

**FANESE - Faculdade de Administração e Negócios do Estado de Sergipe
Campus Santo Antônio
Direito**

Crimes Cibernéticos após a Lei 12.737/2012(Carolina Dieckmann)

José Eduardo da Silva Junior

**Aracaju
2016**

José Eduardo da Silva Junior

Crimes Cibernéticos após a Lei 12.737/2012(Carolina Dieckmann)

Monografia apresentada como exigência parcial para obtenção do título de Bacharel em Direito da FANESE - Faculdade de Administração e Negócios do Estado de Sergipe em julho de 2016 sob a Orientação Carlos Magno de Oliveira

**Aracaju
2016**

CRIMES CIBERNÉTICOS APÓS A LEI 12.737/2012
JOSÉ EDUARDO DA SILVA JUNIOR

Aprovada em 11/06/2016

BANCA EXAMINADORA

Carlos Magno de Oliveira (orientador)

FANESE

Fabio Brito Fraga

FANESE

Afonso Carvalho de Oliva

FANESE

CONCEITO FINAL: _____

DEDICATÓRIA

A Deus, o que seria de mim sem a fé que eu tenho nele.

Ao meu pai em memória que mesmo não presente nesse mundo me ilumina e guia meus passos, a minha irmã Karen Cristina que me ajudou durante os problemas que tive na graduação, minha esposa Maria Alcione Santos, meus filhos Karine Regina e Lucas Matheus e a toda minha família que de alguma forma contribuíram para que eu chegasse até esta etapa de minha vida.

Aos vários amigos e colegas, pelo incentivo, pela força pelo apoio constante.

AGRADECIMENTOS

Ao professor Carlos Magno, pela paciência na orientação e incentivo que tornaram possível a conclusão desta monografia.

A todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia.

Minha energia é o desafio,
minha motivação é o impossível,
e é por isso que eu preciso
ser, à força e a esmo, inabalável.

Augusto Branco

RESUMO

O atual mundo globalizado exige cada vez mais o uso de tecnologias mais céleres e aprimoradas e de respostas imediatas afim de tornarem processos lentos e extensos em mais céleres e eficientes, em se tratando especificamente da área do Direito. Tais necessidades resultam no aprimoramento de novas tecnologias e novos paradigmas, que possibilitaram conjunturas negativas como os crimes cibernéticos, sendo que essas condutas criminosas não estavam previstas e nem eram típicas pelo ordenamento jurídico brasileiro. Como resposta para essa lacuna foi criada a Lei 12.737/2012, que ficou conhecida como Lei Carolina Dieckmann.

O Projeto de Lei que concebeu a Lei Carolina Dieckmann foi proposto em resposta a uma situação vivida pela atriz, no mês de maio de 2011, que teve copiadas de seu computador pessoal por meio de uma fraude cibernética fotos em situação íntima, que acabaram divulgadas na Internet após tentativa de extorsão.

A Lei vem merecendo críticas de vários seguimentos ligados a aplicação e operação do direito como especialistas e profissionais de segurança da informação, pois seus mecanismos são ambíguos, vagos, confusos e podem gerar diversas interpretações, ou até mesmo interpretação subjetiva, o que pode distorcer o enquadramento criminal de condutas triviais, ou dar respaldo a brechas na defesa infratores cibernéticos, o que tornaria a lei injusta e ineficaz. Para outra corrente, pensadora, as penas são insatisfatórias e pouco inibidoras, e a maioria das condutas enquadradas como crime de pequeno potencial ofensivo e seus procedimentos tramitando em Juizados Especiais, o que poderia contribuir para não eficiência no combate ao crime cibernético no Brasil.

O interesse da pesquisa visa verificar a eficiência prática da lei 12.737/13 em relação aos crimes cibernéticos e se a mesma vem sendo aplicada de maneira inadequada, por ter sido elaborada em cima de casos isolados e não ter levado em consideração a situação geral das vítimas de crimes digitais. Se mesmo assim a lei consegue obter êxito (eficaz) para coibir a pratica de tais crimes.

Palavras-chave: Cibernética, Tecnologias, Informática, Crimes, Lei 12.737/2012

ABSTRACT

The current globalized world increasingly requires the use of increasingly rapid improved and immediate responses in order to make processes that are often too time-consuming extensive technologies faster and more efficient in specifically addressing the area of Law. Such needs have brought new technologies and new paradigms that bring with them negative situations as cybercrime, and these criminal acts were not provided, nor were typefaces the Brazilian legal system. In response to this gap was created Law 12,737 / 2012, which became known as Law Carolina Dieckmann.

The bill that conceived the Carolina Dieckmann Law was proposed in response to a specific situation faced by the actress, in May 2011, which was copied to your personal computer, 36 (thirty-six) photos in intimate situation, which ended published on the Internet.

The law has been receiving criticism from various segments linked to application and operation of law as lawyers, experts and information security professionals because their mechanisms are large sometimes vague, confusing and can lead to different interpretations, or even subjective interpretation, which It can be used at the time and made the framework of criminal conduct or even trivial for the defense and support of cyber offenders, which would make the unjust and ineffective law. For another current also the penalties are less inhibitory, and many situations encompassed in the procedures of the Special Courts, which could contribute to the non-efficiency in combating cybercrime in Brazil.

The interest of the research aims to verify the practical efficiency of Law 12,737 / 13 in relation to cybercrime and whether it is being applied improperly, having been drafted on isolated cases and have not taken into account the overall situation of victims digital crimes. If even then the law can be successful (effective) to curb the practice of such crimes.

Keywords: Cybercrime, Techonologies, Computing, Crimes, Law 12.737/2012

Sumário

1 INTRODUÇÃO	9
2 A IMPORTANCIA DA CIBERTNETICA NO ATUAL MUNDO	11
2.1 Conceito de cibernética	11
2.2 Processo judicial eletrônico	13
3 CRIMES CIBERNÉTICOS	15
3.1 Evolução histórica da informática	15
3.2 A história da internet.....	17
3.3 crimes informático.....	18
3.4 classificação do crime cibernético	21
3.5 Crimes comuns contra organizações e indivíduos.....	22
3.6 A deep web.....	24
4 A LEI 12.737/2012(LEI CAROLINA DIECKMANN).....	26
5 CONCLUSÃO	32
REFERÊNCIAS	34
ANEXOS.....	36

1 INTRODUÇÃO

O atual mundo globalizado exige cada vez mais o uso de tecnologias, que necessitam constantemente estarem sendo aprimoradas, serem eficazes e de respostas imediatas, afim de tornarem processos delongados em mais céleres e eficientes, sem falar que hoje a maioria das situações cotidianas da sociedade esta associada a algum elemento da tecnologia ou da cibernética, sendo que essa realidade que a cibernética traz gera grande fascínio sendo ferramenta de entretenimento, diversão além de também possibilitar o uso de uma enorme gama de possibilidades, que também podem ser utilizadas nos mais variados ramos profissionais existentes, tornando a cibernética como um elemento essencial da vida cotidiana, no que diz respeito a área do Direito o aprimoramento de tecnologias motiva mais celeridade nos processos e eficiência aos profissionais desse ramo no desempenho de suas atividades laborais de seu dia-a-dia.

Tais utilidades viabilizam novos paradigmas que possibilitam consigo situações negativas como os crimes cibernéticos, que são condutas que rapidamente tomaram conta do ambiente da grande rede mundial de computadores trazendo um certo de clima de insegurança e receio aos usuários das mais variadas redes e plataformas agregadas ao mundo cibernético, sendo que essas condutas criminosas não estavam previstas e nem eram tipificadas pelo ordenamento jurídico brasileiro. E com intenção de preencher lacuna foi criada a Lei 12.737/2012, que ficou conhecida como Lei Carolina Dieckmann.

A Lei 12.737/2012 foi proposta em razão de uma situação vivida pela atriz que dá nome a Lei em maio de 2011, que teve copiadas de seu computador, fotos pessoais por meio de uma ação fraudulenta de criminosos que atuando na internet visando aplicar golpes, por meio de ações ilícitas conseguiram furtar e divulgar na Internet as fotos que foram surrupiadas do computador pessoal da atriz, logo após tentaram-na extorqui-la, ameaçando-a divulgar as fotos em variados sites da rede mundial de computadores, as ameaças não foram aceitas pela atriz e por seu marido que buscaram o auxílio das autoridades competentes vindo o caso a ser solucionado pela polícia do Estado do Rio Janeiro e na época provocou uma imensa exploração dos veículos de imprensa do país e com isso deflagrou um grande clima de clamor e comoção da população brasileira que passou a reivindicar leis eficientes

e que pudessem ter a devida punição para os cibercriminosos que praticaram a conduta lesiva a atriz.

Outro ponto a salientar é que a internet é uma poderosa ferramenta de entretenimento, de estudo e também de diversão, o número de usuários deste importante veículo cresce de forma descontrolada carecendo cada vez mais a o uso de regulamentos de condutas e modos de agir levando em consideração as leis vigentes e sobretudo o respeito ao meta princípio do direito da valorização da dignidade da pessoa humana.

A Lei tem sido alvo de constantes ataques e críticas de juízes de direito, especialistas e profissionais de segurança da informação, pois seus dispositivos levam a interpretações dúbias e confusas, muitas vezes deixando lacunas e dando ensejo a enquadramentos equivocados, possibilitando brechas e vindo a beneficiar os criminosos digitais, além de que, podem as mesmas darem margens para fomentar a impunidade que impera na sociedade brasileira e que já não são mais toleradas pelo população brasileira em geral.

O interesse da pesquisa visa verificar a eficiência prática da lei 12.737/12 em relação aos crimes cibernéticos e se a mesma vem sendo aplicada de maneira adequada, em contra partida, pelo fato ter sido elaborada em cima de casos isolados, em meio ao clamor provocado pela imprensa e pela sociedade e não ter levado em consideração a situação da maioria das vítimas de crimes digitais, se mesmo assim, a lei consegue obter êxito para coibir a prática de tais crimes e como o Direito se adequa a uma ciência tão dinâmica e que aplica novos paradigmas a um intervalo de tempo tão pequeno como a cibernética, além de mostrar que a internet por ser ainda um universo pouco explorado e sem limites e de constantes mudanças e adaptações.

2 A IMPORTANCIA DA CIBERTNETICA NO ATUAL MUNDO

No mundo globalizado a necessidade de respostas rápidas e precisas no mais curto espaço de tempo possível é uma exigência básica, faz com que a cibernética e as tecnologias agregadas a este ramo tomem papel de extremas relevância na evolução da sociedade de globalizada.

A influência de ramos como a informática é essencial nos processos produtivos que movem o mundo atual chegando a um ponto de dependência extrema das tecnologias, e sua ausência poderiam gerar o caos trazendo a insegurança nas relações e nos variados setores que compõem uma sociedade, além de que, as tecnologias trazem estabilidade e controlam inúmeros processos essenciais a sobrevivência humana, o que torna quase impossível a vida na atual sociedade sem as benéficas da cibernética, e a falta das tecnologias da cibernética levando em consideração o estágio de evolução e dependência da sociedade moderna seria um regressão para humanidade e possivelmente iria instalar o caos e consequentemente insegurança das relações.

Outro ponto a salientar é que a informática que é um ramo agregado a cibernética é meio de inserção e ascensão e possibilita a indivíduos que antes de conhecerem o universo cibernético não possuíam perspectiva alguma de ascensão intelectual e social, passam a ter, com o conhecimento e o domínio de ferramentas tecnológicas a melhoria significativa na qualidade de suas vidas, e com essa inserção passaram a usufruir de melhores condições trabalho e de salários, sem falar que hoje por meio do aparato tecnológico que a cibernética traz consigo tornou a comunicação mais simples e acessível as mais variadas classes sociais, sendo impossível se desvincular da tecnologia, pois as mesmas podem servir como meio para se gerar renda e para se galgar oportunidades atrativas no altamente competitivo campo do trabalho.

2.1 CONCEITO DE CIBERNÉTICA

A cibernética agrega grande número de processos tecnológicos e para ter um entendimento melhor cabe analisarmos o conceito de Cibernética segundo o mestre doutor Ildebrando Chiaveneto.

A) CONCEITO DE CIBERNÉTICA - Cibernética é a ciência da comunicação e do controle, seja na biosfera, seja na tecnosfera. A comunicação é que torna os sistemas integrados e coerentes e o controle é que regula seu comportamento. A Cibernética é uma ciência interdisciplinar, que envolve sistemas de organização, de processamento de informação e de controle. É uma ciência que auxilia a compreensão de outras ciências. Os aspectos operacionais da Cibernética estão relacionados com qualquer campo científico de estudo (como a Engenharia, a Biologia, a Física, a Sociologia, a Psicologia etc.), mas os seus aspectos formais procuram uma teoria geral que, muito embora seja abstrata de todos os campos de aplicação, é apropriada para todos eles. Bertalanffy salienta que “a Cibernética é uma teoria dos sistemas de controle baseada na comunicação (transferência de informação) entre o sistema e o meio e dentro do sistema, e do controle (retroação) da função dos sistemas com respeito ao ambiente”. B) CAMPO DE ESTUDO DA CIBERNÉTICA: OS SISTEMAS O campo de estudo da Cibernética são os sistemas. Sistema “é qualquer conjunto de elementos que estão dinamicamente relacionados”. O sistema dá a idéia de conectividade: “o universo parece estar formado de conjunto de sistemas, cada qual contido em outro ainda maior, como um conjunto de blocos para construção”. Sob um ponto de vista mais prático, podemos definir um sistema como um conjunto de elementos dinamicamente relacionados entre si, formando uma atividade para atingir um objetivo, operando sobre entradas (informação, energia ou matéria) e fornecendo saídas (informação, energia ou matéria) processadas. Os elementos, as relações entre eles e os objetivos (ou propósitos) constituem os aspectos fundamentais da definição de um sistema. Assim, no sistema, temos: um conjunto de elementos (que são as partes ou órgãos do sistema) dinamicamente relacionados em uma rede de comunicações (em decorrência da interação dos elementos), formando uma atividade (que é a operação ou processamento do sistema) para atingir um objetivo ou propósito (finalidade do sistema), operando sobre dados/energia/matéria (que são insumos ou entradas de recursos para o sistema operar) para fornecer informação/energia/matéria (que são as saídas do sistema). (http://www.profcordella.com.br/unisanta/textos/tgs31_cibernetica_e_sistemas.htm)

Entre os ramos da cibernética o que teve significativa ascensão na sociedade e no dia-a-dia de pessoas, empresas, foi a informática que simplificou várias tarefas cotidianas tornando-as mais rápidas e eficientes, porém trouxe uma dependência extrema da informática também, tornando a informática como centro da sociedade moderna, e tal relevância torna os membros da sociedade altamente dependentes a ponto de tornar impossível hoje viver sem a tecnologia e os seus inúmeros benefícios propiciadas pela constante de uso de tecnologias.

Hoje a cibernética é essencial em algumas atividades exemplo é aviação, onde a grande maioria dos aviões são controlados por sistemas informatizados que indicam localização, controlam altitude e temperatura, rotas a serem seguidas e em algumas situações existe a capacidade dos transportes aéreos guiarem-se sem intervenção do homem usando um dispositivo conhecido por piloto

automático. Outro ponto a salientar são os sistemas que gerenciam o tráfego aéreo, que são totalmente informatizados e fazem uso de satélites de última geração o que de certa forma traz uma dependência extrema desses sistemas da cibernética.

Outro ramo de transporte aonde a cibernética tem extrema relevância é o ramo de transportes terrestres, onde é cada vez mais são utilizados semáforos inteligentes gerenciados por ferramentas tecnológicas, sendo usados também no controle do tráfego de veículos também é no monitoramento por câmeras e por outros dispositivos de controle de tráfego de veículos, havendo também o monitoramento de tráfego por meio de radares, câmeras e computadores portáteis.

A medicina do atual mundo também possuiu grande dependência das benéficas propiciadas pelo uso da cibertecnologia que traz análise de exames médicos hospitalares mais precisos, o uso de componentes tecnológicos de ponta e até o uso de robôs e braços mecânicos e raio laser em intervenções cirúrgicas.

Outra área que demonstra a ascensão da cibernética é a área econômica exemplo: são os bancos atividade que tem dependência quase total da informática, sendo impossível hoje dissociar essa atividade da cibernética, exemplos são os mega servidores que gerenciam as atividades bancárias, outro exemplo são os sistemas usados por esses empreendimentos, ferramentas aprimoradas, céleres e de grande eficácia. Agregado ao ramo econômico o ramo das bolsas de valores e futuros que com uso de novas tecnologias mudou comportamentos dos operadores que antes viviam aos gritos para fecharem negócios usam softwares de última geração que produzem resultados mais rápidos e precisos, também na área de bolsa de valores, outro fator que demonstra a importância da cibernética é a bolsa de valores e negócios voltados só para empresas de tecnologias conhecida por Nasdaq. Tais indicadores mostram o crescimento e a força da informática que capaz de mudar costumes e comportamentos.

2.2 PROCESSO JUDICIAL ELETRÔNICO

O ramo do direito com a evolução da cibernética e das tecnologias passou agregar tais benefícios e um exemplo bem claro desta sintonia com as novas tecnologias é o uso PJE Processo Judicial eletrônico que é um sistema que foi produzido pelo Conselho Nacional de Justiça em parceria com Tribunais brasileiros e segue histórico de criação:

O Processo Judicial Eletrônico (PJe) foi lançado oficialmente em 21 de

junho de 2011, pelo então presidente do CNJ, Cezar Peluso. No dia seguinte (22/6), presidentes de tribunais de todo o país participaram de uma apresentação detalhada do sistema e receberam um manual para auxiliar os técnicos na instalação dos softwares. O evento foi transmitido ao vivo pelo portal do CNJ e contou com 1.315 acessos, sendo 135 simultâneos. Além disso, 32 tribunais retransmitiram a apresentação via streaming aos seus servidores. Desde 3 de fevereiro de 2014, o Conselho Nacional de Justiça (CNJ) está utilizando exclusivamente o Processo Judicial Eletrônico (PJe) para o trâmite de novos processos. Os processos em andamento também estão sendo migrados do sistema e-CNJ para o PJe. (<http://www.cnj.jus.br/tecnologia-da-informacao/processo-judicial-eletronico-pje>)

Com sua utilização o PJE trouxe mais celeridade aos processos abrindo um leque para a utilização dos chamados juizados virtuais não utilizando os antigos processos físicos que despendiam um grande uso de materiais e armazenamento além de poupar deslocamento pois os processos não necessitam de protocolamento presencial, tornando o PJE um dispositivo de grande importância para o judiciário brasileiro, mais por ser um serviço que exige uma especialização encontrou de início muitas críticas de usuários que ainda estavam habituados ao modelo antigo e tinha resistência essa nova ferramenta, mas mesmo assim foi implantando e o sistema vem atingindo seus objetivos, mas continua a ser alvo de muitas críticas pois o sistema PJE ainda é dotado de muitas instabilidades, além de ser muito vulnerável, como exemplo podemos citar a invasão do servidor do Tribunal do Estado Sergipe no mês de maio de 2016 aonde o grupo hacker Anonymous Brasil invadiu o servidor deste órgão deixando fora do ar por vários dias e justificaram a ação como um protesto a decisão ao juiz da comarca de Lagarto Marcel Montalvão, que tirou o aplicativo de mensagens instantâneas WhatsApp pelo prazo de 72 horas por não atender determinação para fornecimento das mensagens trocadas por uma quadrilha que agia no município de Lagarto. Este fato expôs a vulnerabilidade PJE e deixou dúvidas com relação a sua segurança, acrescentando que o PJE é um sistema que funciona apenas no browser Mozilla Firefox e tem incompatibilidades diversas com plugins diversos.

O PJE é uma ferramenta positiva, trouxe grandes benefícios, mas precisa de aprimoramentos urgentes e a participação dos usuários para apontarem as falhas a serem corrigidas, desta forma, será ainda mais

3 CRIMES CIBERNÉTICOS

A vida cotidiana tornou o computador pessoal em eletrodoméstico comum chegando a tomar o lugar de outros dispositivos que eram imprescindíveis nos lares do mundo a fora, exemplo é a televisão que alguns programas televisivos já fazem o uso em conjunto com internet como ferramenta de interação e como visto anteriormente a cibernética está em vários ramos da sociedade e para um melhor entendimento e bom observa a evolução da informática.

3.1 EVOLUÇÃO HISTÓRICA DA INFORMÁTICA

A primeira grande invenção da informática se deu no XIX com a invenção do primeiro dispositivo mecânico similar a um computador idealizado pelo engenheiro Charles Babbage que era um experimento rudimentar, a partir do ano de 1940 passaram a haver grandes aprimoramentos o que desenvolveu a chamada primeira geração onde os antigos dispositivos rudimentares passaram a dar espaço a computadores de uso geral que eram capazes de processarem cálculos avançados e já faziam o uso de algoritmo simples mecanismo de extrema relevância na cibernética dos dias de hoje, sendo que esse tipo de dispositivo foi usado durante a segunda guerra mundial pelos nazistas.

Já no ano de 1948 a gigante de tecnologia IBM lançou um computador que aprimorou mais ainda a questão de cálculos avançados, sendo responsável por calcular a posição da lua por meio de sequência eletrônica e também teve destaque esse dispositivo ao traçar a rota da nave espacial Apollo 11.

A década de 1950 já marcada pela invenção dos transistores aprimorou a tecnologia dos computadores por Alan Turing que idealizou um modelo que poderia ser comercializado que ficou conhecido como Univac 1101 que tinha as dimensões de 12 metros de comprimento por 6 de largura e era dotado de 2700 tubos de vácuo que eram responsáveis por seus circuitos era uma máquina avançada que de muita tecnologia no seu tempo e inspirou a criação de outros projetos ao redor do mundo sendo de muita relevância para a evolução da informática.

A década de 1960 e marcada pela invenção dos microprocessadores e ficou conhecida como "Era de Ouro" , microprocessadores dessa época eram extremamente velozes e capazes de realizarem mais de 3 milhões de instruções por segundo e nessa mesma época os computadores já começam a chegar com maior a

frequência as empresas e já atingia vendas expressiva que impulsionaram a década de 1970 que ficou caracterizada pelo uso dos microcomputadores que cada vez mais iam diminuindo de tamanho e tornando cada vez mais velozes e portáteis.

Os anos 80 lançam a chamada quinta geração e os computadores de formato pessoal que iniciaram a grande popularização e a partir dessa década os computadores também passaram a se popularizar e não ser mais apenas restrito ao uso das empresas e impulsionaram a grande popularização da informática nos década que compreende os anos 1990 a 2000. Para melhor compreensão o site especializado em Informática sua pesquisa.com traçou um quadro cronológico.

Segue abaixo um histórico do desenvolvimento da informática e das tecnologias ligadas a computação em geral.1622 - O matemático inglês William Oughtred desenvolve a primeira régua de cálculo.1642 - O pesquisador francês Blaise Pascal cria a primeira calculadora.1822 - O matemático inglês Charles Babbage projeta um computador mecânico, porém este não saiu do papel.1847 - É criado o sistema binário pelo matemático inglês George Boole.1880 - O norte-americano Herman Hollerith cria um processador de dados eletromecânico. O sistema usava cartões perfurados para inserir dados.1930 - Nos Estados Unidos, o engenheiro eletricitista Vannevar Bush desenvolve um computador usando válvulas de rádio.1946 - Os engenheiros norte-americanos John William Mauchly e John Presper Eckart Jr desenvolvem o Eniac, o primeiro computador eletrônico. O Eniac foi desenvolvido para servir aos interesses bélicos dos EUA na II Guerra Mundial. Serviu para fazer os cálculos no desenvolvimento da bomba atômica.1954 - A empresa eletrônica Texas Instruments fabrica o transistor usando silício.1956 - Surge, no MIT - Instituto de Tecnologia de Massachusetts - o primeiro computador que utiliza transistores.1963 - Douglas Engelbart patenteia o mouse.1964 - Paul Baran, pesquisador norte-americano, projeta e cria a primeira rede de computadores interligada por fios.1966 - A IBM desenvolve o Rascal 305, utilizando discos de memória com capacidade de 5 megabits.1968 - Douglas Engelbart cria um sistema com mouse, teclado e janelas (windows).1971 - A Intel cria o MCS-4, primeiro microcomputador pessoal com o processador 4004.1972 - A empresa Atari cria o primeiro videogame com o jogo Pong.1975 - desenvolvem a linguagem Basic, primeira linguagem para microcomputadores, . As linguagens anteriores eram adequadas aos grandes e médios computadores.1975 - Bill Gates e Paul Allen fundam a Microsoft.1976 - Steve Wozniak e Steve Jobs projetam e desenvolvem o micro Apple I. No mesmo ano a dupla a Apple Computer Company.1981 - A IBM lança o micro PC 5150.1985 - A Microsoft o sistema operacional Windows e o Word 1.0 (primeira versão do processador de textos).1989 - Tim Berners-Lee , pesquisador europeu cria a World Wide Web (WWW) que origina a Internet.1991 - Linus Torvald lança o sistema operacional Linux com código-fonte aberto.1992 - A empresa americana Microsoft lança o sistema operacional Windows 3.1. A nova versão do Windows incorpora tecnologias voltadas para a utilização de CD-Roms.1993 - Surge o primeiro browser, o NCSA Mosaic.1993 - A empresa de processadores Intel coloca no mercado o processador Pentium.1994 - É criado o navegador de internet Netscape Navigator.1995 - Chega ao mercado o Windows 95, trazendo incorporado o navegador Internet Explorer.1995 - Criada a linguagem Java pela Sun Microsystems.1997 - Garri Kasparov, campeão mundial de xadrez,

perde pra o computador Deep Blue da IBM.1997 - Justin Fraenkel desenvolve o Winamp, programa utilizado para ouvir músicas no formato MP3.1998 - A Microsoft lança no mercado o Windows 98.1999 - A Intel lança no mercado o processador Pentium III. (<http://www.suapesquisa.com/informatica/>)

3.2 A história da Internet

A internet surgiu na década de 1960 quando dois blocos continentais lutavam pela supremacia bélica no mundo época que ficou conhecida como Guerra Fria conflito ideológico que de um lado um dos estava os Estados Unidos da América e do outro a União das Repúblicas Socialistas Soviéticas. Esses dois países travavam uma guerra de informações marcada por muita propaganda bélica e espionagem o que exigia que as informações cada vez mais restritas.

Os Estados Unidos com medo que suas informações vazassem criaram a ARPANET que seria a rede inicial que eclodiu com a World Wild Web a rede mundial de computadores um fenômeno midiático que transformou a vida cotidiana de muitas pessoas e profissionais, sendo inimaginável um mundo sem as benéficas que a rede mundial de computadores e capaz de gerar.

O atual modelo de internet vem passando por mudanças significativas e a é certo que esse modelo de internet que existe nos dias de hoje irá acabar em virtude pelo grande uso de protocolos, no Brasil um exemplo bem claro de uso exagerado de protocolos está na telefonia celular.

Hoje no país hoje existem mais de 283,4 milhões de linhas e habilitadas mais de 90% dessas linhas tendo acesso a rede a mundial de computadores gerando sobrecarga aos protocolos que estão estagnados e não existe meios expandi-los , outro ponto são a questão de privacidade que a internet no modelo atual passa por cima colocando problemas até que envolve a soberania de países nos quais foram divulgados pelo ex agente da agencia secreta de inteligência norte americana NSA Edward Snowden que discordou das práticas de invasão da agência que fazia parte e divulgou os métodos usados pela agência para espionar empresas governos e pessoas físicas ao redor do mundo e com essa divulgação gerou grande desconforto a diplomacia norte americana e fez reafirmar que na internet no atual

modelo não existe privacidade transformando a web e um ambiente de desconfiança e insegurança colocando cada vez mais em cheque o atual modelo de internet vigente no mundo, esse fato já gera consequências imediatas, a principal e o crescimento de redes não indexadas e de uso de informações criptografadas, redes de difícil rastreamento de controle quase impossível e meios de divulgação de crimes de todas as formas possíveis.

3.3 CRIMES INFORMÁTICO

O cibernético usa várias etimologias e também é conhecido como crime de internet, cibercrime, crime eletrônico, crime digital o conceito dessa modalidade de crime está expresso em:

Tal como a criminalidade tradicional, a cibercriminalidade pode assumir muitas formas e pode ocorrer quase a qualquer hora ou lugar. Os criminosos cibernéticos usam métodos diferentes segundo suas habilidades e seus objetivos. Esse fato não deveria ser surpreendente, afinal, o crime cibernético é nada mais que um "crime" com um ingrediente "informático" ou "cibernético". O Tratado do Conselho Europeu sobre Crime Cibernético usa o termo "cibercrime" para definir delitos que vão de atividades criminosas contra dados até infrações de conteúdo e de copyright [Krone, 2005]. No entanto, outros autores [Zeviar-Geese, 1997-98] sugerem que a definição é mais ampla e inclui atividades como fraude, acesso não autorizado, pornografia infantil e cyberstalking (assédio na Internet). O Manual de Prevenção e Controle de Crimes Informáticos das Nações Unidas inclui fraude, falsificação e acesso não autorizado [Nações Unidas, 1995] em sua definição de cibercrime.

Como é possível observar a partir dessas definições, o cibercrime pode englobar uma gama muito ampla de ataques. Compreender essa ampla variedade de crimes cibernéticos é importante visto que os diferentes tipos de crimes cibernéticos requerem atitudes diferentes para melhorar a segurança do seu computador. A Symantec, com base nas diferentes definições de crime cibernético, o define de forma precisa como qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de hardware. O computador ou dispositivo pode ser o agente, o facilitador ou a vítima do crime. O delito pode ocorrer apenas no computador, bem como em outras localizações. Para compreender melhor a ampla variedade de crimes cibernéticos é preciso dividi-los em duas categorias gerais, definidos para os efeitos desta pesquisa como crimes cibernéticos do tipo I e II. Os crimes cibernéticos do tipo I apresentam as seguintes características: Do ponto de vista da vítima, trata-se de um evento que acontece geralmente apenas uma vez. Por exemplo, a vítima baixa sem saber um Cavalo de Tróia que instala um programa de registro de digitação no computador. Também é possível que a vítima receba um e-mail contendo o que parece ser um link para uma entidade conhecida, mas que na realidade é um link para um site malicioso. Isso é frequentemente facilitado por softwares de atividades ilegais, tais como programas de registro de digitação, vírus, rootkits ou Cavalos de Tróia. Em muitos casos, falhas ou vulnerabilidades no software fornecem um ponto de apoio para o

criminoso. Por exemplo, criminosos que controlam um site podem aproveitar a vulnerabilidade de um navegador da Web para introduzir um Cavalo de Tróia no computador da vítima. Exemplos desse tipo de crime cibernético incluem o phishing, o roubo ou a manipulação de dados ou serviços através de pirataria ou vírus, roubo de identidade e fraude no setor bancário ou de comércio eletrônico. Os crimes cibernéticos do tipo II incluem, mas não se limitam a atividades como assédio e molestamento na Internet, violência contra crianças, extorsão, chantagem, manipulação do mercado de valores, espionagem empresarial complexa e planejamento ou execução de atividades terroristas. As características do crime cibernético do tipo II são: Trata-se geralmente de uma série contínua de eventos envolvendo interações repetidas com a vítima. Por exemplo, o criminoso entra em contato com a vítima em uma sala de bate-papo para estabelecer uma relação ao longo do tempo. Com o tempo, o criminoso aproveita a relação para cometer um crime. Outro exemplo: membros de uma célula terrorista ou organização criminosa usam mensagens ocultas para se comunicarem em um fórum público para planejar atividades ou discutirem sobre localizações para lavagem de dinheiro. Geralmente, eles usam programas que não estão incluídos na classificação de atividades ilegais. Por exemplo, as conversas podem acontecer usando clientes de IM (mensagens instantâneas) ou arquivos podem ser transferidos usando FTP (<http://br.norton.com/cybercrime-definition>)

Em síntese crime cibernético é aquele quando um computador ou uma rede de computadores são usados como uma base para ataque ou se é utilizado como uma base para a prática de crimes.

Essa modalidade de crime pode ocasionar danos tanto a pessoas como a empresas quando seus dados são violados, furtados e divulgados sem expressa autorização ocasionando em determinadas situações prejuízos econômicos, desgaste do nome da empresa junto a cliente, parceiros e consumidores. Já com relação as pessoas o cibercrime também pode afetar com perdas econômicas e contra a imagem pessoal, tipo de conduta que a lei 12.737/2012 não tipificou e da margem a inúmeras condutas delituosas na web por meio desse tipo de conduta ilícita, sendo que esse tipo vem numa escalada crescente e número de casos só fazem aumentar.

Outra modalidade de crime cibernético é chamada "Guerra Cibernética" que consiste em inúmeros ataques por meio da grande rede e em algumas possibilidades existem até a cooperação de países afim de fragilizar um tornar vulnerável outra nação, exemplo desta prática foi o ataque sofrido pelo país do Irã que teve mais de 1000 centrifugas destruídas de seu programa de energia nuclear por meio de um ataque simultâneo que violou a segurança dos dispositivos

invadindo o sistema e fez com as centrifugas se auto destruíssem, sendo que esse episódio ficou conhecido como o primeiro ataque cibernetizar da história e gerou prejuízos significativos e atrasou em mais de um ano o programa nuclear iraniano. Sem falar os prejuízos econômicos gerados que foram cifras expressivas e trouxe a tona crimes contra a soberania dos países situação que agravou-se mais ainda com as revelações do ex agente da NSA Edward Snowden e passou a ser fato que começa a ser discutido nos encontros de cúpula de países e merece atenção especial pois pode jogar o mundo em uma outra grande guerra mundial. Nas palavras de Andy Manoske dá para se medir o tamanho de uma guerra cibernética:

O caça J20 PLAAF de quinta geração, ao lado do caça USAF F-22. Existem teorias que afirmam que o design do J20 foi inspirado em documentos confidenciais obtidos a partir da ciberespionagem. No primeiro caso, podemos usar informações confidenciais destinadas a outrem (espionagem) para ganhar a dianteira na batalha contra seu adversário. Podemos descobrir a velocidade de um míssil e construir um avião que possa ultrapassá-lo. Podemos descobrir para onde um alvo está movendo suas tropas, e planejar uma emboscada. Podemos descobrir quais cientistas são importantes na criação dessas armas, ou qual político foi imprescindível na arrecadação de fundos para o tal sistema bélico — e atacá-los diretamente. Quando se tem o controle desses sistemas, sabotar pessoas também é possível. E se eu colocasse um programa secreto no código-fonte de um míssil que me permita explodi-lo enquanto ele está na terra? E se eu pudesse descobrir como as tropas estão se comunicando, e assim ganhar acesso à rede para que eu possa confundi-los e invadir a base deles? Ou pior: e se eu atacasse funcionários civis e políticos de um país envolvido em uma ação militar? Eu poderia invadir seus sistemas/contas e fraudá-los, me passando por um deles. Eu também poderia usar essas informações para controlá-los e forçá-los a trabalhar para mim: por exemplo, chantageá-los por causa de algo que achei no computador, ou sequestrar suas famílias usando informações privadas. Destruir esses sistemas tem um resultado óbvio: você destrói o que controla esse sistema, e, conseqüentemente, impede-o de funcionar. Um exemplo comum de ciber guerrilha é o uso de ataques DDoS (ataque distribuído de negação de serviço) para desativar sites governamentais e redes sociais. Essa tática foi usada efetivamente pelos russos durante a Guerra da Ossétia do Sul em 2008, causando caos e espalhando informações falsas para a população antes e durante a invasão russa. Quem são os alvos? A guerra cibernética tem como alvo qualquer setor importante para a infraestrutura do inimigo. Isso significa setores óbvios como o exército, a defesa nacional e a indústria bélica. No entanto, esses alvos também podem ser fábricas civis de armas, minas e outras manufaturas que auxiliem no funcionamento dessas fábricas — e o sistema elétrico, que fornece energia para todos esses setores. Na sua versão mais assustadora, a ciber guerra pode ter como alvo o recurso estratégico mais importante de um país: sua população. Um hacker poderia fazer um ataque terrorista para desestabilizar ou desmotivar uma população a lutar. Isso implica em coisas assustadoras como ataques aos setores financeiros, que causariam danos econômicos; ou ataques a sistemas de comunicação — imagine o que aconteceria se a rede de telefonia fosse desativada e a internet caísse. Por que isso ameaça a sociedade. Na minha opinião, a guerra cibernética é assustadora por dois motivos. Primeiramente, a ciber guerra estratégica não faz nenhuma distinção entre alvos civis e

militares. Assim como as armas nucleares da Guerra Fria, as armas digitais podem atingir, indiscriminadamente, alvos civis e militares. Apesar de um míssil causar um dano muito maior do que um vírus, um ciberataque pode, sim, resultar em perdas e mortes de civis. Um bom exemplo seria um ataque ao sistema energético. Nos EUA, este é um recurso estratégico importantíssimo. Se o sistema fosse destruído por um ciberataque (uma possibilidade que assusta o país), não seriam só as fábricas de armas que parariam de funcionar. Um ataque desses resultaria também em acidentes de trânsito, cirurgias interrompidas, falhas em máquinas de suporte à vida — basicamente, umas quantidades absurdas de pessoas morreriam. Em segundo lugar, é muito difícil descobrir o autor de um ciberataque; dessa forma, os governos que financiam esses ataques não tem que lidar com as consequências de suas ações. Um aspecto que faz as armas digitais piores do que as armas nucleares é a atribuição — descobrir quem fez o ataque. É muito fácil esconder a origem de um ataque desses, graças a proxies que mascaram a identificação do autor dos ataques. Mesmo que o governo descubra de qual computador o ataque foi efetivado, ainda existe a dificuldade de descobrir quem era a pessoa atrás da tela — e é ainda mais difícil saber se ele era, ou não, um agente do governo. Sem atribuição, não há responsabilidade. E sem responsabilidade, não existem coisas como intimidação e cessar-fogo. Se um governo não pode ser culpado por ciberataques, existe sempre a possibilidade de este país ir além e partir para ataques semi-terroristas, como a interrupção do serviço elétrico de um país, ou ataques físicos (e perigosos) a fábricas e cidades. Em ambos os casos, cidadãos inocentes podem correr riscos. Quantos desses ataques são financiados por governos? Para ser honesto, ninguém sabe. Não existem estatísticas sobre a divisão entre ciberataques financiados por países e ataques financiados por estados dissidentes ou movimentos como a Al-Qaeda. Esse é um dos maiores problemas da ciberguerra: ela é assimétrica por natureza. Um país pequeno com um forte grupo de hackers pode facilmente atingir um país enorme com uma infraestrutura fraca e um exército incrível. É razoável assumir que hackers financiados por países ricos são mais perigosos. A maioria dos países de primeiro mundo sabe se defender de ciberataques básicos. Hackers financiados por países poderosos são, em sua maioria, mais bem-preparados, e podem organizar ataques que ultrapassam essas defesas, causando danos catastróficos. (<http://gizmodo.uol.com.br/guia-guerra-cibernetica/>)

3.4 CLASSIFICAÇÃO DO CRIME CIBERNÉTICO

Os cibercrime podem ser classificados da seguinte forma segundo Mario Furlaneto e Guimarães:

Crime virtual puro - compreende em qualquer conduta ilícita, a qual atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a parte virtual do microcomputador. Crime virtual misto - seria o que utiliza a Internet para realizar a conduta ilícita, e o objetivo é diferente do citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes. Crime virtual comum - é utilizar a Internet apenas como forma de instrumento para realizar um delito que enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, como messengers, e-mail, torrent ou qualquer outra forma de compartilhamento de dados.

<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>

3.5 CRIMES COMUNS CONTRA ORGANIZAÇÕES E INDIVÍDUOS

Espionagem - quando é realizada a obtenção de dados sem autorização

Falsificação por computador - acontece quando a uma modificação não autorizada de dados

Violação de autorização - quando se usa a identidade de uma pessoa para uma determinada ação é na verdade e executada outra ação.

Vazamento - quando ocorre disseminação indevida.

Falsificação por computador - quando ocorre mutação de dados sem autorização.

Spywares - são programas espiões que são lançados na rede mundial de computadores a fim de captar mensagens e repassar aos desconhecidos.

Trojan horse ou Cavalo da Tróia dos mais comuns vírus de computadores difundido na internet e sua função é abrir vulnerabilidades em sistemas, modificar dados, roubar senhas, destruir hardware, etc...

Sniffers - espécie de vírus de computador de computador que é introduzida no disco rígido e sua função é monitorar e interceptar dados e o tráfego do ambiente de rede.

Cyberbullying é a conduta que é usada para denegrir a imagem de pessoa por meio de dispositivos eletrônicos propagando através da internet. Tais condutas

trazem outras consequências que afetam o dia-a-dia de qualquer indivíduo provocando: depressão, distúrbios do sono, irritabilidade, transtorno alimentares, dores de cabeça, destruição da auto estima, pensamento destrutivos como desejo de ceifar a própria vida.

Pirataria - quando a rede usada para baixar músicas, filmes ou programas que para seu uso exigem o pagamento de licença e estes são copiados em CDS e DVDS que são vendidos sem o recolhimento impostos e direitos autorais.

Pornografia Infantil - conduta muito corriqueira dentro do ambiente da rede mundial de computadores onde abusadores de crianças e adolescentes, pedófilos encontram meios de divulgarem, trocarem fotos, vídeos, sendo que a internet também é uma ferramenta de busca de vítimas para esse tipo de criminoso esse tema é tão frequente que criou-se o até o termo pedofilia digital que é descrito:

A pedofilia na internet é uma realidade graças ao avanço da tecnologia e da informática que provocou uma série de mudanças comportamentais nas crianças, jovens e adultos. Incontroláveis pela gama de informações que a rede nos propõe se faz necessário que fiquemos atentos ao crescimento de web sites que vinculam imagens e vídeos de sexo explícito entre crianças e adultos e outras séries de barbáries sexuais. Pedofilia significa literalmente impulso sexual direcionado às crianças, ou seja, um distúrbio de conduta sexual, onde o indivíduo adulto sente desejo compulsivo por crianças ou pré-adolescentes, sendo este “seleto” grupo composto em sua maioria por homens, muitos deles casados, que não conseguem ter satisfação sexual com uma pessoa adulta. A Lei 8.069/90 – Estatuto da Criança e do Adolescente -, em seu art. 20. considera criança a pessoa até 12 anos incompletos e adolescente e aquela entre 12 e 18 anos. Dentre os vários tipos penais apresentados pelo ECA, encontramos o referente à pedofilia que é o art. 241 que reza: “Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão de um a quatro anos. ” Portanto, entende-se que publicar é tornar público, ou seja, quem insere fotos de crianças e adolescente em cena de sexo comete o crime supramencionado. Este pode ser praticado de várias formas, mas é através de sites, home pages, muitas delas destinadas à pornografia, onde o anonimato é latente que se tem o maior índice desses delitos que tanto preocupa os pais e a sociedade de um modo geral os quais precisam se fazer mais presentes no combate a esta prática criminosa. Como a criação de um web site é muito fácil, bastando apenas se cadastrar em um serviço gratuito de hospedagem em poucos segundos pode ser criada uma página de pornografia infantil. Ressalta-se também, que mesmo sem acesso à página pedófila, as imagens ficam à disposição de todos e, sendo assim, já se configura crime. Isso faz com que nossas crianças fiquem expostas a uma série de imagens pornográficas além da prostituição infantil que é outro grave problema o qual merece uma atenção especial por parte das autoridades competentes. Sendo o bem jurídico protegido pelo ECA, a criança e o adolescente, é necessário afirmar que este bem estende-se a todos, pois a Constituição Federal de 1988 não faz

diferença de tratamento entre brasileiros e estrangeiros residentes no Brasil. Por fim, esclarece-se também que a aplicabilidade da uma suspensão condicional do processo – Art. 89 da Lei 9.099/95 -, não seria possível no caso em tela, pois se deve levar em consideração o grau de perversão da conduta social do criminoso que se utiliza de crianças para satisfazer suas lascívia. É por isso que a sociedade brasileira precisa estar mais atenta aos sites freqüentados pelos seus rebentos, pois a facilidade digital poderá trazer trauma irrecuperáveis à instituição familiar. (http://www.infonet.com.br/faustoleite/ler.asp?id=34884&titulo=Fausto_Leite)

3.6 A DEEP WEB

Uma nova rede de computadores em virtude da internet convencional estar violando a privacidade de usuários com condutas de venda de dados de rede sociais, invasão por meio spammers e cookies entre outra, afim de uma navegação mais particular e com maior privacidade surgiram redes como a Deep Web que é totalmente diferente da internet indexada,

A Deep não faz uso de conteúdo indexado, a forma de navegação é diferente, pois usa um navegador próprio que aloca localização do usuário a um local diferente de onde a pessoa que está conectada na rede sem encontra, a ferramenta que faz essa navegação ficou conhecida como o nome de Thor e foi desenvolvido por uma agência de inteligência e espionagem do governo norte americano no ensejo de poder desfrutar de uma navegação privada.

Essa navegação privada trouxe aspectos negativos e o usuário por sentir-se invisível começou a propagar crimes de todas as formas possíveis na Deep Web. Crimes como: venda de drogas, venda de armas, tráfico de órgãos humanos, pedofilia, comércio de armas químicas e extermínio em massa, etc, a página mais famosa dessa rede que praticava inúmeros desses crimes elencados e movimentava a quantia de 30 milhões de dólares no ano de 2013 era conhecida como "Silk Road", e para que essa quantidade vultuosa de cifras fosse movimentada criou-se uma nova moeda conhecida como Bit Coin que se popularizou e é usado em até outros tipos de transações de produtos lícitos que não estejam associados a crimes.

A deep web é uma rede milhares vezes maior que a rede indexada sendo que a tendência é a deep web crescer cada vez mais em virtude das violações constantes de privacidade da internet comum o que de certa forma está migrando o

usuário de redes indexadas para as redes não indexadas, sendo que esse fator já transformou as redes não indexadas bem mais densas e maiores do que as redes normais indexadas, mas este fato é preocupante pois o monitoramento de redes indexadas é cada vez extremamente complicado propiciando o ambiente ideal a prática de crimes das mais diversificadas formas. O que irá trazer mais problemas é uma nova ameaça e proporções gigantes no que se trata a respeito de crimes cibernéticos e como combater essa modalidade em ambiente tão inóspito como o de redes não indexadas.

Existe uma necessidade urgente das nações começarem a combater as violações de privacidade dentro da internet e empenharem esforços a fim de regulamentarem e organizarem o conteúdo dentro das redes não indexadas, a dinamicidade das redes computadores tornou esse fato uma quase obrigação, pois é claro e notório que apenas com as normas e leis de um país não é possível combater o cibercrime.

4 A LEI 12.737/2012(LEI CAROLINA DIECKMANN)

Uma das primeiras leis brasileira a ser concebida no intuito de combater os crimes cibernéticos nasceu após uma situação vivida por uma atriz de renome da Rede Globo de Televisão o maior complexo mediático brasileiro essa atriz de nome Carolina Dieckmann faz parte de um grupo de atores de ponta da emissora carioca e já teve trabalhos expressivos na teledramaturgia brasileira tendo papéis que emocionaram o público alvo desse tipo de entretenimento, porém até a data que houve a problemática com atriz, já existiam inúmeras vítimas de crimes de tecnologia no país, mas faltava iniciativa e seriedade do poder legislativo brasileiro que possuía inúmeros projetos que nunca chegavam a uma proposta séria de lei ou de uma emenda constitucional.

O momento da mudança deste cenário ocorreu a partir do momento que atriz Carolina Dieckmann em um momento de lazer com seu marido trocaram fotos íntimas por meio do correio eletrônico e está fotos ficaram armazenadas nos itens enviados do email pessoal da atriz e sem perceber a intérprete de novelas da rede globo recebeu por de um email um arquivo infectado que por um vírus que instalou de maneira silenciosa um programa que monitorava tudo que era digitado no computador pessoal da atriz e a partir deste descuido de Carolina Dieckmann o criminosos tiveram acesso a caixa de e-mails pessoais de Carolina ao inspecionar seus email, em poder dessas informações conseguiram lograr êxito ao encontrarem fotos íntimas em situação de nudez que haviam sido enviadas ao marido armazenadas na pasta de itens enviados, os criminosos copiaram as fotos e em seguida começaram a fazer ligações para a interprete tentando extorqui-la para que não divulgassem as supostas fotos na internet.

Mas a atriz não sucumbiu as ameaças e buscou as autoridades policiais do Estado do Rio Janeiro fazendo a denúncia do crime que estava sendo vítima naquele momento, após a denúncia as autoridades competentes os meliantes que a

ameaçavam a atriz e seu marido divulgaram as fotos na rede mundial de computadores propagando o conteúdo das fotos com conteúdo íntimo da atriz num pequeno espaço de tempo para um gigantesco número de usuários da internet no mundo todo. Tal fato gerou uma intensa exploração dos vários veículos midiáticos do país e principalmente da Rede Globo de Televisão empresa de que atriz e empregada, com a exploração excessiva da situação e com isso veio chamar atenção da população brasileira que ainda não estava muito inteirada com relação aos crimes de tecnologia gerando um intenso clamor e o desejo de leis mais eficientes que combatessem e coibisse esta modalidade criminosa. Com a intensa exploração e a pressão da mídia e da população o poder legislativo se viu pressionado a agir no sentido de apresentar respostas as cobranças de uma lei que contemplasse os delitos de tecnologia e tal cobrança gerou efeitos que levaram a elaboração PL 2793/2011 na data de 29/11/2011 apresentada pelos deputados: Paulo Teixeira PT/SP, Luiza Erundina PSB/SP, Manuela D'Avila PCdoB/RS, João Arruda PMDB/PR, Brizola Neto PDT/RJ, Emilian o José PT/BA e de forma célere até demasiadamente transformou-se na Lei Ordinária 12.737/2012 na data de 30/12/2012 com a redação a seguir

Presidência da República Casa Civil Subchefia para Assuntos Jurídicos LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Vigência Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 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 a invasão resulta prejuízo econômico. § 3º Se a 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 Este texto não substitui o publicado no DOU de 3.12.2012 (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm)

Observando o prazo entre o início do processo de instauração do projeto de lei até a mesma ser sancionada foi muito rápido demonstrando que o clamor da população teve efeito, porém etapas foram queimadas e esta corrida insana produziu aberrações e deixou a norma incompleta e dando brechas que a mesma deveria coibir.

Um fato positivo que a Lei 12.737/2012 trouxe foi que partir do momento que foi sancionada os crimes cibernéticos passaram a ser tipificados de forma precisa, a norma com seus artigos passou a se encaixar perfeitamente a uma conduta ilícita a ser coibida, o que antes da existência da lei causava um grande problema, os crimes cibernéticos eram tipificados por meio de analogia e princípios e tal enquadramento deixava duvidoso os inquéritos por não existir norma ou lei que enquadrasse os delitos cibernéticos, além do do confronto contra o princípio da legalidade que está expresso no artigo 5º, inciso II da Constituição Federal Brasileira de 1988, mais por falta de lei os delitos na maioria das vezes eram tipificados por meio da analogia e eram delineados por artigos do Código Penal destaque para os Artigos 155 do CP que traz o crime de furto e o artigo 171 do CP que enquadra o crime de estelionato.

Com a aplicação da Lei 12.737/2012 vemos que agora grande parte dos delitos está tipificado na lei o que traz um grande avanço para o direito e no enquadramento nos inquéritos policiais passam a ser mais precisos sem a necessidade de ter que adequar o fato atípico a outra norma que em regra não tem as características ideais ao ato ilícito.

A nova lei trouxe como novidade os Arts 154-A e 154-B sendo que o primeiro artigo descrito abaixo

"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. "

A Lei trata nesse artigo sobre a invasão de dispositivo informático, a questão dos dispositivos informáticos está bem adequada a realidade da infinidade de dispositivos informáticos que existem e podem vir a se criados futuramente e sendo como exemplos que hoje poderiam estar inseridos de maneira correta ao enquadramento dado pela lei, são os computadores portáteis, notebooks, tablets, smartphones, etc, dessa forma o termo usado sendo e bem adequado neste artigo da lei, também nesse artigo foi colocado de maneira correta o uso ou não da rede mundial de computadores que é tratado de maneira indiferente pela lei, pois a depender: o crime de invasão não depende necessariamente que o mecanismo esteja conectado à internet, também nesse mesmo artigo e feita a menção de obter, adulterar ou destruir dados ou informações, esses requisitos são de extrema necessidade para preservar a privacidade de usuários e de dados inseridos ou gravados em dispositivos eletrônicos, porém a norma peca quando faz a menção a "violação indevida", pois pode haver a violação com autorização do usuário, exemplo: Usuário que leva seu dispositivo para fazer manutenção em uma assistência técnica

autorizada e lá tem seus dados violados durante os reparos de seu dispositivo, tal situação por falha na lei não pode ser interpretado por crime pelo uso do termo "violação indevida" descaracteriza o crime, o correto para que a norma não tivesse essa distorção era apenas usar "violação" assim não deixaria brechas fazendo a tipificação de maneira coesa. Outra situação abordada no referido artigo é o de adulterar ou destruir dados sem autorização situação que é corriqueira no ambiente da internet que ocasiona fraudes e prejuízos o redor do mundo.

O art. 154-A do Código Penal também tem a função de resguardar o sigilo pessoal e também o sigilo profissional, o referido artigo busca punir dois tipos de conduta, sendo que a predominante é a invasão de dispositivo informatizado, mais há disposição também, para se punir a conduta acessória de instalar vulnerabilidade em dispositivo de informática. Essa conduta acessória está fazendo menção clara ao uso de vírus e outras vulnerabilidades que são inseridas no intuito de explorar falhas dos sistemas operacionais deixando os dados e informações do usuário expostos aos cibercriminosos, salientando que essa uma das maneiras mais usadas como meio de invasão em na rede mundial de computadores.

No que diz respeito aos agentes da conduta criminosa a ser combatida pode ser tanto pessoa física como a pessoa jurídica, porém a Lei em relação a esse determinado ponto não deixa claro como será feita tal punição e posteriormente terá que ser complementada por lei especial. Já com relação ao agente passivo será o proprietário do dispositivo informático que podem ser pessoa jurídica ou física, quem também pode ser vítima e a administração pública

Na parte final do artigo existe a atribuição da pena de 3 meses a 1 ano e multa, que enquadra o crime do artigo 154-B do CP como crime de pequeno potencial ofensivo que é outro ponto muito contestados pelos operadores do direito no Brasil, pois a depender do crime de informática praticado tem a capacidade de trazer danos irreparáveis a vida de uma pessoa como exemplo

temos o caso da jornalista Rose Leonel descrito abaixo:

Quase oito anos após ter fotos íntimas divulgadas pelo ex-noivo na internet, a jornalista Rose Leonel, que mora em Maringá, no norte do Paraná, afirma que sofre preconceito constantemente. "Muitas pessoas, tanto homens quanto mulheres, ainda me recriminam pelo que aconteceu, infelizmente", declarou. O caso ocorreu no fim de 2005, logo após o fim do relacionamento do casal. De acordo com a jornalista, o ex-companheiro não aceitou o fim do noivado e, além de divulgar as imagens ainda insinuou em redes sociais que ela era uma garota de programa. A desavença foi parar na Justiça. Em 2010, Rose teve a causa ganha. Contudo, ainda não foi indenizada. Leonel não aceitou o valor arbitrado, de R\$ 30 mil, e tenta recursos para aumentar a quantia. Ao G1, o advogado Thomaz Jefferson Carvalho, afirmou que atitude do ex-noivo configura crime de injúria e difamação e o valor imposto não é compatível. "Dentro disso, ela sofreu vários transtornos. Entre ele perdeu dois empregos e foi julgada pela sociedade em geral", relata. O advogado disse que aguarda uma decisão do Superior Tribunal de Justiça (STJ) sobre o caso. "Apesar de não ter recebido nenhum centavo ainda, quando a sentença saiu, eu me senti aliviada", conta a jornalista. "Foi um alívio moral (...) como se eu tivesse recebido uma absolvição social. Depois da sentença, eu acho que ficou claro para a sociedade que eu era a vítima e ele [o ex-noivo] era o culpado da situação", completa Rose." (<http://g1.globo.com/pr/norte-noroeste/noticia/2013/08/apos-fotos-intimas-pararem-na-web-mulher-diz-sofrer-preconceito-diario.html>)

Analisando o caso Rose Leonel deixa claro que após a divulgação das fotos íntimas da houve um verdadeiro lixamento público da jornalista que passou a sofrer inúmeros julgamentos e teve sua imagem destruída perante a opinião pública em virtude da ação vingativa de seu ex companheiro, e mesmo com o advento da lei não é possível reparar os estragados ocasionados pela divulgação criminosa das fotos na internet. A lei com uma pena de 3 meses a 1 ano que pode ser convertida em multa não consegue ser meio de coercibilidade contra a prática de crimes digitais e muitos doutrinadores e operadores do direito no Brasil defendem penas mais altas e um enquadramento mais rígido ao crime cibernético e que o mesmo não fosse tipificado como crime de pequeno potencial ofensivo, pois a depender do caso concreto o crime cibernético é capaz de fazer estragos significativos na vida das pessoas porém com uma pena majorada até um ano de reclusão que pode ser convertido em uma situação bem mais benéfica e sem o risco da pena de regime fechado dá a lei ares de impunidade. E ainda analisando o caso da jornalista deparamos com o um caso de aonde é violado a privacidade da pessoa por meio da rede mundial de computadores ocasionando um exposição indevida da imagem da pessoa, fato que a Lei 12.737/2012 tratou de forma superficial, que pode ser encarado como um grande erro, pois essa

modalidade de crime e crescente na sociedade brasileira e vem se propagando de forma descontrolada, se a lei fosse mais contundente e punisse de maneira exemplar seria o fator inibidor de tais condutas delituosas

5 CONCLUSÃO

A novas tecnologias e o aprimoramento de dispositivos eletrônicos desde a computação a telefonia são fatores que cada vez mais estimulam e dinamizam o processo de globalização, e neste sistema temos a internet como a ferramenta basilar a impulsionar esta evolução. A cibernética tornou-se essencial na sociedade moderna e o computador uma ferramenta básica na vida de empresas e do cidadão comum na busca de respostas rápidas e simplificadas, e tais mudanças colocam a sociedade num verdadeiro transe, pois as mudanças são drásticas e a grande maioria dos usuários não está preparada para os desafios colocados pelas tecnologias e em especial as trazidas pela internet.

Com várias mudanças e vários paradigmas trazem inúmeros benefícios a população, mais existem o ônus também, que vem revestido por um novo modelo de criminalidade que ficou conhecido por crime cibernético que possui complexidade desmedida e exige ações conjuntas da vários setores da sociedade afim de tentar controlar as condutas dentro da grande rede que ainda e um ambiente gigantesco, pouco explorado e obscuro que exige cada vez mais um planejamento tático e estratégico para pode combater essa modalidade e maligna e outro ponto importante a salientar e que cada vez mais necessário a capacitação de agentes que atuam na investigação de cibercrime, pois e um crime de atividades peculiares, extremamente técnico e de difícil solução e também e notório que os cibercriminosos possuem conhecimento técnico avançado e estão a anos luz na frente de quem deveria coibir e investigar essa modalidade criminosa.

Esses elementos e os conceitos apresentados que compõem esse trabalho geram bastante polemica e controvérsia em virtude de trazer um tema ainda pouco

explorado e que deveria estar regulamentado de forma eficiente junto ao ordenamento jurídico brasileiro, o que não foi feito pela Lei 12.737/2012 que atendeu um desejo de momento e as reivindicações da população brasileira no desejo de se fazer justiça a um fato vivido por uma atriz da maior rede televisiva brasileira, e não levar em consideração os inúmeros casos de crimes cibernéticos que assolam pessoas comuns no país nos dias atuais.

Um primeiro passo foi dado com a Lei 12.737/2012 mas por não contemplar a maioria dos crimes cibernéticos essa lei corre o risco de ficar em desuso, a mesma precisa passar por modificações, onde passe a tipificar um gama maior de condutas criminosas e que a lei possa ter mais efetividade com penas mais gravosas e que coloquem cibercriminosos reclusos e longe de computadores e da rede mundial de computadores.

Contudo e concluímos que a lei não consegue coibir o crimes cibernéticos além de que nem o Estado e nem as autoridades policiais do Brasil estão preparadas para coibir essas condutas criminosas, outro ponto fundamental para atacar os cibercrime é a união de países e nações com ensejo de elaborar tratados internacionais que versam sobre tal matéria e visem coibir o cibercrime.

REFERÊNCIAS

DANILO, **Cronologia dos 40 anos de internet. Cronologia dos 40 anos de internet**, Internet, n.3, p.1, 2009. Disponível em: <<http://a-informacao.blogspot.com.br/2009/09/cronologia-dos-40-anos-da-internet.html>> Acesso em: 30 mar. 2016

O que crime cibernético. Disponível em: <<http://br.norton.com/cybercrime-definition>> Acesso em: 8 mai. 2016

Caso Rose Leonel. Disponível em: <<http://g1.globo.com/pr/norte-noroeste/noticia/2013/08/apos-fotos-intimas-pararem-na-web-mulher-diz-sofrer-preconceito-diario.html>> Acesso em: 20 abr. 2016

Como Funciona a Guerra Cibernética. Disponível em: <<http://gizmodo.uol.com.br/guia-guerra-cibernetica/>> Acesso em: 2 mai. 2016

Conceito de Cibernética.. Idalberto Chiavenato Disponível em: <http://www.profcordella.com.br/unisanta/textos/tgs31_cibernetica_e_sistemas.htm> Acesso em: 15 jan. 2016

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte geral*. V. 1. 16 ed. São Paulo: Saraiva, 2008.

CUNHA, Rogério Sanches; **GOMES**, Luiz Flávio. *Direito Penal: parte especial*. V. 3. Ed. São Paulo: Revista dos Tribunais, 2008.

CAPEZ, Fernando. *Curso de processo penal*. 19. Ed. São Paulo: Saraiva, 2002.

GRECO, Rogério. *Curso de direito penal: parte geral*. V.1. 11 ed. Niterói: Impetus, 2009.

LIMA, Renato Brasileiro de. *Manual de processo penal*. V. 1. Niterói: Impetus, 2014.

MOREIRA, Alexandre Magno Fernandes. *Classificação das infrações penais*. Disponível em <http://www.lfg.com.br>. 14 de abril de 2009. Acessado em 28/04/2013

Crime de Internet. Disponível em:
<<http://www.cjf.jus.br/revista/numero20/artigo9.pdf>> Acesso em: 5 mai. 2016

Historico de Criação PJE. Disponível em: <<http://www.cnj.jus.br/tecnologia-da-informacao/processo-judicial-eletronico-pje>> Acesso em: 28 abr. 2016

Informatica e a Historia da Informatica. Disponível em:
<<http://www.suapesquisa.com/informatica/>> Acesso em: 3 abr. 2016

Lei 12737/2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 6 jun. 2016

O que é crime Cibernético?. Disponível em: <<http://br.norton.com/cybercrime-definition>> Acesso em: 4 mai. 2016

Pedofilia mais um crime digital. Disponível em:
<http://www.infonet.com.br/faustoleite/ler.asp?id=34884&titulo=Fausto_Leite>
Acesso em: 13 abr. 2016

Sistemas e Cibernética. Disponível em:
<http://www.profcordella.com.br/unisanta/textos/tgs31_cibernetica_e_sistemas.htm>
Acesso em: 6 fev. 2016

ANEXOS

Jurisprudência do caso Rose Leonel

Processo: 0756367-3

APELAÇÃO CRIMINAL Nº 756.367-3, (NPU , DA 4ª VARA CRIMINAL DA COMARCA DE MARINGÁ.

RELATORA1: JUÍZA LILIAN ROMERO RECORRENTE: E. G. S.

RECORRIDA: R. L. INTERESSADO: MINISTÉRIO PÚBLICO

PENAL. APELAÇÃO. CRIMES DE INJÚRIA E DE DIFAMAÇÃO. ARTS. 139 E 140 DO CÓDIGO PENAL. AGENTE QUE POSTA E DIVULGA FOTOS ÍNTIMAS DA EX-NAMORADA NA INTERNET. IMAGENS E TEXTOS POSTADOS DE MODO A RETRATÁ-LA COMO PROSTITUTA EXPONDO-SE PARA ANGARIAR CLIENTES E PROGRAMAS. PROVA PERICIAL QUE COMPROVOU A GUARDA NO COMPUTADOR DO AGENTE, DO MATERIAL FOTOGRÁFICO E A ORIGEM DAS POSTAGENS, BEM COMO A CRIAÇÃO E ADMINISTRAÇÃO DE BLOG COM O NOME DA VÍTIMA. CONDUTA QUE VISAVA A DESTRUIR A REPUTAÇÃO E DENEGRIR A DIGNIDADE DA VÍTIMA. AUTORIA E MATERIALIDADE COMPROVADAS. CONDENAÇÃO CONFIRMADA. RECURSO NÃO PROVIDO. 1. O defeito da procuração outorgada pelo querelante ao seu advogado, para propor queixa-crime, sem 1 Em substituição ao Desembargador José Maurício Pinto de Almeida. TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3 menção do fato criminoso, constitui hipótese de ilegitimidade do representante da parte, que, a teor do art. 568 C.Pr.Pen., "poderá ser a todo o tempo sanada, mediante ratificação dos atos processuais"... (STF-1ª Turma, HC 86.994-7/RJ, Rel. Min. Sepúlveda Pertence, julg. 14.03.2006, DJ 31.03.2006, p. 18) 2. "1. A ausência de menção ao fato criminoso na procuração que acompanha a queixa trata-se de vício que pode ser sanado a qualquer tempo do processo-crime, ainda que ultrapassado o prazo decadencial, até o momento da sentença final, consoante o disposto no art. 569 do Código de Processo Penal. 2. Qualquer forma de demonstrar o interesse do querelante na persecução criminal quanto ao seu fato objeto supre o defeito do art. 44 do Estatuto Repressivo, eis que este se foca na possibilidade de futura responsabilização do querelante no caso de cometimento do crime de denúncia caluniosa." (Acórdão nº 24.993, da 2ª C.Criminal do TJPR, Rel. Des. José Maurício Pinto de Almeida, julg. 06.08.2009 - unânime, DJ 28.08.2009) 3. Comete os crimes de difamação e de injúria qualificadas

pelo emprego de meio que facilita a sua propagação arts. 139 e 140, c.c. 141, IIdo CP o agente que posta na Internet imagens eróticas e não autorizadas de ex-namorada, bem como textos fazendo-a passar por prostituta. TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

Vistos, relatados e discutidos estes autos de Apelação Criminal nº 756.367-3, da 4ª Vara Criminal da Comarca de Maringá, em que figura como recorrente E. G. S., como recorrida R. L., como correu Edson Alexandre Domingues Moreno e como interessado o Ministério Público do Estado do Paraná I. Relatório A recorrida R. L. ofereceu queixa-crime contra o apelante, imputando-lhe o cometimento dos delitos previstos nos artigos 138, 139 e 140 do Código Penal, assim descritos na inicial acusatória:

"A vítima manteve um relacionamento íntimo com o Sr. Eduardo, ora réu, por aproximadamente 03 (três) anos, conforme já constou do processo apenso (Busca e Apreensão).

Todavia, inconformado com a decisão da vítima, o Sr. Eduardo passou a agir moralmente, a fim de denegrir a imagem da mesma em seu meio social, perante amigos, familiares, principalmente em seu âmbito profissional, visto que a mesma é jornalista conhecida em toda a cidade.

A primeira conduta assumida pelo réu foi a de encaminhar e-mails a diversas pessoas, passando-se pela vítima, em caráter erótico e sexual, contratando o corréu para fazer o serviço no mundo da internet conforme já ficou comprovado anteriormente perante esse juízo segundo documentação ora inclusa, e o que já consta nos autos supracitados apensados a este.

Os procedimentos dos réus tomaram vulto nacional e internacional conforme comprovação no laudo pericial incluso nos autos de Busca e Apreensão, incluindo-se as diligências que comprovam que as máquinas utilizadas com nova tecnologia surgiram de um ponto comum e de um local só, onde ambos qualificados possuem acessos.

TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

A surpresa última fora quando o perito judicial, qualificado as fls. daquele processo, localizou em um site alemão, novas fotos íntimas da ora vítima,

que fora ameaçada após o cumprimento da ordem judicial nesta cidade em 08/08/2008 às 07 horas da manhã, horário em que fora perseguida pelo Sr. Eduardo, dando origem a um Boletim de Ocorrência lavrado perante autoridade policial responsável pela Delegacia da Mulher.

As ameaças chegam e chegaram por várias formas tais como: por e-mail (documentos nos autos), contato físico, e agora com perseguição, tentando amedrontar a ora vítima, pessoa conhecida no mundo jornalístico que tem o direito de resguardar a sua imagem e que não se mistura com o direito de privacidade.

Para tanto, sabendo das condições gravíssimas que vem ocorrendo, fez lavrar Escritura Pública de Ata Notarial que fez como pessoa vítima nas notas do 2º TABELIONATO ROCHA LOURES, folhas 22 do livro 1-NA, Código Esc. 006, Protocolo 08001101, Folhas 001, lavrado em 31/07/2008, que vem subscrito pelo notário DIDEROT AUGUSTO DA ROCHA LOURES, pessoa capacitada, com fé-pública, inconteste, juramentado perante o juízo e o Tribunal do Estado do Paraná, sendo esta válida em todo o território nacional.

Esse ato fez com que fossem certificados, os endereços dos mais variados sites já examinados, na escritura pública onde fora constatado a inserção de imagens, palavras, fotos e expressões que ferem os princípios morais e da dignidade da Sra. R. L. Corrêa. E, por respeito a esse mesmo juízo, a pessoa vítima, resguardando a dignidade da pessoa humana, simplesmente não reproduziu tais imagens porque foge ao respeito e a decência.

Esta escritura e os exames dos sites ocorreram perante a vítima e, ainda, perante a Sra. Cecília Gonçalves de Alvarenga, Sr. Fábio Yanaga e o Tabelionato cujo nome já consta desta petição.

Toma liberdade para descrever alguns termos constatados nos sites denunciados na Escritura Pública e boa parte constatado pelo perito que subscreveu o laudo ali acostado: -" meter, puta, xupar, rolas, foda, gozar, corno, fode, idiotas, chupa, piro, fudendo, rabo, biscate, buceta, goza, gozo, vadia, xoxota, pinto, merda, babaca, mete, cú, puteiro, rola, chupou, vagabunda, depravada, xupa, fdp, pau, rabão, rolona, caraio, perva, pornô, fuuuuuuuuudeeeeeeeeeuuuu, pica, peladona, piranha, baranga, punheteiro, comeu, orgias, swings, pelada "(vide documento de escritura), e na sequencia tudo mais o que fora possível e atestado por fé-pública e confirmado pela perícia do expert.

VÊNIA! As atitudes que foram tomadas perante o juízo e acarreadas aos autos como comprovante, são inconteste, não podendo ser impugnadas por terceiros tendo em vista que já fora denunciado a fonte de onde partiu: bem como tais provas tornaram-se objeto que confirmam os envolvidos no pólo como réus criminosos.

Nunca esqueçamos que esses, perante um juízo especial, já conhecia de

seus atos e, aquela confissão e o pagamento de quirelas feitas conforme aceito após termos circunstanciados, leva-nos a crer que para tais elementos a justiça não vale nada.

TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

Portanto, estão evidentes todos os atos praticados continuados, violentos, agressivos e enquadrados em cada artigo mais de uma dezena de vezes, cabendo este cálculo a ser apurado na certidão levado aos autos expedidos pelo 2º TABELIONATO DE NOTAS dessa cidade, bem como tudo que fora apanhado e estranho as notas, mas, confirmados pelo perito qualificado nos autos de Busca e Apreensão.

Até agora a injustiça se fez presente, todavia, como a JUSTIÇA é a filha do tempo, chegou o tempo das confissões serem apreciadas frente a nossas leis, pois observamos que os réus, sem nenhum caráter, buscaram a violência contra a dignidade da pessoa humana e, a nível Internacional, nós sabemos que os Direitos Personalíssimos é um dos itens da Declaração Universal do Direito do Homem que o Brasil também subscreveu.

Ademais as fotos utilizadas compunham material pessoal sacadas pelo Sr. Eduardo conforme seu desejo, as quais serviram de base para fotos montagens a fim de denegrir a imagem da vítima.

As fotos foram tiradas em um momento de intimidade do casal, sendo certo que a vítima jamais desconfiou ou sequer pode fazer um juízo de que tais materiais pudessem ser usados para denegrir sua imagem e conduta, mesmo porque, submeteu-se a isso por entender que se tratava de uma "fantasia" de Eduardo (o qual também foi casado e também tem filhos), pessoa com quem teve intimidade e fez planos para o futuro: era uma relação baseada em amor e amizade e não em intrigas, mentiras ou ódio.

Conquanto, para a prática de tais atos de imoralidade, que teve como consequência os prejuízos e danos causados à vítima, o Sr. Eduardo contou com o auxílio e colaboração do Sr. Edson Alexandre Domingues Moreno, a saber: No que tange ao corréu Edson, este é empresário do ramo de informática, exercendo seu labor como prestador de serviços, ganhando para isso, conforme troca de correspondências.

O Sr. Edson conhece a vítima e o réu Eduardo. Certo é que o Sr. Edson conhece dos fatos, eis que este recebera um e-mail com fotos e dados pessoais da vítima.

Ademais, o corréu Edson presta serviços de manutenção de computadores e

assistência técnica para a empresa do Sr. Eduardo.

Ciente das ações continuadas dos réus, a vítima só teve um caminho: buscar, mais uma vez, a justiça nos termos deste pedido uma vez que em outra oportunidade, os réus deram origem ao Termo Circunstanciado registrado sob o nº , que tramitou junto ao Juizado especial Criminal dessa Comarca, a fim de apurar a ocorrência dos crimes de difamação, injúria e ameaça, os quais foram praticados pelos réus.

Eis aí, a pedra de toque para que V.Exa., aceite integralmente este pedido sem exceção, o desrespeito é evidente e a injustiça se faz presente.

Pedimos Vênia para reproduzir alguns termos onde um dos réus reconheceu suas atitudes: quando ouvido pela autoridade policial, o Sr. Eduardo reconheceu que algumas das fotografias utilizadas nos meios eletrônicos foram tiradas em seu apartamento, confirmando que fora ele quem se dirigiu à vítima como " VADIA "nos escritos e nos envelopes que serviram como prova naqueles autos. Em outro momento, quando indagado pela autoridade policial,

TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

o Sr. Edson disse que é possível que tenha recebido algum e-mail do Sr.

Eduardo perguntando sobre como fazer para colocar fotografias em editor de texto, eis que realmente é sua função prestar esse tipo de consulta.

Importante esclarecer que o Sr. Eduardo ameaçou à vítima, deixando claro suas intenções de destruir a ela, bem como a sua família, uma vez que este não concordava com o fim daquele relacionamento, nem com as atitudes tomadas neste momento, pois a perseguição pessoal, ora denunciada, prova que esse senhor não teve ninguém.

Comprovado está que as imagens da vítima foram lançadas no cyber espaço da internet, e chegou até mesmo a ser usada para fazer compras em um magazine do Rio de Janeiro, conforme comprovante em poder da vítima encaminhado ao um dos juízos.

De certo que o réu ou o corréu tem em seu poder muitas fotos íntimas do casal, as quais também serviram de base para montagens eletrônicas, ou seja, evidenciando que existe relação entre o ocorrido e a pessoa do Sr. Eduardo, que, supostamente, recebeu auxílio do Sr. Edson para por em prática os seus planos.

Ainda, no que tange ao processo que tramitou no Juizado Especial Criminal dessa Comarca, cumpre esclarecer que fora firmada transação penal, na

qual ficou estabelecido que os réus deveriam pagar à vítima, o valor pecuniário de R\$ 3.000,00 (três mil reais), sendo R\$ 2.000,00 (dois mil reais) pagos por Eduardo e R\$ 1.000,00 (hum mil reais) pagos por Edson.

Ocorre que, embora houvesse transação penal, não se estipulou, naqueles autos, a devolução do material utilizado (fotografias) em favor da vítima, o que tornou necessária as vias judiciais, novamente, para reintegrar àquele material à mesma, visto que tais fatos não deixaram de ter um fim como aquele feito, aliás, hoje com gravames em todo território nacional e internacional conforme ficou comprovado nesta queixa.

Os documentos juntados levam-nos a crer que outros crimes foram cometidos; os documentos elencados nesta oportunidade, em especial, a investigação virtual, deixam certo que o objetivo dos réus eram ofender.

O pedido vem estribado no Código de Processo Penal, revelando-se via busca e apreensão a existência da materialidade dos delitos.

Diante do exposto, se fez necessário o ajuizamento da presente, pois, além de praticar os crimes acima descritos, feriram também os princípios morais e éticos da pessoa humana.

FUNDAMENTOS DOS CRIMES A CALÚNIA fora bem definida, bem fundamentada, quando levou-nos a crer que os querelados buscaram a imputação falsa de ato libertinos com pessoas ignoradas que teriam se envolvido com a vítima. Fica evidente que a vítima estaria divulgando seus atos, atos esses que por si só afetam a moral.

Configurou-se aí um dos crimes contra a honra, definida no artigo 138 do código Penal.

O primeiro denunciado, buscou difamar pessoa que conhecia, chegando a ferir a sua credibilidade ao espalhar pela internet, falsos e-mails, sites e imagens.

Buscou na verdade a DIFAMAÇÃO da vítima, crime previsto no artigo 139 do Código Penal.

TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

Se manusearmos a farta documentação originária dos sites continuamente, mesmo após o acordo denunciado nestas páginas, não podemos ignorar que o primeiro denunciado buscou a INJÚRIA, ofendendo a dignidade de uma pessoa pública, uma jornalista que mantinha coluna no jornal de grande circulação da cidade de Maringá, independentemente de

programa televisivo.

Tudo isso cometido com a colaboração do trabalho originário do segundo denunciado, até então prestador de serviço do primeiro denunciado. Ambos concorreram para a prática do crime previsto no artigo 140 do Código Penal.

CONCEITO DE HONRA a honra é um complexo ou um conjunto de predicados ou condições que a pessoa humana adquire. Isso confere a essa, consideração social em estima própria.

No caso de R. L., seria a dignidade, a mãe, a professora, o nome, a jornalista. Qualquer pessoa do mundo social é especial quando possui um currículo exemplar, é respeitada em suas condutas e qualquer fato denunciado contrário a moral, consiste na ofensa da honra humana. Isso ocorreu, o gravame é evidente, refletiu na vida social e empresarial.

A ofensa é evidente quando os agentes utilizaram meios aparentemente inocentes (colocar a imagem da vítima em foto maquiada, manipulando o próprio corpo). Em outras fotos examinadas observamos na expressa realidade de seus atos, algo reticente. A ofendida jamais permitiria que se tirasse uma foto com qualquer pessoa" a possuindo ", para denegrir seus modos viventes.

O elemento subjetivo é presente em todos os atos dos denunciados, pois esses vieram para ofender a pessoa da vítima.

CALÚNIA: de todos os crimes contra a honra, é o mais grave e, pelas lições de Paulo José da Costa Júnior, observamos que há nexos casuais uma vez que os denunciados buscaram desabonar a vítima e depreciá-la.

DIFAMAÇÃO: pelas lições do Desembargador Dirceu de Mello, difamação consiste atribuir a alguém, efeito ofensivo à sua reputação, estendendo a honra externa objetiva, a boa fama e o prestígio de uma pessoa ou de qualquer outro cidadão. No caso em pauta buscaram ferir a fama e o prestígio de R. L..

INJÚRIA: pelas palavras de Edgar Magalhães Noronha, a injúria é a palavra que os agentes colocaram como da" vítima ", ofendendo o sentimento de dignidade. No caso em pauta, o exemplo é a criação de um email denominado roseleonel@roseleonel, em momento algum a vítima iria usar o seu nome ou apelido para um site de encontros, isso só na cabeça de uma pessoa viciada com desejo de algo estranho seria possível. A jornalista com conduta moral libada, jamais iria se expor ao ridículo e a uma pecha de" puta ".

Sabemos que a internet vive com um mundo de fraudes, é um mundo diferenciado, onde também se escondem os malfeitores, homens de má índole, sem ética e sem dignidade.

Na internet, via sites, email, vídeos, publicaram imagens maquiadas, fraudadas, com a prática de crimes contra a honra. Até o estelionato aparece

presente, há falsidade ideológica e outros crimes que podem ser objeto de apuração em processo apartado.

TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3

Eis que no dia da busca e apreensão, foram colhidos entre os objetos, e isso fora anotado pela vítima, documentos copiados que essa jamais assinara; crimes contra a paz pública entre outros.

Observou que o primeiro denunciado, possui em seus arquivos, um recibo onde aparece a assinatura de R. L., sendo que, esta, jamais cederá as suas imagens e, até prova em contrário, ali apareceu algo que comunga com uma falsa seção de imagens.

Em melhor exame, observou-se que a má-fé, a má índole, buscou acobertar os seus erros com exibição de possível documento de seção de imagem, que não se sabe a que título fora usado. II DO DIREITO Quem teve a felicidade de ter em mãos o trabalho: "As Garantias da Liberdade Individual em Face das Novas Tendências Penais", do professor Noé Azevedo, datado em dezembro de 1936, sabe-se que, os professores da época, já previam que o juiz deve ter uma visão muito ampla para aplicar a lei dando contorno a certos casos.

Plínio Barreto afirma em reportagem para o jornal O ESTADO DE SÃO PAULO 16 XII 1936 o que segue: "Mais vale a garantia pessoal representada por magistrados capazes de usar de um certo arbítrio em benefício tanto do indivíduo como da sociedade, do que a garantia legal estratificada das rígidas normas, com as quais o mal juiz poderá esgotar os seus desafios, transformando os seus desafetos, transformando factos inocentes, capciosamente interpretados em crime severamente punidos.

Realmente, se o direito penal clássico proíbe a interpretação ampliativa da lei penal para qualificar crimes e impor penas, permite, todavia, que o juiz interprete a seu modo os fatos amoldando-os à precisão legal e transformando em crimes ações não punidas pelo legislador.

Convencendo-me da ineficiência de todas as garantias legais, se os mesmos não contarem com juízes bem formados de liberalismo, entendi que era melhor seguirmos a ideologia da Escola Correcionalista e a de Doniado Monteiro (Prof. Direito USP-1935), formando um direito penal protetor dos indivíduos. "Eis aí pedra fundamental para o juiz exaurir caso a caso e

aplicar a lei, enquadrando crime a crime, caso a caso, para proteger o cidadão vítima de atos criminosos.

Já, em 1935, as grandes liminares de direito já aceitaram que o juiz analise caso a caso, tendo em vista os "avanços dos atos criminosos", o que diremos em nossos dias, quando os legisladores não acompanham o avanço da tecnologia moderna.

Assim, observam o jurista Plínio Barreto, Professor da Faculdade de Direito da USP 1936 "os atos dos juízes tem dado ótimos resultados em todo o mundo. Aguardamos a reforma da legislação penal dos adultos.

Esperavam o Código Penal de 1940 ainda em vigor.

Dizia ainda que o delinquente precisa mais de tratamento do que pena. "É de se pensar se os réus não são pessoas que sofrem de `desvios de personalidade"'. ([http://tj-](http://tj-pr.jusbrasil.com.br/jurisprudencia/20132845/apelacao-crime-acr-7563673-pr-0756367-3/inteiro-teor-20132846)

[pr.jusbrasil.com.br/jurisprudencia/20132845/apelacao-crime-acr-7563673-pr-0756367-3/inteiro-teor-20132846](http://tj-pr.jusbrasil.com.br/jurisprudencia/20132845/apelacao-crime-acr-7563673-pr-0756367-3/inteiro-teor-20132846))

LEI 12.737/2012

**Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos**

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Vigência

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 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

Este texto não substitui o publicado no DOU de 3.12.2012

