**CENTRO UNIVERSITÁRIO**
**"ANTÔNIO EUFRÁSIO DE TOLEDO"**

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

# ANÁLISE JURÍDICA DA LEI 12.737/12

Lívia Peruque Ramos

Presidente Prudente/SP
2015

**CENTRO UNIVERSITÁRIO**
**"ANTÔNIO EUFRÁSIO DE TOLEDO"**

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

# ANÁLISE JURÍDICA DA LEI 12.737/12

Lívia Peruque Ramos

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do Grau de Bacharel em Direito, sob orientação do Prof. Ms. Antenor Ferreira Pavarina.

Presidente Prudente/SP
2015

Ramos,Lívia Peruque.
Analise Jurídica da Lei 12.737/12/ Lívia Peruque Ramos– Presidente Prudente: Centro Universitário Antônio Eufrásio de Toledo, 2015. 46f.

Monografia de conclusão de Curso de Direito – Centro Universitário Antônio Eufrásio de Toledo – Toledo: Presidente Prudente – SP, 2015.

1. Internet 2. Invasão indevida I. Título.

**ANÁLISE JURÍDICA DA LEI 12.737/12**

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

_____

Antenor Ferreira Pavarina

Orientador

_____

Cláudio José Palmas Sanchez

Examinador

_____

Ana Luísa Morabito

Examinadora

Presidente Prudente/SP, 27 de Outubro de 2015.

Dedico este trabalho á minha família e amigos.
Aos meus pais Wilson e Marinilda por todo apoio e compreensão, e principalmente por serem pais espetaculares, que nunca me deixaram desanimar e nem desistir dos meus sonhos. E ao meu irmão Bruno, que sempre foi a minha grande inspiração

Creio que soberano é somente o Direito, pela interpretação dos livres tribunais; que o povo soberano, ele próprio, é sujeito às delimitações das fórmulas legais.
Bastos Tigre

## AGRADECIMENTOS

Primeiramente gostaria de agradecer á Deus, que está sempre presente em minha vida, me abençoando e me guiando pelos melhores caminhos.

Aos meus pais, por proporcionarem essa oportunidade de cursar a faculdade de direito e também por todo amor e carinho que eles têm por mim.

Ao meu Orientador Antenor Pavarina, por toda a dedicação e tempo dispensados a mim, sem os quais seria impossível realizar o presente trabalho.

Aos amigos, por sempre estarem presentes em todos os momentos da minha vida, pelas trocas de experiências e companheirismo durante os anos de faculdade.

A todos, o meu muito obrigado!

## RESUMO

O presente trabalho aborda o surgimento dos crimes virtuais, fazendo primeiramente uma abordagem histórica. Analisando seu conceito, sua classificação e as principais tipificações presentes em nosso ordenamento jurídico. Ressaltando-se a Lei nº 12.737 que foi introduzida na legislação brasileira no dia 30 de Novembro de 2012, que dispõe sobre uma nova modalidade de crime, o de “Invasão de Dispositivo Informático”; lei esta que ganhou repercussão nacional em razão da atriz Carolina Dieckman, que foi vitima de invasão indevida de imagens privadas de seu sistema informático, e tal incidente influenciou o andamento do projeto de lei que tramitava, tornado mais célere a atualização do Código Penal em relação aos crimes de natureza virtual. Outro ponto a ser exposto, recairá sobre os benefícios e malefícios que tal lei trouxe ao ordenamento. E por fim, aborda também os procedimentos realizados na persecução criminal dos crimes de natureza virtual.



**Palavras–chave**: Lei Carolina Dieckmann; Internet; Invasão indevida; Dispositivo Informático; computador; vantagem ilícita.

## ABSTRACT

This present work going grapple the appearance cybercrime, making first one abordage history. Construe your concept, its classification and the essential typifications present in our planning juridical.
Pointing up the law nº 12.737 which was introduce at legislation brazilian in day 30 of November than 2012, that disposes about a new modality of crime, the " invasion decive computer ": law is that who won repercussion national because actress Carolina Dieckman, what was victim of invasion improper of pictures private of system computer, and it incident influenced the progress from the project law, making more fast the updating of criminal code in relation crimes virtual origin. Other point to stated, had fallen about the benefits ands harms that law bring forward planning. Lastly, address the procedures performed at prosecution criminal of crimes nature virtual.



**Keywords:** Law Carolina Dieckman, Internet, improper invasion, computing device, computer, unfair advantage.

**SUMÁRIO**

## 1 INTRODUÇÃO

O presente trabalho abordou em seu conteúdo através de pesquisas na internet, livros e artigos a evolução da internet e dos computadores, com foco na parte histórica de cada um deles até chegar aos problemas atuais causadas por consequência do uso de forma mal intencionada por algumas pessoas.

Também abordou sobre a visão do direito penal em relação á internet, juntamente com o posicionamento de alguns doutrinadores sobre tal assunto e das lacunas que ainda existem no nosso ordenamento jurídico mesmo com a criação da Lei n.º 12.737/12.

Foi abordado também sobre a importância que a internet tem na atualidade, desde quando ela era apenas utilizada para coisas mais simples, como por exemplo, enviar um e-mail, até a sua grande evolução.

Do mesmo modo, buscou esta pesquisa conceituar e classificar os crimes praticados através da internet, conhecido também popularmente por crimes virtuais. A necessidade de tal conceituação para saber se a conduta praticada pelo agente é punível ou não pelo Estado, e também a classificação doutrinaria que o crime praticado através da internet se encaixa.

O trabalho passou sobre os principais crimes praticados através da internet e sua falta de tipificação até chegar ao crime que deu de certa forma um empurrão para o surgimento da Lei n. 12.737/12, conhecida popularmente como Lei Carolina Dieckmann que é o principal assunto do presente trabalho.

Ademais, foi realizada uma analise jurídica profunda da Lei n.º 12.737/12, das mudanças que ela trouxe para a legislação brasileira e dos dispositivos penais como: o bem jurídico tutelado, os sujeitos, tipo subjetivo e objetivo, consumação e tentativa, concurso de agentes, aumente de pena por prejuízo econômico e formas qualificadas.

Também, foi feita uma analise da persecução criminal e toda sua estrutura, bem como a existência de delegacias especializadas, o funcionamento da denúncia, da investigação, dificuldade para a obtenção de provas, competência, ação penal e o procedimento a ser realizado.

Ao final, foi realizada uma analise sobre todos os aspectos positivos e negativos a luz de grandes juristas e criminalistas especializados no assunto, todo beneficio que ele traz para o atual direito penal brasileiro, e de certa forma, no que

ela poderia ser melhor.

Finalmente, foi feita uma conclusão, analisando a lei, os benefícios que ela trouxe a sociedade brasileira e o mais importante, a segurança jurídica aos usuários da internet.

Em suma, estes foram os principais tópicos tratados na respectiva monografia.

# 2 EVOLUÇÃO HISTÓRICA

O presente capítulo traz em seu corpo um breve histórico dos computadores e da Internet, desde o seu surgimento até os dias atuais. Também se fala sobre a relação do direito penal com a Internet, e qual a importância dela para nossa sociedade atual.

## 2.1 Breve Histórico Sobre Computadores

O surgimento do computador teve grande influencia dos primitivos egípcios e gregos, que se utilizavam de pedras para realizar a conta de seus animais. A palavra computador vem do latim *computatore* que significa “aquele que calcula”.

Por volta de 1822, Charles Babbage criou a “Maquina das diferenças” que calculava tabelas, e no ano de 1833 criou também a “Maquina analítica”, que era programada de varias formas diferentes. Por essas criações ele é considerado o pai do computador. Mas somente no final da década de 30 que se aumentou a necessidade de cálculos por conta da II Segunda Guerra Mundial, sendo usado como base a eletromecânica.

Em 1946, John W. Mauchly e John Presper Ecket nos EUA construíram um computador eletrônico de grande porte que foi nomeado de ENIAC – Eletronic Numerical Integrator and Computer que pesava 30 toneladas e medindo 140m² .

Ao passar dos tempos, novas gerações surgiram e Rosa (2002, p. 26/27) salienta sobre as quatro gerações:

> O computador ENIAC deu partida a uma série de gerações de computadores construídos com base em válvulas. Essa geração de máquinas sobreviveu entre os anos de 1946 até 1958. Assim, a International Business Machine – IBM, lança seu primeiro computador eletrônico, o IBM 701. A Siemens, na Alemanha, em 1958, lança o Siemens 2.002, enquanto a IBM nesse mesmo ano lança o IBM 1.401.
> A segunda geração de computadores de computadores caracterizava-se pelo uso de uma novidade tecnológica: os transistores. Cem vezes mais rápidos e confiáveis que as válvulas, os transistores desenvolvidos nos laboratórios Bell da ATT foram criados em 1948, passando a ser utilizados comercialmente nos computadores de 1959. Essa geração se desenvolveu entre os anos de 1959 e 1965, caracterizando-se pela redução surpreendente nas dimensões dos computadores, tornando-se mais confiáveis, mais rápidos e com menor consumo de energia. Foi na segunda

> geração também surgiu o software e as primeiras linguagens de alto nível e também os primeiros sistemas operacionais.
> A terceira geração também advém de uma novidade tecnológica: os circuitos integrados inventados em 1958. Como a fabricação de circuitos integrados era uma tecnologia cara, sua utilização nos computadores só foi possível como o advento do programa espacial da NASA que, com suas necessidades especificas e encomendas maciças, viabilizou comercialmente a adoção dessa tecnologia. Essa técnica permitiu adicionar numa minúscula pastilha (chip) de silício, inúmeros componentes eletrônicos,o que contribui para a sensível redução das dimensões dos computadores, favorecendo o aparecimento dos microcomputadores. Essa geração se desenvolveu até 1971.
> O que caracterizou a quarta geração dos computadores foi o avanço da fabricação de circuitos integrados (CIs). De inicio, surgiu a Integração em Larga Escala – (Large Scale Integrator – LSI), que conseguiu integrar alguns milhares de transistores em um único chip. A fase seguinte, a quarta geração, (chamada Very Large Scale Integator – VLSI, em 1980), permitiu acondicionar centenas de milhares de transistores, após qual surgiu em um único chip. Surgiram, assim os supercondutores e com eles as memórias (Red and Memorize – RAM e Read Memory – ROM).

Na década de 80 surge a quinta geração e até os dias atuais houve muitas evoluções e a tendência é que se evolua cada vez mais.

## 2.2 Breve Histórico Sobre a Internet

O inicio da internet se deu na década de 50, devido ao primeiro satélite espacial que a União Soviética colocou em orbita, Sputnik. Alguns meses depois o presidente americano na época anunciou a criação da ARPA – *Advanced Research Projects Agency*, que foi desenvolvida para missões de tecnologia para as forças armadas.

Na década de 60 o departamento de defesa dos EUA deu inicio a uma pesquisa com a intenção que se eles viessem a sofrer ataques à rede ainda permaneceria ativa, pois seria de grande dificuldade chegar até ao sistema principal.

Já na década de 90 o primeiro provedor de acesso comercial, World, permitiu que todos tivessem acesso a rede e a partir disso surgiram vários provedores tornando cada vez maior a utilização da internet.

Desde então, a evolução não para e a cada dia surgi uma tecnologia diferente, nos tornando cada vez mais vulneráveis, pois hoje em dia tudo está disponível na internet, tanto os dados privados como os públicos.

## 2.3 Direito Penal e a Internet

Com o aumento do uso da internet em grande escala , estamos diante do surgimento de uma nova forma de sociedade. Sendo esta uma sociedade solitária, que vive atrás de um computador, mas esquece de viver; e, em vez de utiliza-la de forma benéfica, e facilitar a vida, tem sido constantemente utilizada para a prática do mal.

Consoante com Rosa (2002, p. 47):

> Hoje, o ciberespaço tem muito em comum com o velho oeste do século XIX. É vasto, não- mapeado, cultural, legalmente ambíguo e verbalmente canhestro, difícil de acessar e aberto á predação. Grandes instituições reclamam que possuem o lugar, mas a maioria dos nativos são solitários e independentes, as vezes ao ponto da sociopatia. É evidente, um viveiro perfeito para 'foras – da –lei' e para novas ideias acerca da liberdade.

De acordo com essas palavras, o que podemos notar é o retrocesso de algumas pessoas em relação ao mundo virtual, pois o homem vem se desfazendo do convívio social para se tornar solitário, conviver em um mundo que não existe, e para o Direto é uma grande e assustadora novidade.

Conforme o que pensa Rosa (2002, p.48):

> É de inteira necessidade a criação de normas que possam regular as condutas praticadas pela Internet para coibir as ações inescrupulosas dos 'fora-da-lei' cibernéticos, tais como as leis que coíbem os criminosos convencionais na sociedade.

Ressalte-se que as lacunas em nosso ordenamento, que ocorrem devido à escassa tipificação em relação aos crimes praticados por meio virtual, contribuem para que direitos sejam violados.

Entretanto, a aplicação da lei penal em casos de crimes virtuais pode sim em alguns casos ser compatíveis com as existentes, pois,o que diferencia do delito normal é o meio em que ele é praticado. Um exemplo seria o crime de estelionato que esta prevista no artigo 171 do Código Penal, que frequentemente é praticado através da Internet.

O que podemos encontrar atualmente na nossa legislação é a Lei nº. 12.737/12 conhecida popularmente com a Lei Carolina Dieckmann, que tipifica apenas a invasão de dispositivo informático mediante adulterar ou destruir dados sem autorização expressa ou tacita ou instalar vulnerabilidades para obtenção de vantagem ilícita, deixando assim uma grande lacuna em relação á outros crimes que

podem ser praticados através da Internet, como por exemplo, a pornografia/pedofilia infantil, que teve um aumento significante durante os últimos anos.

Mas também existem situações em que causam grande dor de cabeça ao operador do direito, como por exemplo, no caso do e-mail, que está muito presente em nosso dia a dia, onde fica difícil estabelecer qual o limite da privacidade de cada um.

Cabe salientar que não só no direito penal que a internet esta presente, mas também no Direito Civil quanto ao comercio eletrônico, e o mesmo regramento para o comercio eletrônico se encontra no Código de Defesa do consumidor em relação às publicidades e propagandas feitas através da internet.

Outro ramo que a internet está muito presente é no Processo Civil em especial aos casos de penhora online, onde o juízo de execução informa ao Banco Central a determinação de bloqueio de aplicações financeiras do executado. Sem contar com a existência dos chamados processos virtuais que existem em grande escala no Juizado Especial Federal.

Sendo assim, é visível que a Internet vem tomando cada vez mais espaço no direito brasileiro e em todas as suas áreas.

## 2.4 A Importância da Internet na Atualidade

A Internet mudou muito com o passar dos anos. No começo dos anos 2000 encontrávamos conteúdo escasso. Mas com o passar dos anos e com o aumento de sua acessibilidade, ela passou a ser de grande ajuda tanto para crianças com trabalhos escolares, quanto para adultos para resolver problemas ligados ao emprego ou até mesmo arrumar um encontro amoroso.

O modo de agir, pensar, interagir e até comprar mudou muito por conta da Internet, pois ao contrario do que muitos pensam, a Internet tornou as pessoas mais sociáveis, aproximando quem estava distante e possibilitando fazer novas amizades, procurar emprego, movimentações bancarias e etc.

Todavia, além dos benefícios que a internet traz para seus usuários, tem contribuído também para o surgimento de novos tipos de criminosos, como por exemplo, os “hackers”. Assim, dando a oportunidade para outros criminosos se utilizarem da Internet para a pratica de delitos, bem como estelionatos, ameaças, tráfico de entorpecentes, pedofilia, pornografia infantil e etc.

No entanto, não podemos esquecer a sua importância, não se pode imaginar os dias atuais sem a agilidade e o conforto que os meios virtuais proporcionam a nós. É preciso saber utilizar de forma saudável, com limites e evitar ao máximo a exposição da vida pessoal, pois são de momentos publicados em redes sociais, mensagens compartilhadas e entre inúmeras coisas possíveis de se fazer através da internet, que pessoas de má índole se aproveitam para cometer crimes.

# 3 CONCEITO E CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

O presente capitulo traz a conceituação de crime virtual e sua necessidade de ser conceituado pelo direito para verificar se a conduta praticada pelo agente é ou não punida pelo Estado.

Se fala também sobre a classificação que poucos doutrinadores na atualidade fazem.

## 3.1 Conceito de Crime Virtual

A necessidade em se conceituar um crime decorre em avaliar se aquela conduta praticada pelo agente pode ou não ser punido pelo Estado.

Não podemos falar em prova nos crimes virtuais sem antes verificar se a conduta do agente se encaixa nos tipos penais, se está presente à culpabilidade na ação delitiva.

A denominação do delito é bem diversificada, sendo conhecido também como cibercrimes, crimes de Internet, crimes de informática, crimes eletrônicos, contudo, todos se referem ao mesmo ilícito penal.

Vários autores buscam conceituar esse tipo de delito, como por exemplo, Fabrizio Rosa (2002, p. 54/55), que denomina diverso conceitos, chegando ás presentes conclusões:

> 1. A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar;
> 2. O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão;
> 3. Assim, o ‘Crime de Informática’ pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los;
> 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Sergio Marcos Roque conceitua crime de informática como toda conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para sua perpetração ou consistir em seu objetivo material (2007, p.25 ).

Ou seja, é de extrema importância que esta conceituação seja feita de forma correta, para assim o Estado ter um aparo legal sobre aquilo que ele deve punir ou não.

### 3.2 Classificação

Poucos doutrinadores fazem distinção dos crimes de informática, porém Carla Rodrigues de Castro (2003, p.10) os classifica como crimes de informática próprios e impróprios. Vejamos:

> Os primeiros são aqueles que só podem ser praticados através da informática, sem ela é impossível a execução e consumação da infração. Na verdade os crimes de informática próprios surgiram com a evolução desta Ciência, são tipos novos, que agridem a informática como bem juridicamente protegido. Daí porque, em face da escassa legislação existente, alguns fatos são atípicos e, portanto, não podem ser punidos.

Em relação aos impróprios, Carla Rodrigues (2003, p. 10) diz que:

> São os que podem ser praticados de qualquer forma, inclusive através da informática. Assim, o agente, para cometer o delito, utiliza, eventualmente, o sistema informático. O computador é um meio, um instrumento para a execução do crime. São delitos que violam bens já protegidos por nossa legislação, como o patrimônio, a honra etc. Exemplo: ameaça, estelionato, calúnia.

Além disso, existe outra classificação para esse tipo de crime, que foi elaborada por Marco Aurélio Rodrigues de Costa[1], que os classifica quanto ao seu objetivo material em crime de informática comum, puro e misto. Vejamos:

> Crime de Informática Comum: São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

[1] Disponível em http://jus.com.br/artigos/1826/crimes-de-informatica/3#ixzz3nsyi6Ra0. Acesso em: 01 set 2015.

> Crime informática puro: São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.
> Crime de Informática Misto: São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

Outra classificação importante seria a tripartite do advogado Aldemário Araujo Castro[2], dividida em:

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

Também podemos classifica-los de acordo com a estação. Se a estação for próxima, uma rede interna, ou se a estação é remota, como a Internet.

### 3.3 Principais Crimes e suas Tipificações

São inúmeros os tipos de crimes possíveis de se praticar através de um computador que tem acesso a Internet, porém a maior dificuldade no nosso ordenamento jurídico atual é a tipificação desses crimes, pois não possuímos leis suficientes para regulamenta-los.

A seguir serão abordados de uma forma geral os crimes mais praticados, e também o crime que deu ensejo a Lei n.º 12.373/12, conhecida popularmente como “Lei Carolina Dieckmann”.

#### 3.3.1 Crime de veiculação de pornografia através da internet.

A tipificação desse crime consiste em dois tipos de conduta que são: oferecer serviço e/ou oferecer informações de caráter pornográfico através da Internet.

---

[2] Disponível em http://www.aldemario.adv.br/infojur/conteudo18texto.htm. Acesso em: 14 ago 2015

Atualmente, houve uma alteração feita pela ECA – Estatuto da Criança e do Adolescente, pela Lei n.º 11.829/08, que em seu artigo 247 até o artigo 247 – E, que regulamentam sobre a pornografia de crianças e adolescentes.

Os artigos acrescentados pela lei tipificam condutas como: “oferecer, trocar, disponibilizar, transmitir, distribuir, publicar, divulgar, adquirir, possuir ou armazenar” vídeos ou imagens de caráter pornográfico que envolvam crianças e adolescentes.

Note-se a abrangência do texto normativo, que dispõe “por qualquer meio, inclusive por meio de sistema de informática ou telemático” (artigo 241-A “caput”, ECA).

Essa norma disposta no Estatuto da Criança e do Adolescente possui um caráter específico, aplicada em casos envolvendo crianças e adolescentes, não abrangendo assim, os demais casos corriqueiros do mundo atual.

### 3.3.2 Espionagem e sabotagem informática

Configura-se espionagem informática a alteração de programas e pela troca de peças, modificando a programação original, e facilitando de certa forma o acesso a dados e registros de todo um computador.

Sendo assim, ocorre o acesso á computadores de forma intencional e não justificada por pessoas que não estão autorizadas pelo proprietário ou operador do computador, configurando um ato sujeito a ser punido pelo Estado.

Já a sabotagem informática tem como elemento objetivo, a destruição ou dano de material ou componente pertencente a um computador. O objetivo da sabotagem são os danos físicos e lógicos, visando inutilizar informações e dados valiosos contidas no computador de alguém.

### 3.3.3 Pirataria

Pirataria consiste na distribuição/venda de produtos sem a autorização dos autores/ proprietários de um produto ou marca, não pagando seus devidos direitos autorais. Atualmente são vários tipos de produtos pirateados, como eletrônicos, bebidas, roupas, cd’s e dvd’s.

Neste caso, iremos falar sobre a pirataria virtual, ou seja, a pirataria de musicas em diversos formatos e extensões, software e filmes.

A pirataria de software consiste em distribuir ou vender programas de computador sem a autorização do proprietário, não pagando os direitos autorais devidos. Essa conduta é tipificada pela Lei n.º 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programas de computadores.

Outro tipo de pirataria que causa muita polemica na atualidade, é a de transferência de musicas através da internet, porém, após 02 de agosto de 2003, essa tipificação começou a ser regulada pela Lei n.º 10.695/93 que alterou os artigos 184 e 186 do Código Penal e acrescentou parágrafos no artigo 525 do Código de Processo Penal.

### 3.3.4 Crimes contra a honra

A calúnia, segundo o artigo 138 do Código Penal seria o ato de imputar a alguém falsamente fato definido como crime.

O agente sabe tem conhecimento que o crime é falso, mas mesmo assim o divulga, tornando de conhecimento público. No caso do contexto virtual, o compartilhamento em redes sociais pode ser considerado uma forma de divulgação do ato.

A difamação encontra-se tipificada no artigo 139 do Código Penal que diz: “difamar alguém, imputando-lhe como fato ofensivo á sua reputação”. Trazendo para o contexto virtual, seria o ato de ofender a reputação de alguém e levar ao conhecimento do público tal ofensa, seria o conhecido “falar mal”.

Já a injúria está prevista no artigo 140 do Código Penal e traz em sua redação: “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro”, porém para se concretizar a injúria não é necessário levar a conhecimento de terceiros, o simples fato da vitíma se sentir ofendida interiormente, já caracteriza o crime de injúria.

Esses crimes podem ser executados de diversas formas, tanto pessoalmente, como através dos meios de informações, como: imprensa, radio, televisão e internet. Porém essas condutas ofensivas são praticas através da internet, dependendo o mesmo utilizado, o tipo pode ser aplicado a Lei n.º 5. 250/67, conhecida popularmente como a Lei de Imprensa, pelo vigente Código Penal Brasileiro.

### 3.3.5 Estelionato e fraude

O estelionato é conhecido pelo artigo 171 do Código Penal, que consiste em obtenção de vantagem ilícita, para si ou para outrem, induzindo ou mantendo a vitíma em erro, mediante meio ardil, ou meio fraudulento.

Remy Gama Silva (2000, p. 8), descreve alguns exemplos:

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

Ressalta-se que para haver estelionato nos casos acima expostos é necessário o elemento “prejuízo alheio”.

### 3.3.6 Tráfico de drogas

O trafico de drogas encontrou um espaço muito eficaz no mundo da Internet. Sites como Silk Road e Atlantics funcionam na Deep Web, ou Web profunda, um portal onde o Google não consegue ter acesso. Essas redes vendem desde produtos contrabandeados, remédios sem receitas, drogas, até mulheres e desafiam a policia com o tipo de criptografia aplicada em seus meios eletrônicos de pagamento, cujo faturamento desses portais ilícitos chega a 22 milhões de dólares por ano.

Essas redes funcionam como uma espécie de conveniência virtual, onde expõem seus produtos e formas de pagamentos, e assim a pessoa escolhe o produto desejado e realiza a compra sem precisar sair do conforto de sua casa, e sendo possível realizar o pagamento dividido em prestações no cartão de credito. Os produtos são entregues através do correio e ultimamente tem sido a febre da Internet.

Essa modalidade de trafico de drogas vem crescendo muito no Brasil e expondo cada vez mais as pessoas ao vicio precoce por conta da facilidade e da difícil localização dos agentes.

### 3.3.7 Crime de dano

A conduta do crime de dano está ligada com a parte computacional de apagar, modificar, destruir ou inutilizar, parcialmente ou completamente, dados ou programas de computador de maneira não autorizada ou indevida. Um exemplo corriqueiro seria o envio de vírus e similares.

O crime está regulado no ordenamento jurídico brasileiro que se encontra no artigo 163 do Código Penal que fala em destruir, inutilizar ou deteriorar coisa alheia. E para a configuração deste crime, é necessário que cause prejuízo econômico a vitíma. Pois, se o agente enviar um vírus e apenas destruir algumas mensagens ou e-mail de caráter afetivo, não haverá a configuração do crime.

Esta conduta está regulada no Projeto de Lei n.º84-A/1999, que até hoje está em tramite e não a previsão de ser constituída como lei, então, por analogia o sistema jurídico brasileiro se utiliza do artigo 163 do Código Penal.

### 3.3.8 Crime de preconceito e discriminação

Preconceito seria um conceito antecipado sem fundamentação, uma opinião formada sem reflexão. Já a discriminação seria o ato de trata uma ou mais pessoas de forma diferente, com restrições.

Como na maioria dos casos citados acima, esse tipo de delito não possui tipificação especifica quando realizado através da Internet, assim é utilizado por analogia à legislação existente que é a Lei n. 7.716/89.

A Lei traz em seu corpo as punições relacionadas a crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Um atual exemplo de preconceito e discriminação através da Internet fora quando a Presidente Dilma foi reeleita e grande porcentual de votos foi da região nordeste. Assim, inúmeras publicações pelas redes sociais culpavam os nordestinos sobre tal reeleição, onde muitos diziam que por se tratarem de nordestinos eles seriam “burros, analfabetos”. Outro tipo de exemplo atual que vem ocorrendo de

forma corriqueira na Internet seria sobre a união homoafetiva, onde as pessoas expõem suas opiniões de forma discriminatória e sem nenhum tipo de punição, por conta dessa lacuna no nosso sistema penal.

### 3.3.9 Crime contra a privacidade

Privacidade tem significado de intimidade. É um direito Constitucional previsto pela Constituição Federal, em seu artigo 5º, inciso X (BRASIL, 1988), que diz:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Com a crescente dos computadores e evolução da Internet, a privacidade se tornou um grande problema para a sociedade atual, pois com a evolução tecnológica, para acessar dados pessoais ficou muito mais fácil.

Foi com o delito cometido contra a privacidade da atriz Carolina Dieckmann que surgiu a Lei n.º 12. 737/12, que visa punir o individuo que invadir dispositivo informático alheio a fim de obter, destruir ou adulterar dados sem a autorização expressa ou tácita do proprietário do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Houve a invasão de seu computador pessoal, e propagada inúmeras fotos da atriz em poses sensuais e também fotos de seus filhos em momento intimo da família. Ou seja, o agente invadiu o computador da atriz, e feriu sua privacidade quando as obteve sem nenhum tipo de autorização.

# 4 ANÁLISE NA LEI 12.737/12

Neste capitulo, será abordado o surgimento da Lei n.º12.737/12 e suas peculiaridades.

## 4.1 O Caso Carolina Dieckmann

Segundo o site G1 da Globo, no dia 7 de maio de 2012 Carolina Dieckmann procurou a policia, deu inicio a investigação sobre trinta e seis fotos da atriz que foram publicadas na internet, incluindo imagens do seu filho de quatro anos. A atriz começou a receber ameaças de extorsão desde o fim de março do mesmo ano e alega não ter prestado queixa antes, pois queria evitar a exposição do caso na mídia.

O hacker além de ligar em sua residência e falar com a sua secretaria de casa sobre as fotos, mandou um e-mail para seu assessor com duas fotos e para não divulga-las pedia o valor de R$ 10.000,00 (dez mil reais).

Nas investigações a policia encontrou quatro suspeitos no interior de São Paulo e Minas Gerais que possuíam fotos intimas da atriz após terem invadido o e-mail e pego tais fotos.

O grupo especializado da DRCI (Delegacia da Repressão aos crimes de informática) junto com a Polícia Civil do Rio de Janeiro usou programas desenvolvidos para esse tipo de situação para chegarem até os suspeitos e sendo detectado que os suspeitos furtaram mais de 60 arquivos da atriz.

## 4.2 A Lei n º 12.737/12

A Lei n.º 12.373/12 apelidada de “Lei Carolina Dieckmann”, foi uma proposta feita pelo Deputado Paulo Teixeira (PT-SP), que altera o Código Penal para tipificar os crimes praticados no mundo da internet.

A lei ganhou esse nome, pois na época em que o projeto tramitava na Câmara dos Deputados e a atriz Carolina Dieckmann teve suas fotos pessoais divulgadas em dois sites. Segundo o autor do projeto, Paulo Teixeira, "Nós precisávamos dessa lei, o Código Penal não dava conta disso". Vejamos o texto legal (BRASIL, 2012):

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 07 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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.

§ 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.

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

§ 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.

§ 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.

§ 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."

"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:

"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)

"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)
> Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
> Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.
> DILMA ROUSSEFF
> José Eduardo Cardozo

## 4.3 Mudanças no Código Penal

O art. 154-A está elencado no Código Penal, na Parte Especial no Título I, Dos Crimes Contra a Pessoa, Capítulo VI – Dos Crimes Contra a Liberdade Individual; Seção IV – Dos Crimes Contra a Inviolabilidade dos Segredos que foi inserido pela Lei n. 12.737/2012.

Este artigo visa repreender o individuo que invadir dispositivo informático alheio mediante violação indevida dos mecanismos de segurança com o fim de obter, adulterar ou destruir dados informáticos sem autorização do titular do bem para obter vantagem ilícita, apenado com detenção de três meses a um ano mais multa.

A mudança que ocorre no Código Penal é que agora ele possui tópicos sobre a violação de equipamentos e sistemas, sejam eles conectados a internet ou não. Também institui penas de detenção que variam de 03 (três) meses a 1 (um) ano ou multa em casos menos graves. Já crimes mais graves, como por exemplo, “obter comunicações eletrônicas privadas ou segredos comerciais” a pena de reclusão vai de 3 (três) meses a 2 (dois) anos além de multa.

## 4.4 Bem Jurídico Tutelado

O bem jurídico tutelado é a inviolabilidade de dados informáticos, abrangendo além do Direito a Privacidade e o Direito ao Sigilo de Dados, como também visa tutelar a integridade e proteção contra qualquer alteração ou destruição.

## 4.5 Sujeito Ativo e Sujeito Passivo

O sujeito ativo é qualquer pessoa não autorizada a acessar os dados. O empregador, o cônjuge e o proprietário do sistema computacional poderão ser sujeitos ativos se não tiverem autorização para acessar os dados.

O sujeito passivo é qualquer pessoa, podendo ser física ou jurídica, proprietária de dados informáticos.

### 4.6 Tipo Subjetivo

É o dolo genérico, vontade livre e consciente de acessar dados informáticos sem autorização da vítima, do sujeito passivo. Não aceitando a modalidade culposa.

### 4.7 Tipo Objetivo

O verbo é acessar, com a ação de ler, escrever ou executar dados armazenados nos computadores. A leitura consiste em recuperação de dados armazenados no sistema com sua consequente interpretação como informações humanamente inteligíveis. A escrita seria a inserção, remoção ou alteração de dados e a execução de dados seria precisamente a de programas, processamento de informações.

### 4.8 Consumação e Tentativa

Por se tratar de crime material sua consumação se da com a leitura, escrita ou execução de dados do sistema computacional.

É admitida tentativa quando, após iniciada a execução o crime não se consuma por circunstancias alheias a vontade do agente.

No caso de dados criptografados se trata de crime impossível. Cabe ainda o arrependimento eficaz, quando logo após a alteração do sistema o agente se arrepende e o restaura.

### 4.9 Concurso de Agentes

É possível a participação e coautoria, podendo ser de forma unilateral ou plurilateral.

Segundo Túlio Lima Vianna é perfeitamente possível à coautoria e a participação. Unilateral quando com todos os agentes se utilizam apenas de um computador para cometer o delito, e plurilateral quando se utilizam dois ou mais computadores pelos agentes. Ainda, Vianna (2003, p. 95):

> Para a teoria formal – objetiva será autor quem emitir o comando ou a sequencia de comandos que der causa ao acesso não autorizado. Aquele que o auxiliar ditando os procedimentos necessários para lograrem êxito será participe.
> Para a teoria do "domínio do fato" ambos serão coautores do acesso não autorizado e responderão na medida de sua culpabilidade.

Pode-se concluir então que para a teoria formal o autor será aquele que emitir o comando, der causa ao acesso não autorizado, e será somente participe aquele que apenas auxiliar. Já pela teoria do "domínio do fato" os dois agentes serão coautores e serão julgados de acordo com a sua culpabilidade.

### 4.9 Concurso de Crimes

Neste caso, quando o acesso não autorizado for crime meio para pratica de outro delito, não será punido. Porém o delito fim será denominado crime informático mediato ou imediato. Estamos diante do principio da consunção, onde o crime fim absorve o crime meio.

### 4.10 Aumento de Pena por Prejuízo Econômico (Art. 154, § 2º)

O caso de aumento de pena vem da qualificação da conduta praticada, ou seja, se agrava a pena pelo fato da conduta causar grande reprovação pela sociedade atual.

Neste caso, ocorre o aumento de pena se a conduta causar prejuízo econômico, e o direito brasileiro da muita importância para a defesa de propriedade e ao interesse econômico. Sendo assim, ganhando maior importância e desencorajar a pratica do crime.

Além do agravamento de pena gerado pelo prejuízo econômico o autor do crime deve reparar o dano causado.

### 4.11 Formas Qualificadas (Art. 154, § 3º)

Neste parágrafo o agente poderá incidir em causa de aumento descrita no § 4º, elevando a pena de um a dois terços.

Segundo esse parágrafo, “se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidos”, porém cabe saliente que este parágrafo gerara muita discussão doutrinaria em razão da sua aplicação em forma qualificada. O âmbito elencando pelo §2º tem uma abrangência muito restrita as figuras qualificadas e também nas principais não se aplicando para essa qualificadora, além de que a forma qualificadora gera prejuízo para o sujeito ativo. Cabe salientar que a causa prevista no §2º poderá causar um bis in idem.

# 5 PERSECUÇÃO CRIMINAL E SUA ESTRUTURA

Apresenta-se nesse capitulo a forma da denúncia, da investigação, ação penal e de toda estrutura envolvida para se realizar a persecução criminal dos crimes virtuais.

## 5.1 Delegacias

A cada dia que passa os crimes virtuais vem tomando espaço em nossa sociedade, pois com o aumento da população, com a facilidade de acesso a computadores e a internet, consequentemente vêm aumentando o número de pessoas que sofrem algum tipo de violação através da internet.

A falta de conhecimento e cautela da população elevou muito o índice de crimes, e com isso houve uma grande necessidade de se criarem delegacias especializadas.

No Brasil, existem 08 delegacias especializadas em crimes virtuais, as quais são: 4º Delegacia de Crimes Eletrônicos que está localizada em São Paulo, Divisão Cibercrimes –SSP – RJ , Delegacia de Repressão aos crimes de informática (DRCI) que está localizada no Rio de Janeiro, Policia Civil – Núcleo de Repressão a Crimes Eletrônicos (NURECCEL) localizada no Espírito Santo, Delegacia Virtual localizada no Pará, Delegacia interativa em Pernambuco, Delegacia Especial de Repressão aos Crimes Tecnológicos (DECAT) no Distrito Federal e a Delegacia Especializada de Repressão a Crimes contra a Informática e Fraudes Eletrônicas ( DERCIFE) localizada em Minas Gerais.

Cabe salientar que a denúncia de crimes virtuais podem ser feitas em quaisquer delegacias de polícia.

Segundo entrevista no site da Policia Civil do Estado de São Paulo, Wilson Roberto Zampieri Delegado titular da Delegacia de cibercrimes os crimes mais comuns são contra honra, estelionato, fraudes bancarias, ameaça e falsificação.

## 5.2 O “Modus Operandi” da Denúncia

A denúncia realizada é a mesma tanto para crimes virtuais, quanto parar crimes comuns. É feita através de um boletim de ocorrência e podendo ser feito em qualquer delegacia de policia civil e não apenas nas delegacias especializadas em crimes virtuais.

No entanto, para maior comodidade e tecnologia é possível também realizar a denúncia através da internet diretamente no site da Policia Civil, e desta forma com isso ele será encaminhado para a delegacia competente.

Com a ciência do ocorrido, será instaurado o inquérito policial ou se atendidos os requisitos da Lei nº9. 099/95, o termo circunstanciado. Porém, se for o caso de fato atípico será encaminhado à autoridade judiciária competente para analise e arquivamento.

## 5.3 Investigação

A finalidade da investigação é fornecer subsídios para que o autor da ação penal possa ingressar em juízo, sendo dever da Autoridade Policial buscar identificar o autor do delito e a materialidade da infração.

Segundo Carla Rodrigues (2003, p. 105) a investigação tem dois focos: o primeiro é descobrir se o crime real existiu, e em caso positivo, quais foram suas circunstancias; o segundo é esclarecer quem praticou a conduta.

Após a denúncia, dá-se inicio a investigação. Nessa fase serão investigadas às provas apresentadas pela vitíma, e caso a autoria do crime for desconhecida e os vestígios que foram deixados para poder identifica-lo.

A grande dificuldade na fase de investigação é a da colheita de provas, pois por muitas vezes a autoria é desconhecida, sendo necessário que ocorra a quebra de sigilo dos dados dos provedores de internet, uma vez que sem a quebra do sigilo se tornando quase impossível a colheita de informações e assim não consegue se chegar ao autor e nem o punir.

Segundo o Delegado assistente, José Mariano de Araújo Filho em entrevista publicada no site da Policia Civil[3]:

> Os crimes feitos por meios eletrônicos sempre deixando vestígios. A investigação dos crimes por meio eletrônico, parte do principio que ao se

[3] Disponível em http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=2901. Acesso: 07 ago 2015.

> utilizar alta tecnologia e o delito venha consumar-se, sempre deixa rastros, portanto nesta modalidade não existe crime perfeito.
> A principal dificuldade está na obtenção de informações, pois existe uma morosidade muito grande na obtenção das requisições junto ás representações judiciais, que prejudicam na maioria das vezes, a agilidade nas apreensões e investigações de materiais que facilitam os rastreamentos judiciais que contribuem para a elucidação de denúncias registrada.

A grande dificuldade que recai sobre a investigação é a falta de uma legislação especifica, pois se torna difícil a tipificação e muitas vezes acaba ocorrendo atipicidade, ou até mesmo não conseguir encaixar aos tipos penais atuais por analogia.

### 5.4 Da Dificuldade de Obtenção de Provas

Para que ocorra a investigação, é necessário que seja realizada a colheita de provas. Porém, é de grande necessidade que ocorra a quebra do sigilo dos provedores de internet e é ainda que a dificuldade aumenta, pois envolve um direito fundamenta garantido pela Constituição Federal, que é regulado pelo art.5, XII (BRASIL, 1988), que cita:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Além disso, a dificuldade se concentra também na identificação da autoria do crime que não se utiliza de dados verdadeiros, e de computadores diversos. Geralmente se utilizam de computadores de terceiros ou das conhecidas *lan houses*.

Para dar continuidade a investigação é necessário o requerimento de autorização judicial para que ocorra a quebra do sigilo de informações. E quando não há elementos suficientes para ser concedida a quebra do sigilo a investigação é encerrada por falta de provas.

## 5.5 Lugar do Crime

Lugar do crime é conhecido pela doutrina como o local em que o crime está sujeito á lei penal de um país. Segundo Damásio de Jesus (2003,p.121) é como cada Estado possui sua própria soberania, surge o problema da delimitação espacial do âmbito de eficácia da legislação penal.

Sendo assim, a soberania dos Estados impõe a aplicação da lei penal em todo o seu território, águas territoriais e espaço aéreo. Porém, muitas vezes o crime pode ultrapassar a fronteira.

No mesmo sentido temos o artigo 6º do Código Penal Brasileiro, que adota a teoria da ubiquidade em que um país pode abraçar a qualquer dos momentos de um crime, seja atos executórios ou consumativos.

Neste sentido, ainda de acordo com o doutrinador Damásio (2003, p.129):

> Assim, quando o crime tem início em território estrangeiro e se consuma no Brasil, é considerado praticado no Brasil. Nestes termos, aplica-se a lei penal brasileira ao fato de alguém, em território boliviano, atirar na vítima que se encontra em nosso território, vindo a falecer; como também ao caso de um estrangeiro expedir a pessoa que viva no Brasil um pacote de doces envenenados, ou uma carta injuriosa. Do mesmo modo, tem eficácia a lei penal nacional quando os atos executórios do crime são praticados em nosso território e o resultado se produz em país estrangeiro.

O lugar dos crimes podem ser analisados de diversas formas, sendo assim em um determinado território pode acontecer o *inter crimes* ou haver o rompimento de alguma das etapas do crime, como acontece nos crimes chamados “crimes fronteiriços”, onde pode abranger diversos países.

Marcelo crespo (2011, p. 117) cita um exemplo:

> Sob uma ótica prática, uma pessoa que vive no Brasil pode modificar dados armazenados na Itália, transferindo-os para a Alemanha de modo a obter vantagem ilícita. Da mesma forma um vírus de computador pode ser desenvolvido em um país e disseminado por milhares de máquinas por todo o globo terrestre. A transmissão de dados pode envolver diversos países, de modo que o lugar do crime seja determinado de forma quase fortuita.

Dessa maneira, os delitos cometidos através da internet podem ser facilmente cometidos entre diversos países, visto que nesse tipo de delito não

existem barreiras territoriais a serem respeitados, não existem fronteiras. Isso exige muito mais dos países um compromisso em detectar a territorialidade da internet.

## 5.6 Competência

A competência gera muitas discussões atualmente. Alguns doutrinadores acreditam que quando um crime é praticado pela Internet ele deve ser julgado pela Justiça Federal, por conta da Internet se tratar de um serviço público da União.

Segundo Túlio Lima Vianna (2003, p. 95), “quando praticados na internet, deverão ser conhecidos e julgados pela Justiça Federal, uma vez que a internet é um serviço público da União”.

Contudo, é um ponto contraditório. Pois, uma parte da doutrina pela interpretação literária do art. 109 da Constituição Federal no corpo de seu texto não se encontra nenhum dispositivo fazendo referência aos crimes cometidos através da internet. O que se pode levar em consideração a competência ser da Justiça Federal seria em relação ao inciso IV, que seria o caso de crimes virtuais cometidos contra o estado, autarquias ou empresas estatais. Vejamos (BRASIL, 1988):

> Art. 109. Aos juízes federais compete processar e julgar:
> (...)
> IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;

Porém, se o crime cometido dentro do território nacional não se encaixar nas hipóteses do rol taxativo do art. 109 da Constituição Federal, entende-se que será de competência da justiça estadual.

Pode- se dizer que não é um ponto pacificado, em que até os Tribunais divergem:

> A Turma, por maioria, decidiu que é de competência da Justiça Federal o crime previsto no art. 218 do CP, quando o paciente fotografou, filmou e publicou, na rede internacional de computadores, imagens de menor, retratando a pratica de atos libidinosos, inclusive sexo explicito. (STJ, HC nº 24.858 - GO, 6ª Turma, Rel. Originário Min. Paulo Medina, Rel. Acórdão Min. Fontes de Alencar, j. 18/11/2003).

> As vitimas foram constrangidas mediante mensagens eletrônicas ameaçadoras enviadas pela internet, segundo as quais pretendia infligir – lhes mal injusto se não providenciassem valores o que levou as vitimas a ofertar a noticia – crime ao Ministério Público Estadual. (STJ, CC nº 40.569 – SP, 3ª Seção, Rel. Min. José Arnaldo da Fonseca, j. 10/03/2004).

No caso de se trata de crime internacional envolveria competências extraordinárias extraterritoriais, pois o Brasil adota o Principio Geral da Territorialidade, onde as leis não se aplicam ao exterior e se limitam apenas no território brasileiro.

De acordo com Sergio Marques Roque (2007, p. 60/61):

> A questão que suscita maiores duvidas é a dos crimes a distancia, como nos casos dos delitos praticados através da internet quando a ação é executada em um país e seus efeitos ocorrem no Brasil.
> Como resolver, então, este problema? A solução estaria na celebração de tratados internacionais. Mas para isso ser possível há necessidade da existência, primeiramente, da dupla incriminação, ou seja, que as condutas constituam crime em ambos os países.
> Outra questão que se coloca é a extradição, pois como o Brasil não concede a extradição e um seu cidadão para ser processado em outro país, haverá reciprocidade no caso da ação ter sido praticada em território estrangeiro por cidadão não brasileiro.

Ainda no aspecto de extradição, se o crime for cometido por brasileiro nato e a vítima estrangeira, segundo redação do art.5, LI da Constituição Federal (BRASIL, 1988):

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> LI - nenhum brasileiro será extraditado, salvo o naturalizado, em caso de crime comum, praticado antes da naturalização, ou de comprovado envolvimento em tráfico ilícito de entorpecentes e drogas afins, na forma da lei;

Nenhum brasileiro nato que se encontrar nessa situação, onde desestabilizaria um grande desequilíbrio em relação aos crimes que ultrapassam as barreiras territoriais brasileiras.

## 5.7 Ação Penal

Quando a delito for praticado contra uma pessoa física\natural, será necessário que esta de a autorização para que o Ministério Público inicie a persecução penal, sendo então, uma Ação Penal Pública Condicionada à Representação. A pessoa para ter o faculdade de representar o sujeito ativo do crime precisa ser o proprietário dos dados violados.

Será desnecessário o representação nos casos em que o sujeito passivo for o Estado; dessa forma, a ação penal é pública incondicionada.

**5.8 Procedimento**

Não existe em nossa legislação atual normal processual especifica para crimes virtuais, devendo ser aplicada por analogia as do Código de Processo Penal e leis especiais.

Se for crime com punição de reclusão, o procedimento a ser seguido será o comum, previsto no Código de Processo Penal, seguindo as seguintes fases: o autor oferecerá a queixa ou denúncia, e assim ocorrera a citação do réu para o interrogatório e apresentação de defesa prévia. A próxima fase será a oitiva das testemunhas arroladas na queixa/denúncia e a oitiva das testemunhas arroladas na defesa prévia, logo após ocorrendo as diligencias, passando para as alegações finais da acusação e defesa. Sendo a sentença o ultimo ato.

Já nos casos de infração de menor potencial ofensivo, será aplicada a Lei n.º9.099/96 (Lei dos Juizados Especiais Criminais). Deste modo, na fase preliminar deverá realizar-se audiência de conciliação prevista no artigo 72 da Lei n.º9.099/95, tentando-se a composição dos danos, artigo 74 da Lei n.º 9.099/95 e transação penal, artigo 76 da Lei n.º9.099/95. Se a conciliação não for obtida com êxito, passa-se para procedimento sumaríssimo com oferecimento da denúncia oral e intimação do acusado para audiência de instrução debates e julgamentos, prevista nos artigos 77 e 78 da mesma lei.

Se tratando de crime punido com detenção e não se tratar de competência do Juizado Especial Criminal, o procedimento aplicado será o sumario, que está previsto no artigo 531 e seguintes do Código de Processo Penal, ocorrendo as seguintes fases: recebimento da denúncia ou queixa e logo em seguida a citação do réu, passando para a fase de interrogatório e defesa prévia. A próxima fase será a de prova de acusação e logo após o despacho saneador, sendo assim designada

audiência de julgamento onde ocorrerá a oitiva das testemunhas de defesa, debates orais e sentença.

## 6 OS EFEITOS DA LEI Nº 12.737/12

Neste capitulo, será abordado os aspectos positivos e aspectos negativos que a presente lei traz ao nosso ordenamento jurídico.

### 6.1 Aspectos Positivos

Com as diversas mudanças do nosso cotidiano houve o desenvolvimento da internet, uma vez que permite as pessoas estarem conectadas ao mundo de outras pessoas atrás de uma tela de computador.

Além da evolução, a internet revolucionou todos os seguimentos da sociedade moderna ficando cada vez mais vulneráveis a ações criminosas de pessoas que antes ficavam impunes.

Segundo Amâncio (2013, p. 28):

> A fragilidade das leis brasileiras foi um dos fatores que mais contribuíram para que surgissem novos crimes, especialmente nos últimos vinte anos, no ambiente virtual. É certo que muitas condutas podiam ser abrangidas por disposições já existentes na Constituição Federal, no Código Civil, no Código Penal, no Estatuto da Criança e do Adolescente, mas a criação de leis específicas para este tipo de criminalidade se tornou cada vez mais impositiva. […], Nesse sentido, merece destaque a Lei Carolina Dieckmann, que pode ainda se apresentar limitada, porém se revelou um grande salto na proteção às vítimas de crimes perpetrados na internet.

Vale ressaltar que a criação da Lei n.º 12.737/12 veio de encontro com as necessidades atuais da população, pois visa protegê-la de atividades criminosas e tirarem uma vantagem ilícita por meio de extorsão da vitíma.

Wanderlei José dos Reis ressalta[4] que a Lei Carolina Dieckmann representa um avanço legislativo pátrio, já que a tutela cibernética criou um novo bem jurídico o dispositivo informático.

Além de tudo, a repercussão da historia ocorrida com a atriz foi muito relevante para a aprovação da lei, pois acabou dando velocidade ao processo legislativo e vontade de mudança. Com o advento da lei acabou trazendo muita segurança jurídica e maior rigor penal, pois o Brasil é um dos países que tem usuários de internet gerando segurança a todos os usuários.

---

[4] Disponível em: http://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12. Acesso em: 05 out 2015

Outra questão que agradou a muitos juízes, foi o fato de que ele não precisará mais adaptar uma lei para punir o autor do delito, pois com o advento da lei ela já esta tipificada.

Segundo Marcos Mazoni (2013, p.60):

> A lei é positiva no sentido de estabelecer maior rigor penal – as penas variam de um a três anos de detenção mais multa. Esperamos que isso possa causar uma sensação de que o risco de punição é maior, apesar de não ser uma relação direta.

É esperada da nova lei sobre crimes virtuais uma justiça mais ágil, pois está repleta de instrumentos capazes de punir a invasão de dispositivos informáticos e que se diminua a ação desses agentes.

## 6.2 Aspectos Negativos

Um dos pontos fracos da lei de acordo com alguns juristas seria a punição. A pena varia de três meses a um ano de detenção, e assim eles entendem que essas penas não são brandas o suficiente para que ocorra a diminuição da pratica do delito.

Outra ressalva, é que a lei foi criada as pressas em resposta ao público fã da atriz e por conta da vitima se tratar de uma celebridade muito visada, ocorrendo assim, a aprovação do projeto de lei de forma que não fossem analisadas outras formas de se cometer crimes através da Internet.

Além disso, outro aspecto que é muito criticado é o uso do termo “dispositivo informático”, pois, de acordo com alguns criminalistas como Luiz Augusto Sartori de Castro, o legislador deveria ter usado o termo “dispositivo eletrônico”, uma vez que atualmente é possível ter acesso a Internet de diversos tipos de dispositivos, como por exemplo: celulares, televisão, tablet e até geladeiras.

Outro ponto de critica está relacionado à violação indevida de mecanismos de proteção do computador, onde se o computador não tem segurança, como senha ou antivírus, não há como demonstrar que ocorreu a violação e nem como tipificar. Cada caso deverá ser analisado de forma única, e entender como o fato foi cometido e assim realizar uma analise completa.

Importante salientar que quem produz dispositivos e programas de computador, como por exemplo, vírus,que também será enquadrado pela Lei. Porém, deixara uma lacuna em relação à clonagem de redes, pois a lei não á tipifica.

## 7 CONCLUSÃO

Diante de todo o exposto, a após análise sobre todo o caminho percorrido desde o surgimento do computador e da internet até os dias atuais, nota-se a forte presença no cotidiano das pessoas, que buscam realizar suas atividades por meio da internet, destarte, importantíssimo uma legislação que versasse sobre os crimes praticados por meio informático.

Pois além de todo beneficio que a internet nos trouxe, percebeu-se que algumas pessoas se aproveitaram disso para pratica de crimes, e com a falta de tipificação tínhamos uma sensação de impunidade, gerando também um aumento significativo da pratica desses crimes.

Desta forma, após algumas tentativas frustradas de inserção de uma lei que tipificasse esse tipo de crime finalmente foi criada uma lei que versa sobre crimes informáticos, conhecida popularmente como a Lei Carolina Dieckmann.

Antes da criação da lei, os crimes virtuais eram punidos através de analogia, e diante disso, muitas vezes não era satisfatório, pois não eram levados em conta as peculiaridades e sua especificação, sendo assim aplicado por analogia de forma totalmente genérica do Código Penal.

A Lei n.º12.737/12 foi um imenso passo dado pelo direito penal brasileiro, além de trazer mais segurança para os usuários da Internet, ela afastou a tipificação genérica que era feita por analogia ao Código Penal, ou seja, hoje temos uma lei especifica para o crime cometido através da Internet, dando á população mais segurança e assim afastando a sensação de impunidade que tínhamos.

Todavia , além de tanto beneficio que ela nos trouxe, é de se notar que muitos ainda criticam tal lei. Alguns juristas acreditam que a lei é muito genérica, que ela deveria abordar melhor sobre tantas outras possibilidades de se cometer um crime através da Internet, pois como foi exposto acima, a evolução tecnológica está tão grande que é possível cometer crimes através de outros dispositivos, como o celular e seus aplicativos com acessos a Internet. Outros ainda acreditam que as penas deveriam ser mais brandas para que assim diminuísse a pratica do delito.

Portanto, é de se notar que demos um grande passo com a criação da Lei, além de segurança, os profissionais que operam o direito ficaram amparados com essa conduta tipificada.

Neste trabalho não houve a pretensão de esgotar os estudos sobre tal tema, mas sim ressaltar a importância que a Lei tem atualmente. É algo muito presente no nosso dia-dia e que precisava de algo que nos trouxesse mais segurança, e esse é o papel da Lei n.º 12.737/12.

**BIBLIOGRAFIA**

AMÂNCIO, Tânia Maria Cardoso. **O impacto da informática na sociedade e o direito no Brasil**. In: Revista Jurídica Consulex, v. 17, n. 405, p. 24/28, dez. 2013.

ARAUJO, Luiz Alberto David. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2008.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

_____. Decreto-lei nº 2.848, de 7 de Dezembro de 1940. **Código Penal**. Rio de Janeiro: 1940. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso: em 05 de out. 2015.

_____. Lei Federal nº 7.716, de 5 de Janeiro de 1989. **Lei do Crime Racial**. Brasília: 1989. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L7716compilado.htm. Acesso: em 05 de out. 2015.

_____. Lei Federal nº 8.069, de 13 de Julho de 1990. **Estatuto da Criança e do Adolescente**. Brasília: 1990. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L8069Compilado.htm. Acesso: em 05 de out. 2015.

_____. Lei Federal nº 9.610, de 19 de Fevereiro de 1998. **Legislação Sobre Direitos Autorais**. Brasília: 1998. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L9610.htm. Acesso: em 05 de out. 2015.

_____. Lei Federal nº 12.737, de 30 de Novembro de 2012. **Tipificação Criminal dos Delitos Informáticos – Lei Carolina Dieckmann**. Brasília: 2012. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso: em 05 de out. 2015.

_____. Superior Tribunal de Justiça. **Habeas Corpus nº 24858 - GO**. Relator Ministro Fontes de Alencar. Julgado em 18/11/2003. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=442701&num_registro=200201306481&data=20040906&formato=PDF. Acesso: em 05 de out. 2015.

_____. Superior Tribunal de Justiça. **Conflito de Competência nº 40569 - SP**. Relator Ministro José Arnaldo da Fonseca. Julgado em 10/03/2004. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=460216&num_registro=200301871451&data=20040405&formato=PDF. Acesso: em 05 de out. 2015.

BRESSAN, Hélio; CARVALHO,Caio César; CRESPO, Marcelo; MANZONI, Marcos e TAVARES, Thiago. **Banditismo em Rede: Nova Legislação do país sobre crimes cibernéticos traz avanços, mas estabelece penas brandas e deixa lacunas em**

**meio à variedade de delitos cometidos na Web**. In: Revista Imprensa Jornalismo e Comunicação, v. 4, n. 286, p. 58/61, jan/fev. 2013.

CASTRO, Aldemario Araújo. **A legalidade penal e os meios eletrônicos**. Disponível em: http://www.aldemario.adv.br/infojur/conteudo18texto.htm. Acesso em: 05 out 2015.

CASTRO, Carla Rodrigues Araujo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Disponível em: http://jus.com.br/artigos/1826/crimes-de-informatica/3#ixzz3nsyi6Ra0. Acesso em 01 set 2015.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DE JESUS, Damásio Evangelista. **Direito Penal**. 27ª ed. vol.1. São Paulo: Saraiva, 2003.

GAMA SILVA, Remy .Crimes da Informática. CopyMarket.com, 2000

GLOBO, G1 - O portal de notícias da. **Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos**. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html. Acesso em: 10 jul 2015.

REIS, Wanderlei José dos. **Delitos cibernéticos**. Disponível em: http://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12. Acesso em: 05 out 2015.

ROQUE, Sérgio Marcos. **Criminalidade Informática - Crimes e Criminosos do Computador**. São Paulo: São Paulo, 2007.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2002.

ROSSINI, Augusto Eduardo de Souza. **Informática telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SÃO PAULO, Estado de. Assessoria de Comunicação da Secretaria de Segurança Pública. **Entrevista com o delegado Wilson Zampieri e José Mariano de Araujo Filho**. Polícia Civil tem forte atuação sobre crimes virtuais. Disponível em: http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=2901. Acesso em: 05 out 2015

VIANNA, Túlio Lima. **Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003.