nov. 2014.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** Campinas: Milennium, 2006.

OLIVEIRA JÚNIOR, E. Q. **A nova lei Carolina Dieckmann**. Disponível em: <www.atualidadesdodireito.com.br>. Acesso em: 10 jun. 2014.

PEREIRA, Leonardo. **Cinco pontos essenciais para entender o marco civil da internet.** Disponível em: < http://olhardigital.uol.com.br/noticia/>. Acesso em: 14 nov. 2014.