UNIVERSIDADE TIRADENTES – UNIT

CURSO DE GRADUAÇÃO EM DIREITO

TRABALHO DE CONCLUSÃO DE CURSO – ARTIGO CIENTÍFICO

# CRIMES VIRTUAIS: Uma Breve Análise da Lei 12.737/12

Evelyn Cristine Andrade Campos

Grasielle Borges Vieira de Carvalho

Aracaju

2015

EVELYN CRISTINE ANDRADE CAMPOS

CRIMES VIRTUAIS: Uma Breve Análise da Lei 12.737/12

Trabalho de Conclusão de Curso – Artigo – Apresentado ao curo de Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em ___/___/____.

Banca Examinadora

---

Professor Orientador

Universidade Tiradentes

---

Professor Examinador

Universidade Tiradentes

---

Professor Examinador

Universidade Tiradentes

# CRIMES VIRTUAIS: Uma breve analise da lei 12.737/12.

Evelyn Cristine Andrade Campos[1]

**RESUMO:**

O presente trabalho tem como objetivo tratar a respeito dos crimes virtuais, como eles ocorrem e analisar a legislação brasileira vigente sobre o assunto. Também são explanado os tipos de criminosos do ramo virtual, segundo a visão de diversos doutrinadores, assim como sua classificação para o Direito Penal, compondo-se um quadro explicativo dos tipos de criminosos que assolam o mundo informático. Faz-se necessária uma critica ferrenha quanto á legislação vigente e seu contexto histórico e cultural.

Palavras-chave: Internet. Crimes virtuais. Lei 12.737/12. Cibercrimes. Delitos virtuais.

[1] Graduanda em Direito pela Universidade Tiradentes – UNIT. E-mail: evelyn_cac@hotmail.com

## 1. INTRODUÇÃO

O direito tem por obrigação tutelar os bens jurídicos relevantes para a sociedade e por consequência deve moldar-se a realidade social em que se encontra em um dado momento histórico- cultural. Com a revolução digital dos anos 90 e a disseminação da internet ao longo dos anos ate os dias atuais onde o indivíduo pode a todo o momento e em qualquer lugar se manter conectado a uma rede há de se entender que o direito deve acompanhar atentamente as transformações ocorridas por meio desta revolução e todo o desenrolar jurídico e social que este momento proporciona a sociedade.

São infinitos os benefícios que o avanço tecnológico trouxe para a vida cotidiana do cidadão comum, porém há também seus traços negativos. Com um novo mundo sendo descoberto no virtual a internet se tornou um campo propício para a prática de delitos.

Pouco se é comentado sobre os crimes virtuais, apesar de ser uma realidade em nossa sociedade. É importante que sejam realizados estudos sobre os crimes virtuais, pois, ainda há por uma grande parte da população a ideia de que a internet é “terra de ninguém”, um novo mundo onde não é necessário respeitar regras e onde os criminosos por possuir o elemento da anonimidade tem a falsa sensação de que não estão se expondo a riscos.

Não há no Brasil atualmente uma preocupação significativa sobre tal tema, apesar de já figurarmos como o 4º (quarto) país com maior número de vitimas virtuais. Em 2001 fora feita uma convenção internacional sobre o tema, porém a primeira lei redigida no Brasil sobre os crimes virtuais deu-se apenas em 2012 e a mesma ainda contem inúmeras falhas e lacunas.

A tipificação dos crimes virtuais feita pela Lei 12.737/12 é bastante superficial e apenas margeia o problema, talvez por falta de conhecimento técnico dos legisladores ou talvez por ter sido feita apenas como forma de mascarar o problema.

Ao longo do trabalho será realizado o estudo dos diversos conceitos existentes sobre o tema, assim como a classificação empreendida por estudiosos do assunto.

Faz-se também uma análise criminológica, tendo enfoque especial em determinados criminosos, quais sejam: *Hacker, Cracker, Carders e Cyberpunks.*

Por fim tem-se como foco principal, a análise critica da Lei 12.737/12 e no contexto em que esta fora aprovada. Provocando uma critica a determinados pontos da lei em que o legislador fora descuidado e ate mesmo omisso.

## 2. A INTERNET

A internet é usada por basicamente toda a população brasileira, pessoas de todas as faixas etárias e que possuem diversas finalidades na *web*, desde trabalhos escolares a compras de imóveis. Justamente por ter essa gama tão vasta de publico, e de conteúdo a internet é um lugar que desperta a atenção de criminosos, que por vezes se aproveitam da ingenuidade e curiosidade de suas vitimas.

Outro ponto que faz com que a rede seja um campo favorável ao crime é a fragilidade legislativa e o fato de ainda não existir muitos profissionais especializados e capacitados em tais casos. Não há muitos estudos e pesquisas sobre o ciberdelito, assim como também são parcos os projetos de leis em tramite no congresso nacional, apesar de existir um forte potencial para o ciberdelito, demonstrado pelo fato do Brasil configurar como o 4º (quarto) país com maior número de vitimas virtuais.

> A criação de um estudo profundo de todo o direito penal enviesado para o ciberdelito é necessária para a compreensão da nova criminalidade. É importante que os operadores do direito compreendam melhor as particularidades da parte geral e da parte especial do código penal – e muito especialmente suas falhas na punição e repressão dessa modalidade de delitos- para que se iniciem frentes de contenção desta modalidade criminosa, aprovações de bons projetos e para que as dúvidas hoje existentes possam ser sanadas. O principio da legalidade é uma garantia penal intransponível no país. Os magistrados são sabidamente submetidos à lei penal,

> obrigados a absolver quando em dúvida e proibidos de praticar analogias *in malam partem*. (SYDOW, 2015, p.25).

Por isso não é incomum observar um juiz se valendo de interpretações paralelas e fórmulas genéricas para conseguir penalizar o delito virtual as penas sejam medíocres e não adequadas ao potencial lesivo que o crime realmente oferece. Uma vez que, por falta de legislação especifica os magistrados se encontram de mãos atadas frente ao principio da proibição da analogia "*in malam partem*".

A sensação de proteção causada pelo anonimato garantido da internet é um fator também bastante contributivo para os crimes virtuais, tanto os criminosos quanto as vítimas possuem essa sensação. No caso do criminoso a sensação de segurança vem da relação impessoal e anônima que há na *web*, é como se houvesse uma mascara protegendo sua identidade. Já no caso da vitima esse mesmo anonimato trás uma sensação de proteção de seus dados e ações e quando ela se sente protegida acaba se portando com menos cuidado e atenção, perdendo cautela ao abrir e-mails de desconhecidos e clicar em links e anexos de procedência duvidosa.

> Se por um lado a tecnologia da aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade. (SYDOW, 2015. Pag.43)

No crime penal do "mundo real" o ofensor e sua vítima precisam, na maior parte dos casos, ter algum tipo de contato próximo, alguma forma de interação física. Em outros casos é comum um planejamento, como em um roubo de banco, por exemplo, onde há necessidade de visitas ao local e, portanto fazendo-se fisicamente capaz para as autoridades a prisão do criminoso no ato ou durante essa preparação.

Enquanto que no crime virtual a possibilidade de uma prisão por exemplo, na preparação é quase nula, visto que os ataques são feitos em sua maior parte de surpresa. A preparação para os crimes virtuais não podem ser

previstos com a facilidade que encontramos nos crimes fora da esfera cibernética.

Por isto, é cabível dizer que o crime no mundo real é passível de um combate muito mais eficiente, visto que o agente criminoso esta limitado no espaço físico. O crime real tem local preciso e a policia pode agir no local em que houve o fato jurídico.

## 3. CRIMES VIRTUAIS - Conceito e Classificação dos Crimes Virtuais.

Para que se tenha inicio o estudo dos crimes virtuais de forma aprofundada é necessário que se faça uma classificação, e ainda mais importante uma conceituação a cerca dos mesmos e dos bens jurídicos envolvidos.

Não há uma unanimidade quanto à nomenclatura utilizada pelos doutrinadores, sendo assim conhecido por diversas formas, tais como: “crimes virtuais”; “crimes cibernéticos”; “crimes da era da informação”; “cibercrimes”; “crimes eletrônicos”; “crimes digitais”; “crimes tecnológicos”; “crimes de internet”, entre outros.

Não havendo realmente uma grande diferenciação entre as terminologias utilizadas, apenas sendo algumas mais abrangentes que as outras.

Da mesma forma como não há com consenso com relação à nomenclatura, também não há um consenso com relação ao conceito, de acordo com a organização para cooperação e desenvolvimento econômico (OCDE) “considera-se abuso informático qualquer comportamento ilícito, aético ou não autorizado relacionado ao processamento automático e a transmissão de dados”.

Porém a definição da OCDE foi considerada vaga e logo vários doutrinadores apresentaram seus conceitos, um dos primeiros a propor tal conceito foi Klaus Tiedmann que conceituava o crime virtual como sendo

“Todos os atos antijurídicos, segundo a lei penal vigente, realizados com o emprego de um equipamento automático de processamento de dados.”.

Por sua vez Marcos Aurélio Rodrigues da Costa conceitua como “Todo aquele procedimento que, utilizando-se de um sistema de processamento de dados, atenta contra os dados que estejam armazenados, compilados, sejam transmissíveis ou em transmissão”.

Um conceito mais amplo pode ser encontrado nos ensinamentos de Rossini:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110).

De acordo com os conceitos gerados obtiveram-se as classificações para os crimes virtuais, mas que assim como os conceitos existe mais de uma forma de classificação para os delitos.

A classificação mais utilizada pelos doutrinados e mais facilmente encontrada em pesquisas sobre o tema é a classificação de Ivete Senise Ferreira, que os divide em crimes informáticos próprios e crimes informáticos impróprios.

Os crimes informáticos próprios são aqueles em que os bens jurídicos novos (ou que necessitam de adaptação legislativa) são o alvo de violação. Enquanto os impróprios são aqueles crimes cometidos pelo uso de ferramentas informáticas como forma de opção do criminoso, porem que não implicam novos raciocínios jurídico-penais.

Podemos usar como exemplo de crimes informáticos próprios a interceptação de comunicação informática ilegal, prevista no art. 10 da lei

9296/96, uma vez que a comunicação informática é um bem jurídico novo. E como Exemplos de crimes informáticos impróprios, a calúnia (art. 138 do CP Brasileiro), a difamação (art. 139 do CP Brasileiro), e a injúria (art. 140 do CP Brasileiro), todos podendo ser cometidos, por exemplo, com o envio de um e-mail, mas que não necessitam do meio virtual de forma especifica para que ocorra.

Porém apesar de ser a classificação mais utilizada, não é a única encontrada no mundo acadêmico, pois os crimes virtuais também podem ser classificados, de forma tripartida. Essa classificação possui apoio de alguns doutrinadores, como Aldemario Araujo Castro e Spencer Toth Sydow. Estes autores classificam os crimes virtuais em: puros, mistos ou comuns.

Nos crimes virtuais puros viola-se o meio informático em si, em seus elementos utilizando-se para isso exclusivamente do meio informático. Para melhor entendimento usamos o exemplo da inserção de um código no computador de um escritório, a partir de um notebook, capaz de impedir que os usuários acessem arquivos fundamentais para a criação de um produto.

Nos crimes virtuais mistos utiliza-se do meio informático como instrumento para atacar bem jurídico diverso do informático. Que seria o caso do envio de um e-mail com o intuito de ludibriar o seu receptor a depositar uma quantidade de dinheiro para ajudar uma instituição de caridade. O crime praticado neste caso é o de estelionato, porém o fraudulento opta pelo uso de sistemas de informática em vez de meio diverso.

Nos crimes virtuais comuns viola-se o meio informático em si, em seus elementos, fazendo o uso de ferramentas comuns. Que acontece, por exemplo, quando o criminoso faz uso de um martelo para destruir o disco rígido de um aparelho, um DVD que contem informações, ou até mesmo a própria maquina. Nesse caso se esta diante de um crime comum, onde o alvo é físico porem que indiretamente implica na violação de dados.

Essas classificações são importantes especialmente para um maior entendimento com relação aos tipos de criminosos, tendo em vista que para os

crimes denominados comuns não se faz necessário nenhum tipo de qualificação específica para o agente. Já nos casos dos crimes puros e mistos se pressupõe um certo perfil, com habilidades e conhecimentos técnicos por parte do agente. Saber o perfil de um cybercriminoso pode vir a ser de suma importância no momento das acareações de uma investigação.

No entanto tais classificações não possuem muita utilidade para a vida real, pois os crimes virtuais estão em constante modificação, sendo assim em geral de mais importância no sentido didático para um melhor entendimento dos pesquisadores e estudiosos do assunto.

## 3.1. Os Criminosos

No campo da criminologia há diversos debates sobre o perfil médio do criminoso virtual. Discute-se em primeiro plano o predomínio de criminosos jovens e do sexo masculino, o que pode ser explicado logicamente pelo fato de que os homens constituem a maior massa de usuários na internet, assim como é notório um maior interesse em tecnologias em geral por parte dos mesmos. Logo se pode afirmar que não apenas o sexo masculino figura como maioria no aspecto criminoso como maioria no aspecto de vitima.

Analisa-se também o poder aquisitivo necessário do criminoso virtual uma vez que, para se obter um computador de boa qualidade que tenha condições de suportar programas e softwares mais elaborados necessários para os crimes cometidos é preciso pagar uma valor muitas vezes abusivo. Apesar do país ter avançado significativamente nos últimos anos com relação à disseminação da tecnologia, ainda há uma boa parte da população brasileira que não possui condições financeiras para adquirir maquinas de valor expressivo.

Certo grau de instrução e educação também são de fundamental importância para o manuseio de tais programas, que em sua maioria é arquitetado em língua estrangeira, o que já se incorpora como outro causador de barreira para os menos afortunados em matéria de escolaridade, uma vez

que uma boa parte da população brasileira não possui a oportunidade de se aprofundar em uma segunda língua.

O crime virtual próprio pode ser por vezes assemelhado ao crime de colarinho branco, já que em ambos os casos há um número limitado de pessoas que possuem o conhecimento necessário para praticar tais crimes, em especial aqueles que envolvem programação no caso dos virtuais. Mas claro que há os crimes de cunho mais simplistas onde não é necessário possuir uma grande habilidade informática, que são os casos dos crimes impróprios, porém estes não são o enfoque deste artigo.

Além da ponderação acerca do perfil médio do criminoso, analisa- se também os diferentes tipos de criminosos que existem na rede, sendo os mais conhecidos denominados como os *Cracker*, os *Carders e Cyberpunks.*.

Em primeiro lugar é preciso esclarecer sobre os chamados *hackers. Hackers* são especialistas em informática que procuram defeitos nos sistemas operacionais e programas e quando os descobrem comunicam aos fabricantes ou publicam para interessados através de informativos periódicos ou grupos de discussão. Esses indivíduos geralmente fazem isto por mero prazer ou curiosidade, porém são constantemente mal vistos pela sociedade por serem divulgado erroneamente na mídia como agentes causadores de danos.

Os *crackers*, no entanto são os verdadeiros criminosos, assim como seu nome deixa transparecer , cracker vem do inglês crack (quebrar), estes possuem o claro interesse de invadir redes, roubar dados, quebrar sistemas de segurança, disseminando vírus com a intenção de sabotar para fins criminosos, geralmente agindo em grupo.

Os *Carders* são os criminosos que geralmente usufruem das técnicas descobertas pelos hackers e se especializam na criação de programas que geram ou roubam números de cartão de crédito para conseguir dinheiro ou ainda para roubar informações e praticar extorsão.

Há ainda os denominados *cyberpunks*, que desenvolvem vírus com a finalidade de sabotar redes de computadores e gerar o DoS (*denial of service*)

gerando a queda de sistemas de grandes provedores, impossibilitando o acesso de usuários e causando grandes prejuízos econômicos.

Superado os conceitos essenciais para o entendimento dos crimes informáticos, passemos para o ponto central do artigo. A crítica da lei 12.737/12.

## 4. LEI 12.737/12

Já há crimes abarcados pelo direito penal brasileiro que são os considerados crimes impróprios como já explanados previamente. Neste caso há um amplo entendimento de que não há uma necessidade de novas normas, uma vez que os casos deveram ser julgados da mesma forma que os crimes comuns.

Porém o que cabe discussão são os crimes próprios cujas condutas não se encontram tipificadas no sistema penal brasileiro.

Encontramos na legislação brasileira a lei 12.737/12 que necessita de contextualização para melhor entendimento. A lei que também é conhecida pelo apelido de “Lei Carolina Dieckman” foi aprovada no dia dois de abril de 2012 e é oriunda do Projeto de lei 2.793/11 apresentada pelo deputado Paulo Teixeira (PT/SP).

A lei carrega este apelido dado pela mídia por ter sido aprovada logo após o vazamento de fotos pessoais da atriz global, nas quais a mesma aparece completamente despida.

As fotos, que estavam no e-mail de Carolina, foram furtadas por um craker que disseminou as fotos na internet após a atriz se recusar a realizar o pagamento de cem mil reais que fora pedido a mesma.

Já havia há dois anos no ordenamento jurídico uma tentativa de aprovação de leis contra os crimes cibernéticos, porém com a grande

repercussão que houve em volta do acontecido a câmara se viu pressionada pela população a aprovar o projeto que há tempos se encontrava estático.

Uma das maiores críticas com relação à lei 12.737 encontra-se fundada justamente na forma acelerada com a qual esta fora sancionada, em busca de uma aprovação da sociedade.

Segundo o advogado criminalista Luiz Augusto Sartori de Castro embora as regras tratem de muitas condutas atentatórias contra diversos bens jurídicos que não possuíam tipificação penal, na pratica pecam pela qualidade técnica de sua redação. Ele aponta ainda ausência de definição de diversos termos técnicos inseridos na lei.

Demonstrado o contexto histórico – social, passemos agora a analisar de forma critica e pontual a letra da lei, que é composta de apenas quatro artigos e que possui implicações também na ordem processual.

O primeiro artigo da lei versa:

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

Porém o que podemos vislumbrar após o estudo de toda a lei é que de certo só fora realmente criada um delito de natureza virtual, e não múltiplos delitos como da a entender o primeiro artigo da lei. Uma vez que os outros três artigos apenas englobam situações que antes não poderiam gerar consequências penais pela inexistência de previsão legal e pela proibição de interpretação analógica *in malam partem*.

*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.*

Neste artigo fora criada o novo delito informático, que pode ser definido segundo os ensinamentos de Spencer Sydow como o Ingresso não autorizado de um usuário no sistema alheio, mesmo que este não tenha intenção de obter nenhum tipo de vantagem. Apesar de o nome intrusão remeter a ideia de violência e brutalidade não há necessariamente o uso de meios violentos ou ardilosos neste caso.

Porém qualquer que seja a forma de entrada no sistema informático alheio é necessário que haja um consentimento por parte do usuário, caso contrario entende-se que esta é uma ação a ser considerada abusiva sendo comparada por alguns doutrinadores com o crime de violação de domicilio.

Um ponto a ser debatido a respeito deste artigo esta na expressão “com o fim de...”, pois tem-se a ideia de que para que o crime seja realizado precise ter alguma finalidade específica, quando em verdade o mero ingresso desautorizado sem finalidade específica já deveria configurar na seara criminal, assim como no crime de violação de domicílio, onde o mero fato de adentrar a casa de outrem sem sua permissão é tipificado. Na forma como está escrito o artigo haverá o dever de se demonstrar a finalidade especifica do agente ao que se refere à violação, e as denuncias sem especificação do objetivo encontraram dificuldade em continuar, dificultando o trabalho dos investigadores.

*§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no* ***caput****.*

Neste primeiro paragráfo tem-se a ideia do participe do delito principal que pode ser defino como:

> O participe não pratica a conduta descrita pelo preceito primário da norma penal, mas realiza uma atividade secundaria que contribui, estimula ou favorece a execução da conduta proibida. Não realiza atividade propriamente executiva. (BITENCOURT. 2012, p.553)

*§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.*

Conclui-se que a causa de aumento de pena para casos de prejuízo econômicos são tanto para o autor quanto para o participe, posto que não há uma clara distinção no parágrafo.

*§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:*

*Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.*

No terceiro parágrafo encontramos a modalidade qualificadora, em que da invasão resultar a obtenção de conteúdo sigiloso. Onde há uma duplicação da pena do crime simples.

*§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.*

Causa de aumento do parágrafo terceiro para o caso de divulgação dos conteúdos sigilosos obtidos.

*§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:*

*I - Presidente da República, governadores e prefeitos;*

*II - Presidente do Supremo Tribunal Federal;*

*III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou*

*IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."*

Causa de aumento geral, tanto para o crime simples quanto para o qualificado em casos onde o crime for cometido contra personalidades dos altos cargos públicos, que merecem proteção especial por representarem instituições de suma importância para o país. Porém deve ressaltar que ficaram de fora deste rol taxativo algumas personalidades tão importantes quanto, como seria o caso de diplomatas e embaixadores que diversas vezes possuem informações privilegiadas sobre a economia e politica externa do país.

Algumas críticas devem ser expostas com relação a este artigo como um todo:

É clara a falta de preparo técnico do legislador ao redigir tal lei, uma vez que há por diversas vezes falta de definição de termos informáticos, como: dispositivos informáticos e mecanismos de segurança, deixando assim margem para diversas interpretações.

Outro ponto é que podemos concluir pela leitura do texto que a autorização do titular do dispositivo (expressa ou tácita) somente pode ser aplicada nos três primeiros núcleos do artigo (obter, adulterar e destruir), uma vez que o legislador optou por utilizar a palavra OU após as três primeiras condutas, separando a expressão "autorização do titular do dispositivo" da conduta de instalar vulnerabilidade para obter vantagem ilícita.

Deve também destacar a falta de um tópico importante na lei, que seria a revogação da permissão de acesso, uma vez que as permissões podem ser revogadas a qualquer momento bem como elas podem ter caráter limitado ou apenas de forma parcial. Neste caso deveria existir um paragrafo que coibisse a permanência de terceiro no caso de revogação de sua permanência.

Devemos tocar no ponto também sobre a vantagem ilícita mencionada no artigo, onde não há por parte do legislador uma definição de qual tipo de vantagem, pois por hermenêutica podemos considerar não apenas a vantagem patrimonial, mas também intelectual, a sexual entre tantas outras. A letra da lei deixa margem para uma vasta gama de interpretações.

Porém no caso da invasão de dispositivo informático com a finalidade de instalar vulnerabilidade para obter vantagem ilícita, devemos entender que apenas se trata de meio tipificado se o agente instalar vulnerabilidade no dispositivo alheio, causando assim uma limitação em sua aplicação.

Vejamos os ensinamentos de Spencer Toth:

> Nesse raciocínio, se alguém ingressa num computador aberto, vulnerável por si só porquanto em pagina em que consta escrita informação de cunho confidencial, e a partir disso obtém vantagem ilícita (obtém informações privilegiadas de qualquer natureza), mesmo assim não é delito da segunda figura da invasão de dispositivo informático. Isso porque não houve movimento positivo da instalação de vulnerabilidade. (SYDOW, 2015, p. 307)

***"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."*

Este artigo legisla sobre direito penal processual, pois define ação penal publica condicionada a representação nos casos de vitima comum e ação penal publica incondicionada nos casos de vitimas especiais tais como a administração publica citada no próprio artigo.

No que se refere ao tramite processual a critica a ser observada é que pela pena de grande parte dos casos não ser superior a dois anos, cumulada

ou não com multa o crime terá seu julgamento no juizado especial criminal que tem por pressuposto um julgamento célere e simplificado. Contudo, os crimes virtuais por conta da sua complexidade demandam de uma atenção e um tempo muito maior do que o juizado especial possa oferecer, visto que se faz necessária em muitos casos uma analise técnica minuciosa e trabalhosa, que poderá vir a ser sacrificada em detrimento da agilidade requisitada no procedimento sumaríssimo.

*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:*

***"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública***

*Art. 266. .....*

*§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.*

*§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)*

A mudança realizada pela lei no art. 266 do Código Penal teve a intenção de acrescentar no crime já previsto a interrupção ou perturbação de serviços informáticos, telemático ou de informação de utilidade publica.

Cabe ressaltar que a pena imposta no artigo é de detenção de um a três anos, e multa, porém o crime, que pode ser praticado por qualquer pessoa, tem como vitima a sociedade como um todo. Esta interrupção ou perturbação pode ser realidade de diversas formas, mas podemos visualizar a figura do ataque DoS, como sendo as mais utilizada pelos cibercriminosos.

> Os ataques DoS (sigla para **Denial of Service**), que podem ser interpretados como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que servidores tenham

> dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares[2], o autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de não conseguir dar conta delas. Em outras palavras, o computador fica tão sobrecarregado que *nega serviço*. (Revista Info Wester 2012)

Sendo assim os ataques DoS tem a capacidade de violar serviços que atualmente são considerados vitais para a sociedade, como por exemplo, ataques a grandes bancos impedem de que seus clientes possam fazer pagamentos na data correta gerando juros para estes, ou a impossibilidade de compra de uma passagem aérea para uma entrevista de trabalho, as possibilidades são infinitas.

Mais um ponto falho na normal é a falta de definição dos termos "informático" e "telemático", gerando uma norma penal em branco devido à expressão genérica e dúbia, pois não há no ordenamento jurídico uma definição especifica dos termos, devendo ser suprida por portaria do Ministério de Ciência e Tecnologia.

***"Falsificação de documento particular***

*Art. 298. .....*

***Falsificação de cartão***

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

Neste caso fora apenas acrescentado o paragrafo único ao artigo já existente, elevando o cartão de credito à classificação de documento particular após inúmeras discussões sobre a natureza do mesmo. Há quem acredite que o cartão de credito deveria ter sido acrescido no artigo 289 (Moeda falsa), visto que o cartão de credito poderia ser entendido como "dinheiro plástico", porém o

[2] Malwares: Abreviação de "*malicious software*" ou "programa malicioso", é o termo que representa códigos criados com intenções espúrias e/ou lesionadoras de arquivos e sistemas alheios.

legislador optou pelo entendimento de que o cartão de credito deveria ser considerado moeda, mas sim documento particular.

Somente a conduta de falsificar fora tipificada, logo ter a posse de um cartão clonado, não sendo o possuidor o responsável pela falsificação, ficara de fora do tipo penal.

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

Superada a analise da Lei vigente sobre cibercrimes no Brasil, cabe expor duas organizações virtuais de extrema importância tanto para o plano internacional quanto nacional, sejam elas a *WikiLeaks* e a *Anonymous*.

A *Wikileaks* é uma organização transnacional sem fins lucrativos, que fora fundada em 2006, possuindo sede estabelecida na Suécia e tem como objetivo divulgar informações consideradas confidenciais, mas que são de interesse publico. O principal membro do *Wikileaks* é o jornalista australiano Julian Assange que se tornou mundialmente famoso em 2010 quando se expos como face da organização no caso da divulgação de arquivos confidenciais dos Estados Unidos.

Nestes arquivos se encontravam diversas situações em que o país norte-americano violava de forma reiterada os direitos humanos, em especial nas guerras do travadas no oriente médio. Diversas empresas americanas manifestaram-se contra a organização, sendo assim tornando-se alvos de retalia por parte do *Wikileaks*, transformando-se em uma verdadeira ciberguerra.

Apesar de possuir diversos opositores a associação também possui diversos defensores em especial no mundo virtual, diversos *hackers* saíram em defesa do *Wikileaks* e a apoiaram, inclusive ajudando-os durante os ataques a empresas de cartões de credito como Visa e Mastercard, gerando um enorme quantitativo de prejuízo para as mesmas.

Além de defensores no mundo virtual, houve também a defesa por parte de alguns governos e meios tradicionais de informação, como por exemplo, o jornal The New York Times, considerado um dos mais importantes do mundo. O parlamentar da Noruega Snorre Valen acredita tanto na atuação da organização que a indicou para o Premio Nobel da Paz em 2011.

Na plano nacional podemos encontrar a atuação do grupo *Anonymous*, que se ato denominam como uma legião. O grupo que teve origem em 2004 representa o conceito de um cérebro global e existe em todo o mundo, não apenas no Brasil. Os próprios participantes não acreditam na denominação organização e nem na ideia de lideres.

Os participantes do grupo acreditam como o próprio nome sugere no anonimato de suas ações, no Brasil a ideia do *Anonymous* é similar a do *Wikileaks*, levar informações diretas e muitas vezes confidenciais a publico. A diferença básica entre as duas manifestações é a de que o anonymous brasileiro combate em primeiro plano a corrupção brasileira.

As diversas manifestações ocorridas no Brasil em junho de 2013 teve uma influencia direta de diversos grupos virtuais, tendo como um dos principais o grupo Anonymous que organizava grande parte das manifestações através das redes sociais.

Em 2012 o grupo fora noticia em todo país quando por meio de ataques do tipo DoS retirou do ar por quase um dia inteiro instituições bancarias como as empresas BMG, Citibank e PanAmericano, gerando um imenso prejuízo econômico como forma de chamar atenção para o grupo e suas atividades que objetivam o combate a qualquer forma de censura da internet.

## 5. CONSIDERAÇÕES FINAIS

O presente artigo teve como objetivo a critica pontual da legislação brasileira vigente, com enfoque especial na lei 12.737/12. Onde fica restada a conclusão de que apesar de demonstrar um avanço na direção correta para o

acompanhamento do problema social que o crime virtual tem criado, a lei ainda é superficial e falha.

Há na esfera nacional o conhecimento técnico necessário para o entendimento dos crimes estudados, porém o que se falta é a aplicação destes por meio dos intérpretes do direito na seara legislativa. Uma vez que estes não são especialistas no assunto, as leis acerca dos crimes informáticos deveriam ser elaboradas com o auxilio de especialistas qualificados.

Com o avanço da era tecnológica ocorre também o avanço na investida dos crimes virtuais, tanto próprios quanto impróprios, e que devem ser amplamente reprimidos pelo direito penal. Uma vez que este é um tipo de crime extremamente difícil de se combater, devido a amplitude presente no mundo cibernético e a forma como ele se modifica diariamente.

No artigo foi feito um breve levantamento também a cerca dos criminosos específicos dessa modalidade criminal e como podemos observar suas condutas dentro da esfera digital, pois para que se entenda o crime é de suma importância ter conhecimento sobre seus participantes, tanto vitimas quanto delinquentes.

Outra questão abordada foi a classificação destes crimes, pois assim como o entendimento dos elementos que participam deste é também imperativo que a comunidade jurídica esteja ciente de como podem ocorrer os crimes para que assim seja feito um estudo de como combate-los com maior eficácia.

No que tange as organizações citadas no trabalho, sejam elas: WikiLeaks e Anonymous, vale ressaltar que ambas são organizações que possuem como “sede” o mundo virtual, e que tem como claro objetivo a exposição de noticias e fatos que sem a internet seriam basicamente impossíveis de vir a ser conhecimento publico.

## REFERÊNCIAS


ALECRIM, Emerson. Ataque DoS (denial of service) e DDoS (distributed DoS). Disponível em: <http://www.infowester.com/ddos.php> Acesso em: 01/05/2015.

ALECRIM, Emerson. Ataques derrubam sites de vários bancos brasileiros. Disponível em: < http://www.infowester.com/noticias/ataques-derrubam-sites-de-varios-bancos-brasileiros/> Acesso 01/05/2015.

ANONYMOUS. Quem somos. Disponível em: <http://www.anonymousbrasil.com/sobre-anonymous/> Acesso em: 01/05/2015.

BITENCOURT, Cezar Roberto. Tratado de direito penal. São Paulo. Saraiva. 2012.

BRITO, Audriney. Análise da Lei 12.737/12 – “Lei Carolina Dieckmann”. Disponível em: <http://politicacidadaniaedignidade.blogspot.com.br/2013/04/analise-da-lei-1273712-lei-carolina.html> Acesso em: 01/05/2015.

COSTA, Marco Aurelio Rodrigues da. Crimes de informática. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826> Acesso em: 01/02/2015.

ESSE, Luiz Gustavo. Wikileaks e a primeira ciberguerra da história da humanidade – uma revolução ou apenas uma manifestação sufocada? Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=10718&revista_caderno=17> Acesso em: 01/05/2015.

FERREIRA, Ivette Senise. A criminalidade informática. In: Direito & internet: aspectos jurídicos relevantes, Bauru: Edipro 200.

MACEDO, Fausto. Juristas e criminalistas apontam falhas na lei Carolina Dieckmann. Disponível em: <http://politica.estadao.com.br/noticias/geral,juristas-e-criminalistas-apontam-falhas-na-lei-carolina-dieckmann,1016111> Acesso em: 01/05/2015.

NERY, David Cesar de Jesus. A importância do escritório sem papel na segurança da informação. Disponível em: <http://www.mbis.pucsp.br/monografias/Monografia_-_David_Cesar.pdf> Acesso em: 01/05/20115

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memorial jurídica, 2004.

SYDOW, Spencer Toth. Crimes informáticos e suas vitimas. São Paulo:Saraiva, 2015.

VALLE, James Della.Lei Carolina Dieckman entra em vigor nesta terça feira. Disponível em: <http://veja.abril.com.br/noticia/vida-digital/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/> Acesso em: 01/05/2015.

VIRTUAL CRIMES: A brief analysis of the law 12.737/12.

**ABSTRACT:**

The present work has as goal to talk about virtual crimes, how they happen and the current Brazilian legislation on it. It is also explained the criminals types of the virtual work according to various experts, as well as its classification for the doctrine, composing a explanatory list of criminal's types that exist in the informatics world. It's made necessary a tough critic about the current legislation and it's cultural and historic context.

Keywords: Internet. Virtual crimes. Law 12.737/12. Cyber crimes. Virtual offense.