



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

ALOIR DE ARAÚJO FERNANDES

CRIMES NA INTERNET, LEI CAROLINA DIECKMANN E SUAS FALHAS.

BARBACENA
2015

Aloir de Araújo Fernandes

CRIMES NA INTERNET, LEI CAROLINA DIECKMANN E SUAS FALHAS.

Artigo Científico apresentado à
Universidade Presidente Antônio Carlos –
UNIPAC, como requisito parcial para
obtenção do grau de Bacharel em Direito.

Aprovado em: __ / __ / ____

BANCA EXAMINADORA

Prof. Esp. Rodrigo Corrêa de Miranda Varejão
Universidade Presidente Antônio Carlos – UNIPAC

Prof. Esp. Cristina Prezoti
Universidade Presidente Antônio Carlos – UNIPAC

Prof. Esp. Luiz Carlos Rocha de Paula
Universidade Presidente Antônio Carlos – UNIPAC

CRIMES NA INTERNET, LEI CAROLINA DIECKMANN E SUAS FALHAS.

Aloir de Araújo Fernandes *

Rodrigo Corrêa de Miranda Varejão **

Resumo

O mundo atual está cada vez mais globalizado e todos que tem acesso à rede mundial de computadores podem saber o que ocorre do outro lado do mundo, em poucos segundos. A informação não é mais privilégio de uma classe exclusiva dominante, atualmente quem está conectado à internet, pode saber de acontecimentos nacionais e internacionais em apenas poucos cliques. Entretanto assim como o meio cibernético trás inúmeras vantagens, há inúmeros riscos, e os criminosos aproveitando-se do aparente anonimato, vêm aplicando inúmeras fraudes à sociedade moderna, alguns golpes gigantescos, trazendo prejuízos de centenas de milhares de dólares, por exemplo. A Lei 12.737/12, popularmente conhecida como Lei Carolina Dieckmann, trouxe um avanço na tipificação de crimes ocorridos na internet, entretanto muitos doutrinadores a fazem críticas ferrenhas, visto que o legislador aparentemente introduziu alguns termos desnecessários e com ambiguidade, o que iremos analisar neste trabalho, desde o surgimento da internet, aos problemas no texto da referida lei. Irá se debruçar sobre a legislação ora mencionada, além de doutrinas, jurisprudências, e, sobretudo de artigos científicos da internet.

Palavra-chave: Lei Carolina Dieckmann. Falhas na lei. Crimes na internet.

1 Introdução

Este trabalho de revisão bibliográfica tem objeto fim de demonstrar aos cidadãos a importância da regulamentação dos crimes praticados na internet, com um olhar voltado ao direito e brechas que a atual legislação, mesmo recente, conseguiu trazer aos tribunais.

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

**Professor Orientador – Especialista em Direito Penal. Professor da Universidade Presidente Antônio Carlos. Email: rodsvare@hotmail.com

É de conhecimento geral que a internet conecta e deixa o mundo globalizado de forma imediata, que acontecimentos importantes em rincões longínquos são notificados de forma quase instantânea; pode-se estudar com cliques e pagar contas com os mesmo botões, mas a facilidade na vida do homem não é apenas para a boa utilização, há pessoas que utilização de toda esta receptividade do meio cibernético para praticar inúmeros ilícitos penais.

O corpo acadêmico, principalmente da área jurídica, tem o dever de conhecer a legislação vigente para poder de forma eficaz aplica-la para se defender ou proteger seus clientes para que não sejam acusados injustamente.

Irá se abordar a atual legislação apelidada de Lei Carolina Dieckmann e suas falhas, além de fatos que já provocaram prejuízos ao erário e algumas situações famosas no cotidiano.

2 Internet x Crimes

O meio cibernético oferece a ilusão ao usuário de que tudo pode ser feito sem interferência direta do mundo real, este no qual ao sair à rua pode ser motivo de roubo, atropelamento, confusões, agressões entre tantos outros problemas, mas a expectativa de um meio blindado de problemas cai por terra, ao computador, smartphone, ou outro meio eletrônico é invadido e todos os dados vão parar na mão de criminosos.

Cassanti (2015)¹ confirma este posicionamento, “Os crimes digitais são cada vez mais comuns porque as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem leis. A falta de denúncias também incentiva fortemente o crescimento dos números de golpes virtuais e violência digital (como o cyberbullying).”

2.1 Internet

A internet transformou-se ao longo de anos, em um dos meios mais utilizados de troca de informações, com inúmeras vantagens, desde a rapidez, até a facilidade atual em conseguir o sinal. Podendo ser vista como um meio necessário para se inserir globalmente, pois seu acervo é imenso e a maior parte do noticiário é publicado praticamente

¹ <http://www.crimespelainternet.com.br/o-que-sao-crimes-virtuais/>

instantaneamente pelos principais jornais e até televisões, e pela acessibilidade até uma criança hoje publica e compartilha informações no mundo digital.

Seus primórdios remetem à Segunda Guerra Mundial, onde se fazia necessária troca de informações criptografadas e que a espionagem tentava decifrá-las. Seu início se deu inicialmente, portanto no meio militar, e passou posteriormente para o meio científico e acadêmico.

Tait (2007)² reporta seu surgimento:

A internet nasceu em 1969, nos Estados Unidos, interligava originalmente laboratórios de pesquisas e se chamava ARPAnet (ARPA: Advanced Research Projects Agency). Era uma rede do Departamento de defesa norte-americano, no auge da guerra fria (era o nome dado à disputa entre EUA e a União Soviética).

O termo internet apenas foi utilizado em 1971 por Vinton Cerf, Kleina (2011)³ destaca que é realmente é o primeiro evento com destaque, pois em meados deste ano a equipe de Cerf, definidos como criadores, tentaram estabelecer conexão entre três redes distintas, a expressão em inglês inicialmente utilizada foi “*interneting*”, e ficou imortalizada como vocábulo internet abreviadamente.

Contudo uma verdadeira revolução ocorreu no ano de 1989, quando Tim Berners-Lee, na Suíça, cria uma nova forma de troca dos textos na rede, de forma mais dinâmica. O cientista criou o WWW, isto é, “Word Wide Web”. Barwinski (2009)⁴ assegura que “Este cientista também é responsável pelo desenvolvimento de duas ferramentas indispensáveis para a Internet: o código HTML e o protocolo HTTP.”

Na década de noventa a rede mundial vira moda e é disseminada.

No Brasil em 1987 na Universidade de São Paulo um grupo de pesquisadores, representantes do governo e das telecomunicações se reúnem para discutir uma rede brasileira com fins acadêmicos, ligando o Estado Nacional às outras redes estrangeiras. (TAIT, 2007)⁵ e transcreve:

² <http://www.din.uem.br/~tait/evolucao-internet.pdf>

³ <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>

⁴ <http://www.tecmundo.com.br/historia/1778-a-world-wide-web-completa-20-anos-conheca-como-ela-surgiu.htm>

⁵ <http://www.din.uem.br/~tait/evolucao-internet.pdf>

Em julho de 1990 é lançada a rede nacional de pesquisas (RNP), um projeto do Ministério da Educação, para gerenciar a rede da academia brasileira, até então dispersa em iniciativas isoladas. A RNP, em 1992, significou a primeira espinha dorsal conectada à Internet nas principais universidades e centros de pesquisas do país, além de algumas organizações não governamentais. Em 1994 começaram a funcionar os primeiros servidores web do Brasil e a ser testado o acesso discado com fins comerciais.

Continua afirmando que em 1995 foi liberado o uso comercial. Praticamente no ano em que a Microsoft criou a Internet Explorer, sistema operacional que gerenciaria o acesso à Internet, dois anos após ser criado o primeiro, Mosaic.

Em 2004 surge o Mozilla Firefox, com código aberto, isto é, todos poderiam ter acesso a sua linguagem de programação, e o sucesso foi tanto, que em 99 dias mais de 25 milhões de usuários o baixaram em suas máquinas. (KLEINA, 2011)⁶.

Da simples troca de mensagens e arquivos, a internet mudou seu conceito, hoje há troca de vídeos, imagens, além da famosa rede social.

2.1.1 Das Redes Sociais

Atualmente o mundo digital está tomado por redes sociais, isto é, um grupo de pessoas interage por sites que as agrupam.

O mais utilizado nos dias de hoje é o denominado “Facebook”, que veio a substituir o antigo “Orkut”. E como a internet não para de se desenvolver, os sites deram lugar aos aplicativos de celulares, onde por programas, o usuário conversa e compartilha arquivos por seus smartphones, tendo como aplicativo mais empregado o “Whatsapp”.

Mie (2015)⁷ destaca como o “Facebook” hoje vem sendo usado até por empresas:

Com mais de 1,3 bilhões de usuários ao redor do mundo, o Facebook é uma das maiores redes sociais de todos os tempos.

⁶ <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>

⁷ <http://www.oxygenweb.com.br/artigos/06-vantagens-facebook-para-empresas/>

Uma ferramenta de marketing perfeita para aqueles que desejam alcançar seu público-alvo, a plataforma 'Facebook para Agências' foi lançada e já é adepta de várias empresas.

Como todas as facilidades advindas do mundo cibernético a legislação foi se defasando e muitas violações a direitos dos usuários passaram a ser tomadas de forma geral pelo judiciário, quando era possível, e outras deixadas de ser aplicadas, por falta de legislação pertinente.

2.2 Crimes Notórios na Internet

Tendo inúmeros meios de acesso, o mundo virtual tornou-se um local prospero para pessoas cometerem crimes.

O maior prejuízo já relatado ocorreu entre os anos de 2005 a 2012 nos Estados Unidos, ondem invasores, conseguiram fraudar cartões de créditos causando um prejuízo com cifras de 300 milhões de dólares. A justiça americana acusou 5 homens do feito, sendo 4 de origem russa e 1 ucraniano.

O site G1 (2013)⁸ noticiou o ocorrido:

Cerca de 15 empresas e a bolsa eletrônica Nasdaq foram vítimas do grupo de hackers formado por quatro russos e um ucraniano com idades entre 26 e 32 anos. As invasões promovidas entre agosto de 2005 e julho de 2012 afetaram as empresas 7-Eleven, JCPenney, JetBlue e Dow Jones. (...)

Autoridades de New Jersey informaram que cada envolvido tinha uma especialidade: os russos Vladimir Drinkman, de 32 anos, e Alexandr Kalinin, de 26, invadiam redes de computadores, enquanto Roman Kotov, de 32 anos, explorava os dados das redes comprometidas. Eles acobertavam suas atividades em serviços de hospedagem on-line anônimos fornecidos pelo ucraniano Mikhail Rytikov, de 26 anos.

O quinto integrante do grupo, o russo Dmitriy Smilianets, de 29 anos, é acusado de vender os dados roubados e distribuir os lucros.

No ano de 2015 diversas prefeituras brasileiras passaram a ser alvo de invasores que via internet bloqueavam pagamento de servidores e exigiam dinheiro para destravar os sistemas municipais.

⁸ <http://g1.globo.com/tecnologia/noticia/2013/07/hackers-sao-acusados-em-maior-cibercrime-da-historia-nos-eua.html>

Exemplo disto ocorreu no Município de Pratânia/São Paulo, onde a prefeitura teve bloqueado seus sistemas e lhe foi exigida um depósito de 3 mil dólares. Apesar da perícia técnica, não foi possível a princípio se saber de onde vinha propriamente o bloqueio, apenas que sua origem era no Canada (AGÊNCIA NEWS 14, 2015)⁹.

O que ocorre também é que muitas vezes, o crime não é praticado com vulto, e sim de forma a denegrir a imagem de alguém, roubando-lhe fotos íntimas, e até mesmo dados pessoais.

No mês do corrente ano, o ator Stênio Garcia, ganhou as manchetes nacionais após ter divulgadas fotos íntimas com sua esposa. Até o presente momento não houve divulgação de acusados e informações pormenorizadas. Apenas que houve denuncia e que será investigado.

O caso brasileiro que gerou uma das maiores repercussões ocorreu em 2012 quando fotos da atriz Carolina Dieckmann foram divulgadas na internet.

3 Lei Carolina Dieckmann e suas Falhas

Em sete de maio do ano de 2012 fotos íntimas da atriz Carolina Dieckmann foram publicadas na internet, imagens que expunham em sua maioria sensualidade e nudez.

Inicialmente, no final de março houve contato de hackers através de e-mail com o empresário da atriz, fazendo um pedido de 10 mil reais para não divulgar as fotos. Entretanto não houve respostas e na data mencionada, no mundo virtual as fotos foram divulgadas inicialmente em dois sites eróticos.

A suspeita inicial era de que o computador formatado há dois meses, tivesse sido acessado pelos técnicos e retirado às fotos de lá, entretanto a investigação da Polícia Civil descobriu que através de um vírus, enviado no e-mail da atriz e acessado por ela, deu acesso aos criminosos às imagens. Agindo rápido os policiais utilizaram um programa e conseguiu rastrear os hackers através do número da IP de suas máquinas, que estavam localizados em São Paulo e Minas Gerais. Com a ação, os sites retiraram as fotos do ar e sites de buscas estão em negociação para evitar a publicação das mesmas.

⁹ <http://agencia14news.com.br/botucatu/hacker-invade-site-da-prefeitura-e-pede-3-mil-dolares-para-desbloquear-sistema/>

Um grupo especializado da Delegacia de Repressão aos Crimes de Informática (DRCI) da Polícia Civil do Rio usou programas de contraespionagem para chegar aos suspeitos. De acordo com a investigação, o roubo teria começado com um e-mail usado como isca (spam), que ao ser aberto liberou uma porta para a instalação de um programa que permitiu aos hackers entrarem no computador da atriz. (G1, 2012)¹⁰

Sem um crime específico para responderem, os réus responderam por extorsão, difamação e furto, o que ascendeu ao legislador ainda mais necessidade da criação de uma legislação específica para tipificar o crime.

Entretanto o poder legislativo pressionado pela mídia a fazer algo, elaborou e discutiu em pouco mais de 5(cinco) meses uma mudança no ordenamento jurídico, utilizando um projeto de lei do final do ano anterior.

Resultado, a Lei 12.737/12 foi promulgada e passou a vigorar a partir de 3 de abril do ano de 2013, com algumas falhas apontadas pelos setores jurídicos.

3.1 Lei Carolina Dieckmann

A Legislação entrou em vigor após 120 dias de sua publicação, com a determinação em seu artigo primeiro de que se tratava de tipificação dos crimes cibernéticos.

No artigo segundo definiu que acrescia ao artigo 154-A e 154B do código Penal, isto é, o Decreto-Lei nº 2.848 de 1940.

O artigo 154-A tipifica o crime de invasão de dispositivo informático, informando que penetrar em dispositivo informático de outrem, este estando ou não conectado á rede, sob violação de mecanismo de segurança, com a finalidade de ter, modificar ou extinguir dados, sem autorização do proprietário e ainda instalar dispositivo para tornar mais fácil este acesso para obter vantagem ilícita, haverá detenção de 3 meses a 1 ano, além de multa.

No parágrafo primeiro retoma que também comete a mesma infração se produzir, distribuir, oferecer, difundir ou vender programação para a prática do caput do artigo.

Já no parágrafo segundo descreve o aumento de pena de um sexto até um terço se do delito resultar perda econômica.

¹⁰ <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>

Alude o parágrafo terceiro se da invasão houve aquisição de objeto de comunicação eletrônica reservada, segredos da área comercial ou industrial, e informações sigilosas definidas em legislação, ou ainda controle remoto do meio invadido, haverá reclusão de 6 meses a dois anos, além de multa, salvo se o crime não for tipificado mais gravemente em outra legislação.

No quarto informa que se aumenta a pena do 3º, de um a dois terços se resultar divulgação, comercio ou transmissão à terceiro do que houve sido retirado do dispositivo.

No § 5º define o aumento de pena de um terço à metade se o crime for contra os representantes do poder executivo e legislativo, tanto na esfera Federal, Estadual ou Municipal; contra o Presidente do Supremo Tribunal Federal, e ainda diretor máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O artigo 154-B define a ação penal, que ocorrerá a partir de representação, salvo no caso do fato ter ocorrido contra a administração pública direta ou indireta de qualquer dos Poderes e esferas, e ainda contra as empresas representantes de serviços públicos.

O artigo terceiro faz acréscimo na redação dos artigos 266 e 298 e em seu parágrafo único define que cartão de crédito ou débito é equiparado a documento particular.

A lei 12.737/12:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

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.

(...)

“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.”

Art. 3º Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

(...) Falsificação de cartão

Parágrafo único. “Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial. (VADE MECUM, 2014)

3.2 Controvérsias da Nova Legislação

Com legislação recente o texto legislativo já entrou em vigor repleto de críticas, desde ao tempo de prisão até a capacidade da polícia técnica para investigar tais crimes.

3.2.1 Da Pena e a Certeza da Impunidade

Observa-se que o tempo proposto como sanção para a prática delituosa é deverás brando, pois sua pena máxima inicial é de até 1 (um) ano, o que resulta para réus primários, em sua maior parte, pagamento de cesta básica.

Ribas Júnior (2012)¹¹ reporta que o criminoso, não temendo que vá ser preso, não desistirá da prática, visto que dificilmente irá à cadeia:

Vê-se que o crime de invasão de computadores, punido com detenção de três meses a um ano em seu tipo básico, dificilmente levará o infrator à cadeia, salvo não seja ele réu primário ou detentor de bons antecedentes.

Assim, aliando-se o pouco ou nenhum receio de que venha a ser pego e punido, sabe o criminoso, que geralmente conhece bem as leis penais – sobretudo aquele que pratica o crime com habitualidade, caso de muitos hackers (naturalmente contam com bom nível intelectual e educacional), que na hipótese de vir a ser descoberto e se punido vier a ser, não chegará a ser condenado à prisão, eis que a pena do artigo 154-A do Código Penal é branda o bastante para assegurar ao faltoso o regime aberto de cumprimento de pena desde o início.

¹¹ <http://corporate.canaltech.com.br/coluna/juridico/Lei-Carolina-Dieckmann-e-o-sistema-penal-brasileiro/#comentarios>

3.2.2 O Verbo Invadir e Suas Definições

O termo Invadir apresentado na Lei 12.737, é alvo de ferrenhas críticas, visto que o seu significado alude à violência ou grave ameaça, e pouco se observa isto em crimes via internet.

Ocorre que raríssimas vezes os hackers agem sozinhos ou sem anuência das vítimas, ou terá acesso direto na máquina da pessoa, o que não é objeto direto da lei, ou quando o usuário acessa indevidamente algum aplicativo em seu e-mail ou pendrive, que terminará por instalar em sua máquina um programa que passará a fornecer ao criminoso os dados pretendidos, isto tudo ocorrendo sem nenhuma violência, e sim sob falsa percepção de segurança.

O Professor e advogado Sartori de Castro (2012)¹² permeia este pensamento:

(...) em nenhum de acesso remoto se pode dizer que o agente mal-intencionado agiu de modo violento para obter os dados do usuário. O que houve foi o emprego de artil. Para resumir o que se sucede nesses casos, acaba sendo o próprio usuário a permitir que seus dados sejam acessados.

Desta maneira, embora cotidianamente se noticiem invasões de determinado servidor e ou empresa por hackers que invadiram seus sistemas e acessaram informações indevidamente, o que se deve ter em mente é que isso só foi possível porque o próprio usuário assim o permitiu, ainda que por desconhecimento sobre o funcionamento do sistema computacional e por isso mesmo foi vítima de um artil.

Continua informando que a ilusão de que hackers invasores que quebram mecanismos de criptografia somem para ter acesso a uma única conta, é coisa de filme. Na realidade existem pessoas com más intenções que conseguem que o usuário termine lhe dando acesso a máquina, ou seja, não há acesso violento e muito menos com emprego de força.

Termina por concluir que uma simples troca terminológica, poderia corrigir o problema com o verbete invadir, ao se trocar por acessar, que acabaria por tipificar corretamente o acesso por “malwares” e terminaria com o problema.

Borges (2013)¹³ discorda deste entendimento, ao informar que o termo invadir deve ter um entendimento mais amplo, exemplificando que mesmo uma pessoa que deixa a porta

¹² <http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet>

aberta de sua casa, ao criminoso entrar, estará sim cometendo o crime de invasão de domicílio.

Invadir pressupõe a utilização de força, artimanha, violação indevido de mecanismo de segurança, desrespeito à vontade do proprietário do equipamento, ultrapassar o limite de autorização fornecida pelo titular do equipamento. É o tipo comissivo, em que o agente realiza a conduta proibida. Imagine uma situação em que você encosta a porta de sua casa, quem chega, não deve ir entrando só porque você não passou a fechadura, a violação do lar se configura do mesmo jeito.

Siena (2013)¹⁴ reforça este entendimento de que o verbo deverá ser entendido de modo que a pessoa entrou sem ter direito ou sem autorização, caso contrário o modo de execução da conduta tipificada seria incompatível com o real entendimento da palavra invadir, já que raríssimas vezes nos crimes cibernéticos irá se empregar força ou grave ameaça.

Nota-se que o legislador errou ao definir a conduta dessa forma, pois os que não criticam utilizam uma interpretação extensiva da lei, o que no modo de ver o direito penal, prejudica a sua execução.

3.2.3 Necessidade de Haver Dispositivo de Segurança

A violação só será válida se o meliante tiver que transpor um dispositivo de segurança, esta dicção do artigo, dificulta a aplicabilidade da lei, visto que como o verbo violar, nem sempre a pessoa mais leiga, e mesmo pessoas que entendem de informática, não necessariamente utilizam tais dispositivos.

O UOL (2013)¹⁵ alude que isto é uma celeuma legislativa, visto que diversos especialistas concordam que para haver o crime, o infrator deverá obrigatoriamente romper a barreira de segurança, o que por exemplo, impediria a punição de um colega de trabalho que acessa computador alheio, que está desbloqueado, e o rouba dados.

¹³ <http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal>

¹⁴ <http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>

¹⁵ <http://tecnologia.uol.com.br/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm>

E ainda corroborando neste entendimento Oliveira (2013)¹⁶ transcreveu:

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.

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.

E reforçando ainda o tema Penido (2013)¹⁷ diz que para alguns conhecedores, se não houve senha, antivírus, tela de bloqueio, com certeza não ocorrerá crime previsto no artigo 154-A e ainda:

Somado a isso, na vida corporativa, esse artigo pode causar transtornos entre os profissionais especializados em procurar vulnerabilidades em sistemas alheios visando solucionar ou evitar falhas de segurança, a depender de como se dá o trabalho do profissional e de como esteja redigido o contrato de prestação de serviços, prevendo a exclusão de eventual incidência criminosa nessas atividades.

3.2.4 Capacidade de Investigação

Os crimes tratados na Lei 12.737/12 são de difícil localização do autor, o que torna necessário uma polícia capacitada e com bons equipamentos para fazer o rastreamento do criminoso.

Entretanto no país, o poder de polícia investigadora, está totalmente sucateado por descaso dos governantes, e sem o apoio ficará muito difícil conseguir uma sentença favorável e localização do sujeito.

E reportando Gomes (2013) transcreve:

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.

¹⁶ <http://jus.com.br/artigos/23655/lei-carolina-dieckmann>

¹⁷ <http://www.tiespecialistas.com.br/2013/04/os-crimes-previstos-na-lei-carolina-dieckmann/>

Tavares (2013) reporta sobre o tema:

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.

Reforçando este entendimento o informativo Online Folha do Oeste (2010) afirma das dificuldades de localização dos criminosos:

Sobre os principais problemas para as investigações de crimes virtuais, Colli salienta que alguns pontos foram destacados durante os três anos de pesquisa, principalmente na definição de ‘o que é um crime cometido pela internet’. “Às vezes, algumas condutas podem ser danosas, mas não serem consideradas crimes. Outro grande problema ainda é a identificação dos criminosos, já que no meio virtual o que se identifica são máquinas e números, e não pessoas e seus documentos, por exemplo. Outro problema é que um computador pode ser utilizado por muitas pessoas, como nas lan houses, onde até mesmo em uma casa que moram diversas pessoas. A dificuldade está mesmo em fazer essa relação de máquina e pessoa, além da questão territorial, sendo envolvidas pessoas de diversas cidades, estados e países no crimes”, enaltece o advogado.

Considerações Finais

A Lei 12.737/12 trouxe inovação jurídica ao ordenamento pátrio, entretanto por má dicção também trouxe problemas em sua interpretação.

Face necessária alterações nela, para que passe a ter uma melhor interpretação e evite equívocos.

Apesar de mesmo antes dela, o direito penal já cobrir por volta de noventa e cinco por cento de todos os crimes cibernéticos praticados, ela veio sim como um marco para o direito brasileiro, e apesar dos seus problemas, trará uma melhor segurança jurídica para o acesso ao mundo globalizado.

ABSTRACT

Today's world is increasingly globalized and all that has access to the World Wide Web can know what is happening across the world in a few seconds. Information is no longer the privilege of a dominant unique class, who is currently connected to the Internet, you can find national and international events in just a few clicks. However as cyber half behind many advantages, there are numerous risks, and criminals taking advantage of the apparent anonymity, have applied numerous scams to modern society, some huge blows, causing losses of hundreds of thousands of dollars, for example. Law 12.737 / 12, popularly known as the Law Carolina Dieckmann, brought a breakthrough in the classification of crimes committed on the Internet, though many scholars to make critical fierce, as the legislator apparently introduced some unnecessary and ambiguous terms, which we will examine in this work, since the emergence of the Internet, the problems in the text of that law. Will focus on the legislation mentioned herein as well as doctrines, jurisprudence, and especially of scientific articles the internet.

Keywords: Law Carolina Dieckmann. Flaws in the law. Internet crimes.

Referências

Agência News 14. **Hacker invade site da Prefeitura e pede 3 mil dólares para desbloquear todo o sistema.** Disponível em: <<http://agencia14news.com.br/botucatu/hacker-invade-site-da-prefeitura-e-pede-3-mil-dolares-para-desbloquear-sistema/>>. Acesso em: 12 out. 2015.

BARWINSKI, Luísa. **A World Wide Web completa 20 anos, conheça como ela surgiu.** Disponível em: <<http://www.tecmundo.com.br/historia/1778-a-world-wide-web-completa-20-anos-conheca-como-ela-surgiu.htm>>. Acesso em: 04 out. 2015.

BRASIL. [Leis, decretos, etc...]. **Vade mecum:** Saraiva. 17.ed. São Paulo: Saraiva, 2014.

BORGES, Abimael. **Lei Carolina Dieckmann - Lei nº. 12.737/12, art. 154-a do Código Penal.** Disponível em: <<http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal>>. Acesso em: 24 out. 2015.

CASSANTI, Moisés de Oliveira. **O que são Crimes Virtuais?.** Disponível em: < <http://www.crimespelainternet.com.br/o-que-sao-crimes-virtuais/>>. Acesso em: 03 out.2015.

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

BRASIL. [Constituição, 1988]. **Constituição Federal.** 7.ed. atual e ampl. São Paulo: Revista dos Tribunais, 2002. 266 p.

FOLHA DO OESTE. **Ciber Crimes: pesquisador aponta dificuldades na investigação em livro.** Disponível em: < <http://www.folhadooeste.com.br/imprensa/seguranca/ciber-crimes-pesquisador-aponta-dificuldades-na-investigacao-em-livro-1.580707#.VirPkCvmjQx>>. Acesso em 24 out. 2015.

FLOR, Roberto. Perspectiva para os novos modelos de "investigação tecnológica" 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.

G1. **Hackers são acusados em maior cibercrime da história nos EUA.** Prejuízo com invasão e venda de cartões superou US\$ 300 milhões. Bolsa eletrônica Nasdaq e 15 empresas foram vítimas dos invasores. Disponível em: < <http://g1.globo.com/tecnologia/noticia/2013/07/hackers-sao-acusados-em-maior-cibercrime-da-historia-nos-eua.html>>. Acesso em: 12 out. 2015.

G1. **Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'.** Atriz deu entrevista a Patricia Poeta no Jornal Nacional desta segunda (14). Trinta e seis fotos pessoais dela foram publicadas na internet. Disponível em: <<http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>>. Acesso em 23 out. 2015.

GOMES, Luiz Flávio. **A (in)eficácia da Lei Carolina Dieckmann.** Disponível em: <<http://congressoemfoco.uol.com.br/noticias/a-ineficacia-da-lei-carolina-dieckmann/>>. Acesso em: 24 out. 2015.

KLEINA, Nilton. **A história da Internet: pré-década de 60 até anos 80 [infográfico].** Disponível em: < <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>>. Acesso em: 03 out. 2015.

MIE, About Karen. **06 Vantagens do Facebook para Empresas.** Disponível em: < <http://www.oxigenweb.com.br/artigos/06-vantagens-facebook-para-empresas/>>. Acesso em: 12 out. 2015.

OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann.** Disponível em: <<http://jus.com.br/artigos/23655/lei-carolina-dieckmann>>. Acesso em: 24 out. 2015.

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: 25 out. 2015.

PINHO, Rodrigo César Rebello. **Teoria geral da Constituição e direitos fundamentais.** 10.ed. São Paulo: Saraiva, 2010. 724 p. v.1.

SARTORI DE CASTRO, Luiz Augusto. **"Lei Carolina Dieckmann" seria a salvação da internet?.** Disponível em: < <http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao%20da+internet>>. Acesso em 24 out. 2015.

SIENA, David Pimentel Barbosa de. **Lei Carolina Dieckmann e a definição de “crimes virtuais”**. Disponível em: <<http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>>. Acesso em 24 out. 2015.

TAIT, Tânia Fátima Calvi. **Evolução da Internet: Do Início Secreto à Explosão Mundial**. Disponível em: <<http://www.din.uem.br/~tait/evolucao-internet.pdf>>. Acesso em: 03 out. 2015.

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.