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

TARCÍSIO ALVES TAVARES

ANÁLISES INICIAIS E CRÍTICAS À LEI 12.737/2012 – LEI CAROLINA DIECKMANN

BARBACENA
2013

ANÁLISES INICIAIS E CRÍTICAS À LEI 12.737/2012 – LEI CAROLINA DIECKMANN

Tarcísio Alves Tavares *

Colimar Dias Braga Júnior **

Resumo

A Lei 12.737/12, conhecida como Lei Carolina Dieckmann trouxe à esfera penal normatização para invasão de informações em computadores e outros equipamentos eletrônicos. Necessário é tratar este assunto por todos os membros da sociedade acadêmica ou não, para portar-se de forma coesa e ter conhecimento e respaldo jurídico. Este artigo irá apresentar as principais falhas como a terminologia utilizada na lei, a pena máxima branda, a precariedade da polícia técnica, objetivando discutir e reportar ao cidadão sobre a existência de uma lei que em suas linhas trouxeram falhas que podem dificultar e até impossibilitar a aplicabilidade para o fim pretendido, isto é, segurança jurídica contra crimes cibernéticos. Metodologicamente será utilizada a literatura da rede mundial de computadores (internet) e livros sobre o assunto. O artigo abordará como a imprensa brasileira conseguiu obter êxito através da pressão no Congresso para que se dessem respostas imediatas contra os crimes virtuais devido à violação virtual da intimidade da atriz Carolina Dieckmann, entretanto a legislação foi feita, tramitada, votada, promulgada e publicada, mas acabou contendo falhas no texto legal e sendo alvo de alguns pontos críticos.

Palavra-chave: Lei 12.737/12. Lei Carolina Dieckmann. Invasão de Privacidade.

1 Introdução

Este artigo tratará sobre a Lei 12.737/12[1] e objetiva dar subsídios à população para entrar na discussão do tema. Legislação que torna ilícito penal a prática da invasão à dispositivo alheio para obtenção de vantagens indevidas.

Vale ressaltar que a Lei foi recém-criada e há muita discussão sobre diversos pontos, iremos aqui destacar apenas os mais relevantes e complicadores da aplicabilidade do caso

* Acadêmico do 10º período do Curso de Graduação em Direito da Universidade Presidente Antônio Carlos – UNIPAC Barbacena - MG - E-mail: tavarestarcisio85@gmail.com

** Professor Orientador – Especialista em Direito Penal e Processual Penal. Professor de Medicina Legal e Direito Penal da Universidade Presidente Antônio Carlos. E-mail: colimarjunior@hotmail.com.

[1] http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

abstrato instituído na lei dentro do caso concreto.

Tudo começou em uma sexta-feira, 04 de maio de 2012, quando a vida da atriz Carolina Dieckmann mudou totalmente, fotos de sua intimidade foram publicadas na internet. Em sua maioria fotos sensuais feitas com celular em que a atriz aparecia nua.

E como na República Federativa do Brasil vemos diversas vezes o Congresso Nacional funcionar com presteza apenas através da pressão popular e/ou da mídia, foi o que ocorreu. Sendo uma atriz "global" houve forte lobby da Rede Televisiva Globo e o projeto do Deputado Paulo Teixeira (PT-SP), que apesar de não ter sido propriamente feito para o caso específico, mas que já estava em tramitação, foi aprovado no Congresso e publicado em 30 de novembro de 2012, isto é, pouco mais de seis meses após o ocorrido. Entretanto com "*vacácio legis*" de 120 dias, sendo assim, aplicabilidade no mundo real apenas após este prazo, ocorrendo em 03 de abril de 2013.

A Lei ficou, portanto, conhecida com Lei Carolina Dieckmann pelo fato notório ocorrido em sua tramitação.

2 Análises Iniciais e Críticas à Lei 12.737/2012 – Lei Carolina Dieckmann

A legislação entrou em vigor, entretanto com pontos obscuros e que representam grande temor, pois a sua aplicabilidade poderá não ocorrer devido a falhas e preciosismo demasiado do legislador.

Penido (2013)[2] bem introduz a discussão do artigo:

> Muito se tem falado sobre a Lei de Crimes praticados na Internet (Lei nº 12.737/2012), projeto do deputado federal Paulo Teixeira (PT-SP), mais conhecida como "Lei Carolina Dieckmann". Alguns criticaram a rapidez com que o projeto caminhou depois que a atriz Carolina Dieckmann teve suas fotos íntimas arquivadas em seu computador pessoal divulgadas na internet, afirmando tratar-se de um "casuísmo"; outros louvam a iniciativa.
> A verdade é que antes da Lei 12.737/2012, os especialistas da área de direito penal eletrônico afirmavam que 95% dos crimes ocorridos no meio informático já estavam previstos, havendo necessidade de se preencher essa lacuna de 5%. Só o tempo dirá se a lei atingiu seu objetivo.

2.1 A Lei

A legislação inova no ordenamento jurídico brasileiro por ter sido a primeira que tipifica como ilicitude penal, sujeitando a pena, a invasão de dispositivo informático de

[2] http://www.tiespecialistas.com.br/2013/04/os-crimes-previstos-na-lei-carolina-dieckmann/

outrem, estando ou não em rede (internet/intranet), através de violação de dispositivo de segurança, para obter vantagens ilícitas:

> [...]Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.[...]

E define como a ação penal condicionada a representação, isto é, só cabe o Poder Judiciário se manifestar, como órgão inerte que é, quando a parte que sofreu o crime, representar contra seu autor. Havendo exceção apenas no caso do crime contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, incluindo até concessionárias de serviços públicos:

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

Resumidamente temos em seu artigo 1º a lei define que tratará da tipificação de delitos informáticos e dará outras providências.

No artigo 2º acresce ao código penal os artigos 154-A e 154-B.

O artigo 154-A define que a invasão a dispositivo alheio, conectado ou não à internet, violando mecanismo de segurança para obter, adulterar ou destruir informações sem autorização do proprietário ou instalar vulnerabilidade para obter vantagem ilícita ocorrerá em pena. No parágrafo primeiro define que enquadrará na mesma tipificação quem fornece dispositivo para facilitar esta invasão.

Milagre (2013)[3] ressalta semelhança do dispositivo com a convenção de Budapeste:

> No que diz respeito a empresas de pesquisa e segurança da informação, a Lei tenta "imitar" os princípios da convenção de Budapeste, também punindo aquele que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da invasão. Temos que entender ou "ler", no intuito de permitir a prática da invasão com fins ilícitos, tal como previsto no artigo 154-A (A Convenção do Cibercrime de Budapeste recomenda até mesmo a punição de quem disponibiliza senhas para acesso a ativos de terceiros).

[3] http://webinsider.com.br/2013/04/16/o-que-mudou-com-a-lei-carolina-dieckmann/

> Assim, distribuições Linux como Backtrack, programas para invasão como sqlmap, havij, e frameworks como Metasploit, são amplamente utilizados por profissionais de segurança e empresas na consecução dos seus trabalhos, e não poderão ser confundidos, por autoridades, como, por exemplo, códigos para coleta de dados de cartão de crédito, Keyloggers bancários desenvolvidos especificamente para lesar correntistas, dentre outros códigos que por sua natureza e diante do contexto do caso concreto, avaliada por perito digital, restar claro não se tratar de ferramentas usadas para "boas finalidades".

No parágrafo segundo há hipótese de agravante caso resulte prejuízo econômico.

Já no terceiro parágrafo define que se a invasão viola algo protegido em lei, como sigilo industrial, comercial, ocorrerá em pena mais gravosa, definida no parágrafo seguinte.

E em último agrava-se a pena quando se trata de crimes contra Presidente, Governadores, Prefeitos, Ministros do Supremo Tribunal Federal, Presidente da Câmara e correspondentes a nível municipal, estadual e federal.

O artigo 154-B define a forma de representação, isto é, será condicionada a representação da vítima, salvo os casos contra a administração pública e concessionárias de prestação de serviço público.

Já o artigo 3º modifica os artigos 266 e 298 do código penal, incorrendo em mesma pena o indivíduo que interromper o serviço telemático ou de informação pública, ou ainda impedir ou dificultar o seu estabelecimento, sendo agravada a pena no caso de ocorrer o crime quando de uma calamidade pública. E por fim equipara o documento particular ao cartão de crédito no parágrafo segundo.

2.2 Da Pena

Observa-se que a lei tem pena muito branda no que tange a pena máxima, limitando assim o poder do julgador, pois há casos em que a extensão pode ser muito grande e com a pena máxima em até um ano, caberá muitas benevolências que a lei penal traz ao apenado, como regime aberto, transação penal, entre outros, além de não caber prisão temporária ou preventiva (OLIVEIRA, 2012)[4].

[4] http://jus.com.br/artigos/23655/lei-carolina-dieckmann

2.3 O Termo Sistema de Segurança

A Reportagem da UOL (2013)[5] destacou que "[...] feita para proteger usuários de crimes cometidos no ambiente virtual, ela só vale para casos de violação de eletrônicos com algum tipo de sistema de segurança [...]".

Oliveira (2012)[6] critica veementemente a lei, visto suas brechas:

> Não deixem seus computadores ligados, pois a lei exige "violação indevida de mecanismo de segurança", de sorte que, se o computador estiver ligado e não for exigida nenhuma senha, não haverá crime. Aliás, nesse tocante, pode-se entender que sequer houve invasão, já que se trata de um termo técnico que mereceria explicação.

Realmente houve preciosismo do legislador ao informar este termo "mecanismo de segurança", pois apenas a palavra violação se completa, não seria necessário o termo, que acaba jogando de certa forma a responsabilidade para o usuário por outrem que venha a invadir seu computador, celulares, etc.

Ratificando este entendimento Oliveira (2012)[7] ironiza a situação:

> Não deixem seus computadores ligados, pois a lei exige "violação indevida de mecanismo de segurança", de sorte que, se o computador estiver ligado e não for exigida nenhuma senha, não haverá crime. Aliás, nesse tocante, pode-se entender que sequer houve invasão, já que se trata de um termo técnico que mereceria explicação.

Milagres (2013)[8] dispõe sobre este caso:

> Invadir significa devassar, entrar a força. Esta "invasão" deve se dar em um dispositivo informático, que embora esteja associado a um "hardware" que armazena, trata ou processa informações ou dados, possa ter sua interpretação estendida por autoridades nos casos de invasão de ativos lógicos como um disco virtual, rede social, webmail de um serviço web ou ativos lógicos protegidos que armazenem informações (Embora tais interpretações devam ser freadas pelo principio da legalidade, é o que esperamos.)
> Deve-se esclarecer que a invasão, para ser criminosa, deve se dar sem a autorização expressa ou tácita do titular dos dados ou do dispositivo. Logo, o agente que realiza teste de intrusão "pentest", não pode ser punido, por não estarem reunidos os elementos do crime. Caberá, no entanto, às empresas de segurança e auditoria, adaptarem seus contratos de serviços e pesquisa neste sentido, prevendo expressamente a exclusão de eventual incidência criminosa nas atividades desenvolvidas.

[5] http://tecnologia.uol.com.br/noticias/redacao/2013/04/24/lei-carolina-dieckmann-so-vale-para-eletronicos-com-sistema-de-seguranca.htm
[6] http://jus.com.br/artigos/23655/lei-carolina-dieckmann
[7] *Ibidem*
[8] http://webinsider.com.br/2013/04/16/o-que-mudou-com-a-lei-carolina-dieckmann/

2.4 Finalidade da Invasão

Outro ponto criticado é a finalidade da invasão, isto é, obter vantagem ilícita, pois caso o criminoso queira apenas ver informações da pessoa e não termine por obter nenhuma vantagem, ele não estará cometendo crime previsto e sim apenas uma violação às informações da pessoa, sem que haja qualquer punição. Nestes termos também expressa preocupação Oliveira (2012)[9]:

> Pergunta-se: Utilizar o computador de outra pessoa sem autorização configura invasão? Se houver violação indevida de mecanismo de segurança, como a senha por exemplo, pode-se dizer que sim, mas se a pretensa vítima esqueceu o computador ligado a resposta será negativa. De todo modo, o tipo penal me parece um pouco genérico.
> Somente haverá crime em caso de invasão de dispositivo (computador, periféricos, etc). Se o autor limitar-se a invadir um perfil de rede social, um e-mail, banco de dados ou um álbum de fotografias, sem passar pelo computador da vítima, não incidirá no crime em análise. Cuida-se de um erro crasso do legislador.

Para Milagres (2013)[10] a finalidade de obter dados é algo imensamente polêmico para alguns juristas, segundo ele, a simples espiada não seria problema, só se falando em obtenção no caso de cópias de dados dos dispositivos, ou quando o agente entra na posse de dados. Doravante, outra corrente defende que o simples acesso (um select na tabela da vítima) entraria de encontro ao bem jurídico protegido pelo Direito Penal, e demonstrando assim a intenção de obter dados eis que já permite ao "cracker", em certos eventos, vantagens das informações, portanto o contato com os dados já enquadraria perfeitamente no tipo penal que é obter dados.

Permanecendo na discussão Milagres (2013)[11] escreve:

> É o Judiciário quem vai interpretar esta questão, porém ao contrário do que alegam alguns advogados, não é necessário a cópia dos dados para a prática do crime, pois trata-se de crime formal e de perigo abstrato, diga-se, basta a invasão com a "intenção da obtenção dos dados". Tal fato poderá ser provado por perícia técnica.

E são diversos relatos negativos neste ponto, como Oliveira (2013)[12]:

---

[9] http://jus.com.br/artigos/23655/lei-carolina-dieckmann
[10] http://webinsider.com.br/2013/04/16/o-que-mudou-com-a-lei-carolina-dieckmann/
[11] *Ibidem*
[12] http://olivattack.blogspot.com.br/2013/04/falhas-na-lei-carolina-dieckmann.html

> Outro ponto, está ainda no art. 154-A. Existe um trecho do artigo que diz que será enquadrado na lei, quem violar o "mecanismo de segurança" do dispositivo informático alheio. Dessa forma, se o computador da vítima não tiver mecanismos de segurança (antivírus, firewall, proteção por senha, etc), o invasor poderá ficar impune.

Assim como Penido (2013)[13] segue a linha de pensamento:

> Outro ponto relevante levantado por especialistas, ainda com referência ao artigo 154-A seria a sua segunda parte:"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". "Adulterar ou destruir" não causam problemas de interpretação; já o verbo "obter" pode dar margem a dúvidas: a mera "espiadinha" em um sistema, entrando e saindo dele configuraria a obtenção de dados ou não? Há quem diga que sim e quem diga que não; na verdade somente a jurisprudência (conjunto de decisões dos Tribunais que formam a orientação na forma de interpretar a lei) irá solucionar essa dúvida com o passar do tempo.

Isto demonstrando os diversos problemas da terminologia pode causar em uma legislação, ainda mais nos tempos em que se vive uma democracia onde se proteja muito o réu contra a sociedade.

2.5 Capacidade para Investigação

E por fim acreditar que nossa polícia técnica, civil, totalmente sucateada terá condições hábeis de apurar os crimes cibernéticos e crer praticamente em fadas e duendes. Apenas algumas cidades possuem recursos tecnológicos para isto, mas em quase totalidade dos municípios brasileiros não haverá pessoal técnico capacitado para promover corretamente a apuração dos crimes e o mais provável que ocorra é que apenas quando envolver pessoas de grande renome e/ou que a mídia tenha interesse que se apure que poderá haver solução dos casos.

Colli (2010)[14] antes da existência da lei destacava que a definição do que é crime cometido na internet dificultava, pois por vezes condutas podem ser danosas mas não consideradas crimes e outro grande problema é a identificação dos criminosos, pois no mundo virtual o que se identifica são máquinas e números e não pessoas com seus documentos. E como máquinas e números podem ser usados por diversas pessoas, como em "*lan houses*" ou em uma casa que moram várias pessoas utilizando o mesmo computador, acaba dificultando ainda mais a localização do infrator. Pois há dificuldade em se fazer relação de máquina e

[13] http://www.tiespecialistas.com.br/2013/04/os-crimes-previstos-na-lei-carolina-dieckmann/
[14] http://www.adjorisc.com.br/jornais/folhadooeste/impressa/seguranca/cibercrimes-pesquisador-aponta-dificuldades-na-investigac-o-em-livro-1.580707#.Uk2-B9J6Ync

pessoa. E ainda há crime pela internet que envolvem diversos usuários em pontos distantes do país. Sendo assim a polícia técnica terá imensas dificuldades de apurar, além de seu poder, da sua jurisdição estadual e ainda por falta de recursos logísticos.

Gomes (2013)[15] ressalta neste liame que:

> Quem conhece minimamente o funcionamento da justiça criminal no Brasil não pode se iludir: ela está, em geral, sucateada. Porque sucateada está a polícia civil (investigativa), que conta com incontáveis cadáveres nas suas portas, o que já é suficiente para sugar todos os seus recursos materiais e pessoais. Medidas civis urgentes são mais eficazes nessa área. De qualquer modo, houve intenção de se suprir uma lacuna no Brasil.

E não é um problema apenas do Brasil, em publicação do site Linha Defensiva (2011)[16] traz relatório do Departamento de Justiça dos Estados Unidos em que se verificou a competência do FBI para investigação de crimes de tecnologia e observou-se que há problemas na capacitação de agentes e complementa:

> O relatório informa que 36% dos agentes envolvidos no combate ao cibercrime não têm qualquer experiência com os conceitos de informática e redes necessários para a realização desse tipo de trabalho. A política de rotatividade do FBI – que coloca agentes em variadas funções para aquisições de experiência diversificada – causa problemas no combate ao cibercrime, devido ao conhecimento especializado necessário.
> As agências envolvidas na investigação de crimes digitais também não compartilham suas informações, impedindo o trabalho em conjunto. De 36 agentes entrevistados, apenas 2 tinham completado o curso do FBI para especializar agentes em crime digital. Embora 18 tivessem uma graduação em tecnologia da informação, só 8 tinham experiência em administração de redes.

Em entrevista realizada pelo jornalista Pereira (2013)[17] Rogério Nogueira Meireles, destaca "Problema mais palpável é a falta de uma delegacia especializada em investigações cibernéticas."

3 Considerações Finais

Considerando que a sociedade acadêmica deve compreender a aplicabilidade da lei dentro do campo fático, é importante trazer as divergências da nova legislação, através de

[15] http://jus.com.br/artigos/23897/lei-carolina-dieckmann-e-sua-in-eficacia
[16] http://www.linhadefensiva.org/2011/05/relatorio-aponta-dificuldades-do-fbi-em-investigar-crimes-virtuais/
[17] http://diariocatarinense.clicrbs.com.br/sc/policia/noticia/2013/05/lei-melhora-combate-a-crimes-ciberneticos-mas-apresenta-deficiencias-4126522.html

falhas terminológicas que poderão a vir complicar e até inviabilizar a aplicabilidade da lei não caso concreto.

Nota-se que o texto precisa de revogação de certos pontos, como a finalidade da invasão, a necessidade de violação dos dispositivos de segurança para configurar o crime e ainda a insignificância da pena imposta, retificando assim o entendimento e punindo de maneira condizente com o delito, para que não reste dúvida no campo real e a sociedade possa realmente estar resguardada no mundo cibernético que vivemos.

Não apenas a mídia deve atuar na pressão ao Congresso, pois uma sociedade calada é culpada por todos os maus políticos que estão na gerência do país.

INITIAL ANALYSIS AND CRITICAL TO THE LAW 12.737/2012 - LAW CAROLINA DIECKMANN

Abstract

Law 12.737/12, known as Law Carolina Dieckmann brought the criminal sphere normalization for invasion of information on computers and other electronic equipment. Necessary to address this issue is for all members of the academic society or not, to behave in a cohesive manner and have knowledge and legal support. This article will present the major flaws like the terminology used in the law, the maximum penalty bland, poor police technique, aiming to discuss and report to citizens on that there is a law in their lines brought flaws that may hinder or even preclude the applicability for the intended purpose, ie, legal cybercrime. Methodological literature will be used worldwide web (internet) and books on the subject. The article discusses how the Brazilian press was able to successfully get through the pressure on Congress to make themselves instant responses against cybercrimes due to violation of virtual intimacy of actress Carolina Dieckmann, however the law was made, transact, voted promulgated and published, but eventually containing flaws in the legal text and the target of some critical points.

Keyword: Law 12.737/12. Law Carolina Dieckmann. Invasion of privacy.

Referências

ARAUJO, Marilene. A constituição francesa de 1958 e a liberdade de comunicação audiovisual e da internet. **Revista de Direito Constitucional e Internacional**, São Paulo: Revista dos Tribunais , v.19, n.75, p. 251-282, abr./jun. 2011.

BRASIL**.** Lei 12.737, 30 de novembro 2012. **Lei Carolina Dieckmann**. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 dez. 2013.

CASTRO, João Antônio Lima (Coord.). **Direito processual**: interpretação constitucional no estado democrático de direito. Belo Horizonte: PUC/Minas, 2010. 1016 p.

COAN, Emerson Ike. @ internet e o direito á privacidade na sociedade do imaginário. **Revista Ciencias Humanas**, Taubate: UNITAU, v.10, n.02, p. 91-97, jul./dez. 2004.

FLOR, Roberto. Perspectiva para os novos modelos de "investigação tecnologica" e proteção de direitos fundamentais na era da internet**.Revista Brasileira de Ciências Criminais**, São Paulo: Revista dos Tribunais, v.20, n.99, p. 69-100, nov./dez. 2012.

GOMES, Luiz Flávio. **Lei "Carolina Dieckmann" e sua (in)eficácia**. Disponível em: <http://jus.com.br/artigos/23897/lei-carolina-dieckmann-e-sua-in-eficacia>. Acesso em: 20 set. 2013.

GOUVÊA, Sandra**. O direito na era digital**: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. 164 p.

MAIA, Guto. **Lei Carolina Dieckmann só vale para eletrônicos com dispositivo de segurança.** Disponível em: < http://tecnologia.uol.com.br/noticias/redacao/2013/04/24/ lei-carolina-dieckmann-so-vale-para-eletronicos-com-sistema-de-seguranca.htm>. Acesso em: 01 set. 2013.

MILAGRES, José Antônio. **O que mudou com a Lei Carolina Dieckmann.** Disponível em: < http://webinsider.com.br/2013/04/16/o-que-mudou-com-a-lei-carolina-dieckmann/ >. Acesso em: 20 set. 2013.

MOURA, Pâmela Aline Rocha. **Crime cibernético e seus aspectos no universo jurídico**. Barbacena: [s.n.], 2012. 41 p. Trabalho Conclusão de Curso (Bacharelado em Direito)-Universidade Presidente Antônio Carlos. – UNIPAC, 2012.

NUCCI, Guilherme de Souza. **Código penal comentado**. 9.ed. São Paulo: Revista dos Tribunais, 2008. 1278 p.

OLIVEIRA, Willian César Pinto**. Lei Carolina Dieckmann.** Disponível em: <http://jus.com.br/artigos/23655/lei-carolina-dieckmann>. Acesso em: 10 set. 2013.

OLIVEIRA, J. **Falhas na Lei Carolina Dieckmann.** Disponível em: http://olivattack.blogspot.com.br/2013/04/falhas-na-lei-carolina-dieckmann.html>. Acesso em: 08 out. 2013.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000. 141 p.

PENIDO, Flávia. **OS crimes previstos na Lei Carolina Dieckmann.** Disponível em: <http://www.tiespecialistas.com.br/2013/04/os-crimes-previstos-na-lei-carolina-dieckmann/>. Acesso em: 08 out. 2013.

PEREIRA, Felipe. **Lei Melhora Combate a Crimes Cibernéticos, mas apresenta deficiências.** Disponível em:< http://diariocatarinense.clicrbs.com.br/sc/policia/noticia/ 2013/05/lei-melhora-combate-a-crimes-ciberneticos-mas-apresenta-deficiencias-4126522. html >. Acesso em: 08 out. 2013.

PINHO, Rodrigo César Rebello. **Teoria geral da Constituição e direitos fundamentais.** 10.ed. São Paulo: Saraiva, 2010. 7 245 p. v.1.

SOUZA, Sérgio Ricardo de. **Temas de direito processual penal constitucional aplicado**. Niterói: Impetus, 2006. 208 p.

TEOTÔNIO, Paulo José Freire; HORAGUTI, Flávia Castilhano. Pornografia e pedofilia na internet, prevenção e punição. **Revista Magister de Direito Penal e Processual Penal**, Porto Alegre: Magister, v.8, n.43, p. 10-35, ago./set 2011.

TOURINHO FILHO, Fernando da Costa. **Código de processo penal comentado:** (Arts. 1º a 393). 13.ed. rev. atual. São Paulo: Saraiva, 2010. v.1. 981 p.

VIEIRA, Vítor. **Lei Carolina Dieckmann enfrentará dificuldades na prática.** Disponível em:<http://www.conjur.com.br/2013-abr-03/aplicacao-lei-carolina-dieckmann-enfrentara-dificulda des-tribunais>. Acesso em: 21 set. 2013.