

CRIMES CIBERNÉTICOS: UMA ANÁLISE DA LEI 12.737/2012 E DO MARCO CIVIL DA INTERNET

Maria Alice de Araújo Leocádio da Silva¹

Sandresson de Menezes Lopes²

RESUMO

A evolução da sociedade e o direito estão diretamente ligados, paralelamente a esse desenvolvimento o direito tenta acompanhar as mudanças sociais, novas normas vão sendo criadas para regulamentar a convivência. O mundo contemporâneo vivencia uma nova realidade, a era digital, onde milhões de usuários estão conectados na internet das mais diversas formas, diante deste avanço tecnológico com a sua inserção no dia a dia das pessoas, surgiram usuários que utilizam desta praticidade que a rede nos proporciona, deste ambiente livre e sem fronteiras para desenvolver uma nova modalidade delitiva, os crimes cibernéticos. Ante este paradigma o direito verificou a necessidade de regular as relações que passaram a se desenvolver nesse mundo virtual ou ciberespaço, surgindo assim novas leis que tipificam os crimes informáticos que apesar de algumas críticas é considerando um grande avanço para a legislação brasileira. No decorrer deste estudo será abordada essa nova criminalidade, os crimes virtuais, essa nova tipologia de condutas criminosas perpetuadas no ciberespaço, serão levantadas características peculiares dos crimes informáticos, assim como, uma análise das legislações vigentes, mas especificamente a lei 12.737/12 e o Marco Civil da Internet.

Palavras- chaves: Crimes cibernéticos. Ciberespaço. Lei 12.737/12. Marco Civil da Internet.

CYBER CRIMES: AN ANALYSIS OF THE LAW 12.737/2012 AND THE CIVIL FRAMEWORK INTERNET

ABSTRACT

The evolution of society and the law are directly connected in parallel to this development right tries to monitor social changes, new standards are being set up to regulate coexistence. The contemporary world has experienced a new reality, the digital age, where millions of users are connected to the internet in many different ways, before this technological breakthrough with its insertion into everyday life of people, arose users using this practicality that the network in provides, this free and borderless environment for developing a new

¹ Acadêmica do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. Email: leocadioalice@hotmail.com

² Professor do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. Email: sandersson1@hotmail.com

modality delitiva, cyber crimes. Right before this paradigm, noted the need to regulate relations which began to develop in this virtual world or cyberspace, thus resulting in new laws that criminalize computer crime that despite some criticism is considering a major breakthrough for the Brazilian legislation. During this study will be addressed this new crime, cybercrime, this new type of criminal behavior perpetuated in cyberspace, will be raised peculiar characteristics of computer crimes, as well as an analysis of existing laws, but the law specifically 12 737 / 12 and Civil Rights Framework Internet .

Keywords: Cyber Crimes. Cyberspace. Law 12.737 / 12. Civil Rights Framework Internet.

1 INTRODUÇÃO

No mundo contemporâneo o chamado “mundo virtual” ou “ciberespaço”, que nada mais é do que o lugar onde as pessoas se interagem diariamente utilizando-se dos mais diversos meios computacionais, já conta com milhões de pessoas a ele conectadas por todo o mundo. O que antes era restrito a apenas alguns grupos sociais, se faz presente hoje em praticamente todos os ambientes, sendo usado por todos independente da classe social, idade, nível de intelectualidade.

A Internet já penetrou praticamente todos os âmbitos das nossas vidas, de forma que hoje dizemos que vivemos na era da informação. A web tem sido utilizada para inúmeras finalidades, seja para realizar negociações comerciais, buscar conhecimentos, conhecer pessoas, manter relacionamentos, produzir atividades, buscar diversões e em alguns casos, promover transtornos para outras pessoas, incluindo prejuízos financeiros das vítimas.

Portanto, não a como negar os benefícios que o uso da rede nos proporcionou e nos proporciona até hoje, a nossa vida se tornou mais prática, atividades que antes eram realizadas no lapso temporal muito longo, passaram a ser realizadas quase de forma instantânea. Sendo assim, é crescente o número de usuários da internet a cada ano que passa, e isso se justifica em virtude de tanta evolução tecnológica, assim como o barateamento dos computadores e dispositivos móveis de acesso á rede mundial.

Diante de todo esse paradigma e praticidade houve uma grande repercussão no âmbito do Direito Penal e Processual Penal, por não conseguir acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é exatamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, os chamados crimes cibernéticos.

Criminalidade essa desenvolvida por agentes que se aproveitam de tantas facilidades, de uma idéia aparente de anonimato e muitas vezes em virtude da fragilidade de normas, haja

vista que até 2012 a internet era isenta de qualquer regulamentação jurídica específica e em consequência disto tornou-se um meio apto para a ação de crimes e condutas danosas.

No decorrer desse trabalho será realizado uma análise das legislações vigentes que tipificam os delitos informáticos, em particular a Lei 12.737/12 e o Marco Civil da Internet e seus aspectos inovadores, tendo como base doutrinas, jurisprudências, artigos, códigos, pesquisas e comentários sobre crimes cibernéticos.

2 CONSIDERAÇÕES INICIAIS SOBRE A INTERNET E CIBERESPAÇO

O mundo virtual atualmente conta com milhões de pessoas conectadas em toda parte do planeta. Existindo serviços que são exclusivamente criados pela Rede Mundial de computador – a internet. É utilizada por todas as classes sociais, por pessoas de todas as idades, por setores públicos ou privados, e quase tudo que fazemos está direta ou indiretamente ligado a um computador.

Podendo assim dizer que estamos vivenciando a era digital e de certa forma a rede mundial de computadores contribuiu grandemente para o nível de globalização que se encontra o mundo. As redes informáticas se constituíram como nervos da sociedade, que cada vez mais depende dos computadores e das intranets (redes internas). E para melhor compreensão do tema é necessário conceituar dois pontos importante, o que é a internet e o que representa o ciberespaço.

Com o surgimento da internet como uma rede mundial de computadores criou-se um novo espaço para expressão, comunicação interpessoal e conhecimento. Porém, trata-se de um espaço que não é real, que não existe fisicamente, mas virtualmente, o ciberespaço. Entretanto, revela-se como um lugar verdadeiro onde coisas reais lá acontecem devido à prática de ações humanas reais, próprias e individuais, que são capazes de gerar relações jurídicas e que podem ter consequências muito específicas.

O segundo conceito conforme entendimento de Marcelo Crespo, “trata-se de uma ampla rede capaz de interligar computadores de todo o mundo, possibilitando, assim, a comunicação entre eles conhecido por internet” (CRESPO, 2011). A Internet deve ser entendida como a base técnica e operacional do ciberespaço que possui uma compreensão mais ampla que a Internet.

Nas lições de Kellen Cristina Bogo, define internet como sendo:

[...] internet pode ser entendida como “um conjunto de redes de computadores interligadas que têm em comum um conjunto de protocolos e serviços, de forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial”³. (BOGO, 2007, p.1)

Portanto o que hoje forma a Internet iniciou-se em 1966, quando algumas Universidades se uniram para desenvolver a Advanced Research Projects Administration-Administração de Projetos e Pesquisas Avançadas (ARPANET)⁴, criada pela ARPA, uma subdivisão do Departamento de Defesa dos Estados Unidos. Naquela oportunidade seu uso era exclusivo das Forças Armadas norte-americanas.

Seu propósito era promover um contínuo funcionamento daquela rede, mesmo em casos de calamidade como um ataque nuclear. Diante disto, era de suma importância não haver um comando central que pudesse ser alvejado. Este é o típico retrato do medo causado pela Guerra Fria, que dominava o mundo naquela época.

A ARPANET cresceu muito com a grande expansão de telefonia norte-americana. Porém, foi na década de 80 com a implantação do Protocolo de Controle de Transferência/Protocolo de Internet (TCP/IP)⁵ que efetivamente possibilitou o surgimento da internet. Esse protocolo é o responsável pela interligação dos diversos computadores, permitindo que atuem em grupo.

O tempo foi passando mais o princípio básico da internet não desapareceu. Até os dias atuais ela baseia-se na idéia de não se produzir comandos centrais tornando todos os pontos equivalentes, sendo assim, não importa onde esteja o computador, seja no Brasil, na França ou na China.

Diante de toda essa evolução fez com que as relações comerciais, as administrações Públicas e a sociedade em geral passassem a depender muito da eficiência e segurança da chamada tecnologia da informação. Grande parte das transações financeiras, no âmbito comercial é feita por computador. No empresarial, muitas empresas guardam eletronicamente seus arquivos. Os sistemas marítimos aeronáuticos e espaciais dependem em grande parte de sistemas informáticos modernos.

³ BOGO, Kellen Cristina. A história da Internet: como tudo começou. Disponível em:

<<http://kplus.cosmo.com.br/matéria.asp?co=11&rv=Vivencia>>. Acesso em: 08 de set. 2014.

⁴ Advanced Research Projects Agency Network - é idéia da construção de uma rede de computadores que pudessem trocar informações.

⁵ Toda vez que um computador conecta-se à uma rede recebe um número IP. Ele pode ser considerado um endereço e é representado por números e pontos. É o IP responsável, muitas vezes, pela identificação de um criminoso. Atualmente, devido ao grande número de computadores que tem acesso à internet, está sendo disponibilizado um IP com mais dígitos, a fim de que todos os computadores possuam a referida identificação.

Atualmente é possível acessar a Internet por microcomputadores incluindo notebooks, palm tops, celulares, TVs, tablets, etc. Podendo a conexão ser feita por linhas telefônicas fixas e móveis, por cabo, por satélite, por rádio e infravermelho.

2.1 A INTERNET NO BRASIL

Neste contexto a história da Internet no Brasil iniciou-se bem mais tarde, no início da década de 90, mais especificamente em 1991, com a Rede Nacional de Pesquisa (RNP), uma operação acadêmica subordinada ao Ministério de Ciência e Tecnologia (MCT). A RNP trouxe a Internet para o Brasil, com o objetivo de atender à conexão das redes de universidades e centros de pesquisas, mas logo as esferas federais e estaduais começaram também a se interligar.

Contudo, no dia 20 de dezembro de 1994, a Embratel apresentou o serviço experimental a fim de conhecer melhor a Internet. No ano seguinte em 1995, os Ministérios de Comunicações e de Ciência e Tecnologia abriram a Internet para operação comercial, e os provedores puderam contratar conexões com a RNP e, depois, com a Embratel. E finalmente, houve a abertura ao setor privado da Internet para exploração comercial da população brasileira.

Sendo assim, a RNP ficou responsável pela infraestrutura básica de interconexão e informação em nível nacional, tendo controle do backbone⁶. Hoje o Brasil possui diversos backbones interligando todos os Estados do país, bem como centenas de conexões com outros países.

3 CRIMES CIBERNÉTICOS

Diante os inúmeros benefícios que surgiram com a dissipação dos computadores e do acesso à Internet, surgiu conforme esse crescimento os crimes e criminosos especializados na informática, multiplicando-se por todo o mundo. Tais crimes possuem várias nomenclaturas e podem ser chamados de crimes cibernéticos, virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras terminologias.

⁶ Coluna dorsal de uma rede, o *backbone* representa a via principal de informações transferidas por uma rede, neste caso, a Internet.

Conforme entendimento de Deborah Fisch Nigri⁷, os crimes cibernéticos podem ser entendidos como aquele praticado contra o sistema de informática ou através deste, incluindo os crimes praticados contra o computador e seus periféricos e os realizados através do computador. Inserem-se nesta definição os delitos praticados através da internet, pois tem como pressuposto o acesso a rede, utilizando na maioria dos casos um computador.

Portanto os crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis contra ou praticadas com o emprego de sistemas da informática. Nas lições de Holanda Ferreira⁸, define-se computador como: “Máquina capaz de receber, armazenar e enviar dados e de efetuar, sobre estes, seqüências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas” (HOLANDA, 2000, p. 1016).

Os Crimes cibernéticos podem ser ainda definidos como sendo às condutas de acesso proibido a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autoria, incitação ao ódio e discriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, dentre outros.

Sendo assim, o Direito Penal enfrenta novas realidades quanto às práticas delitivas, de forma que não se pode ignorar a realidade de novos *modi operandi* e novas ponderações sobre condutas danosas. Para uma melhor compreensão deste assunto se faz necessário entender como se classificam os crimes cibernéticos, para identificarmos quais condutas são definidas como informática.

3.1 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Um dos grandes desafios relativo aos crimes cibernéticos é discorrer sobre sua classificação. Justifica essa dificuldade pelo grande número de autores com entendimentos divergentes que se aprofundam nessa questão.

É importante classificar os crimes digitais, pois é apartir daí que será possível a identificação de certas condutas ilícitas. Portanto diante de todas as classificações e vários entendimentos, será acolhida neste trabalho a menos complexa e mais adotada pelos autores dentre eles Vicente Greco Filho. Sendo assim, classificam-se as condutas ilícitas como: a)

⁷ NIGRI, Deborah Fisch. Crimes e segurança na Internet. **Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, 2000. p. 38.

⁸ HOLANDA, Aurélio Buarque Ferreira de. **Novo Dicionário de Língua Portuguesa**. 2. ed. Rio de Janeiro: Nova Fronteira, 2000.p.1016

condutas praticadas contra um sistema informático; b) condutas praticadas contra outros bens jurídicos⁹.

Portanto, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são classificadas como próprios. Ao passo que as demais condutas que se dirigem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

Depreende-se que os crimes virtuais próprios são aqueles em que o agente se utiliza especificamente do computador o sistema informático da vítima, no qual o computador como sistema tecnológico é utilizado como objeto e meio para prática do crime.

Ante o exposto, foi precipuamente neste sentido que, a Lei nº 12.737/12, inserindo o art. 154-A ao Código Penal (BRASIL. Lei nº 12.737, de 30 novembro de 2012), criou o delito de invasão de dispositivo informático, prevendo, assim, o chamado crime de informática próprio, isto é, aquele na qual a conduta ilícita tenha por objetivo exclusivo o sistema de computador. (BRASIL, Lei nº 12.965, de 23 de abril de 2014).

Nas lições de Marco Túlio Vianna os crimes informáticos próprios são “aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade dos dados ou informações”¹⁰. (VIANNA, 2003)

Ao passo que os crimes virtuais definidos como impróprios são aqueles praticados com a utilização do computador, ou seja, através da máquina que é usada como instrumento para a execução de condutas ilícitas que atinge bens jurídico já tutelados como crimes e que, portanto, já tipificados. Sendo assim, Marco Túlio Vianna classifica como crimes informáticos impróprios “aqueles em que o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico, inviolabilidade dos dados ou informações”¹¹(VIANNA, 2003)

Sendo assim, para identificar um crime como sendo de informática, é necessário uma análise inicial, primeiramente para verificar se o mesmo é um crime cibernético ou não, e depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado.

⁹ GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrin, São Paulo, Ed. Esp., ano 8. N. 95, out. 2000.

¹⁰ VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

¹¹ Idem

3.2 AS AMEAÇAS NA REDE MUNDIAL DE COMPUTADORES

De acordo com a Bitdefender¹², empresa de segurança na internet, em cada 15 segundos, um cidadão brasileiro é vítima de fraudes tendo seus documentos roubados ou informações furtadas na rede. No primeiro semestre deste ano foram criadas mais de 11 mil pragas virtuais para o Windows. Os prejuízos causados pelo cibercrime chegaram a 17,5 bilhões de dólares, segundo as estimativas do Fórum Systems. São roubos de identidade, fraudes, desvios de dinheiro, espionagem, chantagem¹³.

A maior parte dos crimes cibernéticos é feita através das redes sociais, o Brasil está entre os cinco países com maior assiduidade de ataques de Phishing. Entretanto, Existem várias possibilidades de se vitimar um computador, as técnicas mais aplicadas são através de e-mails, arquivos compartilhados e páginas da web infectadas.

Suas consequências também são as mais variáveis, algumas têm como instrução infectar computadores alheios para, em seguida, danificar seus componentes, seja excluindo arquivos, seja alterando o funcionamento da máquina ou até mesmo deixando o computador vulnerável a outros tipos de ataques.

No entanto existem aqueles que não têm o intuito de prejudicar a máquina, mas sim, seu usuário, como os softwares que têm como objetivo capturar informações sigilosas, como senhas e números de cartões de créditos para repassá-las para terceiros, causando graves transtornos às vítimas.

Sendo assim, dentre os modos desenvolvidos para se praticar crimes digitais com o uso de recursos da tecnologia como meio de ataque estão os Malwares¹⁴, os mais conhecidos são os seguintes.

3.2.1 Vírus

São pequenos programas de computador construídos para causar danos na máquina infectada, apagando dados, capturando informações ou alterando o seu funcionamento.

¹² **Baixe Bitdefender Antivírus e tenha um eficiente antivírus.** Disponível em: <<http://www.techtudo.com.br/tudo-sobre/bitdefender-antivirus.html>>. acesso em 09 de set. 2014.

¹³ A ERA da vigilância. Disponível em: <<http://info.abril.com.br/infosmb/edicoes/001/18-1.shl>>. Acesso em 09 de set. 2014.

¹⁴ Termo geralmente aplicado a qualquer software desenvolvido para causar danos em computadores

O nome vírus vem da grande semelhança que estes programas têm com os vírus biológicos, pois, depois de infectar um computador, ele se instala em um programa e o usa como hospedeiro para se multiplicar e se disseminar para outros computadores¹⁵.

Podem agregar-se a quase todos os tipos de arquivos. Podendo exibir apenas mensagens ou imagens, sem danificar arquivos da máquina infectada, mas consumindo a capacidade de armazenamento e de memória ou diminuindo o desempenho do computador infectado.

Os usuários dos sistemas operacionais da Microsoft são as principais vítimas dos vírus, já que esses sistemas são os mais usados no mundo, existindo para este sistema vários tipos diferentes de vírus. Até algum tempo atrás, a contaminação era feita através do compartilhamento de arquivos em disquete, mas atualmente a internet é o seu principal meio de propagar a contaminação atingindo milhares de computadores em poucos minutos. Os métodos mais comuns são através de e-mails, comunicadores instantâneos e páginas html infectadas.

3.2.2 Vermes (ou Worms)

É um programa auto-replicante, assim como o vírus, porém a principal diferença entre eles é a forma de se propagar, que pode ocorrer rapidamente para outros computadores, pela net ou por redes locais, tirando cópias de si mesmo em cada computador.

É um programa completo e não precisa de um hospedeiro para entrar em ação, como o vírus. Primeiro, ele controla os recursos que permitem o transporte de arquivos e informações, e logo após o verme se desloca sozinho para outros computadores. Em alguns casos possibilitam que a máquina infectada seja controlada remotamente, ou seja, que um terceiro leia arquivos acesse contas, exclua programas, espione intimidades etc.¹⁶

3.2.3 Cavalo de Tróia

Também chamado de Trojan Horse, ou apenas Trojan, é um programa diferentemente dos vírus e dos vermes, não se duplica, alguns sendo até programado para se auto-destruir após algum tempo ou com algum comando do cliente. A infecção acontece através de

¹⁵ CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

¹⁶ Ib. Idem

arquivos anexos a e-mails, mensagens instantâneas, downloads, por CDs ou disquetes. O programa é quase sempre através de uma animação ou imagens pornográficas, mas é durante a exibição dessas imagens que o computador está sendo infectado¹⁷.

Sua função é abrir o computador para o ataque de um eventual invasor, passando para este o controle da máquina infectada.

De acordo com a cartilha do CERT, o cavalo de tróia.

É um programa, normalmente recebido como um “presente”(por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogos etc), que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são: instalação de keyloggers ou screenloggers; furtos de senhas e outras informações sensíveis, como números de cartões de créditos...alteração ou destruição de arquivos¹⁸.

3.2.4 Phishing

É uma espécie de golpe on-line de falsificação. O phishing funciona da seguinte forma: uma pessoa mal-intencionada envia uma mensagem eletrônica (pode ser um e-mail, um recado em uma página de relacionamento etc.) a outrem e, utilizando-se de pretextos falsos, tenta enganar a pessoa receptora da mensagem e induzi-la a fornecer informações como numero de cartões de créditos, senhas, dados de contas bancárias, ou ainda, instigar a baixar ou executar arquivos que permitam a futura subtração ou roubo de informações ou acesso não autorizado ao sistema da vítima¹⁹.

As identidades usadas nessas mensagens na maioria dos casos são de órgãos do governo como a Receita Federal ou Banco Central, ou ainda, Bancos, Empresas de cartões de créditos. Essas mensagens trazem links que direcionam para sites falsos, onde existem formulários que a vítima deve preencher com as informações solicitadas. O conteúdo preenchido no formulário é enviado ao criminoso, que se vale das informações em prejuízo da vítima.

¹⁷ WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **CRIMES CIBERNÉTICOS: Ameaças e Procedimento de Investigação**. 2. ed. São Paulo: Brasport, 2013.

¹⁸ CERT.br.Cartilha de Segurança para Internet. Disponível em: <HTTP://cartilha.cert.br>. Acesso em: 06 de set. 2014.

¹⁹ CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011

3.3 AUTORES E VÍTIMAS DOS DELITOS INFORMÁTICOS

Como já citado, há duas categorias de crimes virtuais: os próprios e os impróprios. Sendo que para cometer um delito denominado como impróprio não se faz necessário a verificação de grandes diferenças quanto o *modi operandi*. Em outros termos, embora mude a modo pelo qual se pratica a ação delitiva, é dispensável a necessidade de conhecimentos técnicos específicos.

Já no tocante as condutas ilícitas denominadas como próprios, dependem de conhecimentos específicos de computação. E aqui se enquadram os *hackers* simplesmente pelo fato de ser necessário um maior nível técnico para a realização de delitos classificados como próprios.

Muito sem tem destacado quando os *rackers* são citados como sendo sempre os vilões da rede, porém, não é certo o que se afirma, visto que, são varias as denominações identificadas como autores de condutas ilícitas, vejamos alguns.

3.3.1 Os hackers

Hackers é o nome genérico dado aos chamados “piratas” de computador, onde a melhor tradução para a referida expressão inglesa é “fuçador”. O conceito dado por um hacker²⁰ a tal palavra é no sentido daquele que invade sistemas em benefício próprio, obtendo dados e informações de terceiros (documentos, programas, músicas etc.), mas sem causar prejuízos.

Apesar de serem conhecidos como “criminosos virtuais”, nem todo *rackers* deseja o prejuízo alheio. Há aqueles que se dizem “*rackers* do bem”, pois eles invadem os computadores, mas alertam as vítimas da presença de um risco, aconselhando-a a procurar uma proteção mais efetiva.

Caso recente foi divulgado na mídia de um hacker que invadiu o site oficial do escritor Graciliano Ramos, autor de obras como “vidas secas” e destruiu um acervo de 14 anos de trabalho²¹.

²⁰ SPYMAN. Manual Completo do Hacker. 3. Ed. São Paulo: Book Express, 1999.

²¹ Site do escritos Graciliano Ramos é invadido por hackers e tirado do ar. Disponível em: <<http://g1.globo.com/pop-arte/noticia/2014/10/site-do-escritor-graciliano-ramos-e-invadido-por-hackers-e-tirado-do-ar.html>>. Acesso em: 15 de out. 2014

3.3.2 Os crackers

Os crackers são considerados por Marcelo Crespo como verdadeiros criminosos da internet. Este indivíduo usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos²².

São verdadeiras quadrilhas que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio de informática para causar prejuízos de milhares de reais, tanto para pessoas físicas, jurídicas órgãos públicos e etc.

3.3.3 Os carders

Os carders conforme lições de Marcelo Crespo são estelionatários típicos. São chamados dessa forma por realizarem compras pela rede utilizando cartões de créditos alheios ou gerados por programas de computador²³.

Esse tipo de agente criminoso invade os computadores das administradoras de cartões de crédito e subtrai os números dos cartões e dados dos usuários. Muitas vezes age em operação conjunta com os crackers, onde os crackers ficam responsáveis pelas invasões e roubos de números de cartões, enquanto os carders fazem as compras.

3.3.4 Os phreakers

Este indivíduo é o terror das companhias telefônicas, pois são especialistas em burlar sistemas de telefonia, fixa ou móvel²⁴. Os prejuízos são enormes e incalculáveis.

Esse agente usa seu conhecimento para fazer ligações gratuitas ou escutas telefônicas. Porém essas escutas não são aquelas colocadas em postes, nas ruas. Trata-se de mecanismos em que são usados computadores e, quando um telefone toca, o do phreakers também o faz, possibilitando a ele que ouça toda conversa. No entanto, a atividade deles não se limita somente a isso, eles ainda são capazes de fazer ligações sem pagar a conta.

²² CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011

²³ Ib. Idem.

²⁴ NOGUEIRA, Sandro D' Amato. **Crimes de informática**. 2ª. ed. Leme-SP: Bh Editora, 2009.

Quanto ao Sujeito passivo do crime, qualquer um de nós pode ser vítima, todos que tem acesso a rede mundial de computadores está arriscado a ser vitimizado dos crimes virtuais, isto porque, pode chegar via e-mails ou termos nosso computador invadido causando danos ou até mesmo termos dados e senhas furtados.

4 COMPETÊNCIA

A identificação do foro competente para processar e julgar um crime cibernético é feita através de uma análise das circunstâncias e o foro que o crime foi executado. Na internet não existe fronteiras, uma vez publicado algo ele terá repercussão mundial, sendo acessível em qualquer lugar. E devido o fato da rede ter um caráter internacional por ser aberta é que existem tantas problemáticas relativas à competência.

Conforme a nossa atual jurisdição processual penal de acordo com o art. 70 do código de processo penal, em regra, a competência é definida pelo lugar em que o crime for consumado, ou, na forma tentada, pelo lugar em que foi realizado o último ato de execução.

Já o artigo 6º do Código Penal nada mais é que a Teoria da Ubiquidade, que afirma que o lugar do crime é aquele em que se realizou qualquer dos momentos do *inter criminis*. Ocorre que o *inter criminis* dos crimes informáticos, via de regra, ocorrem em lugares distintos.

Sendo assim é possível encontrar a primeira problemática, pois nos crimes cometidos na internet existe uma enorme dificuldade das autoridades policiais para identificar o lugar em que se deu o crime. Visto que o agente que comete os crimes na maioria dos casos não utiliza o seu próprio dispositivo eletrônico para cometer a conduta ilícita e na grande maioria dos casos adota lugares públicos tais como shoppings, lan houses, universidades.

No processo investigatório é perceptível a utilização de dados e e-mails falsificados e até mesmo a propagação de vírus a fim de ocultar as condutas ilícitas.

A jurisprudência dos Tribunais Superiores já vem firmando entendimento, em alguns julgados, determinando diretrizes processuais no âmbito virtual. Neste sentido o Superior Tribunal de Justiça entendeu que a competência para processar e julgar crimes de racismo praticado na rede é o do lugar onde se originou as mensagens de caráter ofensivo racista, conforme previsto o art. 70 do CPP.

No entanto, caso a conduta seja praticada por diferentes agentes e em lugares diversos, mas contarem com o mesmo *modus operandi* restará caracterizado o nexa probatório, sendo

assim, a competência será do juízo que conheceu primeiro os fatos. Assim tem entendido o STJ conforme julgado²⁵ a seguir:

PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO PORINTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET. USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃO DESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO.

1. A competência para processar e julgar o crime de racismo praticado na rede mundial de computadores estabelece-se pelo local de onde partiram as manifestações tidas por racistas. Precedente da Terceira Seção.

2. No caso, o procedimento criminal (quebra de sigilo telemático) teve início na Seção Judiciária de São Paulo e culminou na identificação de alguns usuários que, embora domiciliados em localidades distintas, trocavam mensagens em comunidades virtuais específicas, supostamente racistas. O feito foi desmembrado em outros treze procedimentos, distribuídos a outras seções judiciárias, sob o fundamento de que cada manifestação constituía crime autônomo.

(...)

4. Caracterizada a conexão instrumental, firma-se a competência pela prevenção, no caso, em favor do Juízo Federal de São Paulo - SJ/SP, onde as investigações tiveram início. Cabendo a este comunicar o resultado do julgamento aos demais juízes federais para onde os feitos desmembrados foram remetidos, a fim de que restitua os autos, ressalvada a existência de eventual sentença proferida (art. 82 do CPP).

5. Conflito conhecido para declarar a competência do Juízo Federal da 9ª Vara Criminal da Seção Judiciária de São Paulo, o suscitante. (CC 116926 SP 2011/0091691-2 Relator(a): Ministro SEBASTIÃO REIS JÚNIOR, S3 - TERCEIRA SEÇÃO, DJe 15/02/2013). (BRASIL, 2011).

Portanto a competência para julgar os crimes cibernéticos em regra será da Justiça Estadual, somente será competência da Justiça Federal se for verificada uma das hipóteses previstas nos incisos IV e V do art. 109 da CF/88.

A constituição Federal determina a competência da Justiça Federal para julgar os crimes praticados em fronteiras e os demais crimes Federais. Também estabeleceu em seu art. 109, inciso IV, competência aos juízes federais para julgar as infrações praticadas em detrimento de bens, serviços ou interesses da União ou de suas entidades autárquicas ou empresas públicas. Sendo assim, compete a Justiça Federal julgar os crimes cibernéticos contra a Administração Pública.

²⁵ BRASIL. Tribunal Superior de Justiça. Conflito de competência : cc 116926 sp 2011/0091691-2. Relator Sebastião Reis Júnior. Terceira Seção DJe 15/02/2013. Disponível em: <<http://stj.jusbrasil.com.br/jurisprudencia/23052425/conflito-de-competencia-cc-116926-sp-2011-0091691-2-stj>>. Acesso em: 08 de out 2014.

Por fim, conforme o art. 109, inciso V, da Constituição Federal determinou a estes juízes federais o julgamento de crimes pronunciados em tratados ou convenção internacional, quando a infração tiver início no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.

5 ANÁLISE DA LEI 12.737/12

Diante a nova era digital alguns fatores tais como relacionamento na rede, transações bancárias, o aumento do comércio eletrônico deram impulso ao crescimento de ocorrências de crimes cibernéticos. Até 2012 não havia em nosso ordenamento jurídico regramento específico para proteger novos bens jurídicos violados quando cometidos na rede.

É importante salientar que já é pacífico na doutrina o entendimento de que há bens jurídicos tutela no direito penal que são violados e que a internet é utilizada apenas como instrumento para o êxito da prática da conduta delituosa na internet. No caso a internet é utilizada para a prática de um crime já tipificado no Código Penal.

Assim leciona o doutrinador Luiz Flávio Gomes:

[...] os crimes informáticos dividem-se em crimes contra o computador e crime por meio do computador, em que este serve de instrumento para atingimento da meta optada. O uso indevido do computador ou de um sistema informático (em si um fato “tipificável”) servirá de meio para a consumação do crime-fim.²⁶ (ARAS, 2001, p.1)

Portanto, os crimes que já possuem tipificação legal e por consequência, bem jurídico protegido pelo Código Penal, com a internet, ficaram percebidos apenas como uma nova instrumentalização da modalidade delitiva. É o caso dos crimes contra honra: calúnia, injúria e difamação e estelionato, que independente do instrumento utilizado para o êxito da conduta já possuem tipificação legal. Este é inclusive o entendimento dos tribunais superiores, entre eles o Superior Tribunal de Justiça.

Entretanto, novas condutas que violam os direitos e garantias da coletividade e que não são bens jurídicos protegidos pela nossa legislação como dano informático, violação ao dispositivo informático entre outros, pela falta de previsão, quando ocorria alguma violação a esses bens não havia como ser punidos. Tendo em vista não ser permitido no direito penal

²⁶ **Crimes de Informática.** Uma nova criminalidade. Disponível em: <<http://jus.com.br/artigos/2250/crimes-de-informatica>>. Acesso em 15 de out. 2014.

tipificação por analogia em prol do princípio da legalidade, conforme exposto na CF, em seu art. 5º, XXXIX “Não há pena sem lei anterior que o defina, nem pena sem prévia cominação legal”.

Porém, essa inércia do legislado foi quebrada com o advento da lei 12.737/12 com cognome dado pela mídia de “Lei Carolina Dieckmann”, sob o título Invasão de Dispositivo Informático. Foi sancionada pela presidente Dilma Rousseff no dia 30/11/2011, sem veto, com publicação no DOU dia 03/12/12 e entrou em vigor após 120 dias de vacância no dia 02 de abril de 2013.

Contudo, a lei assim que entrou em vigor já foi apontado como alvo de muitas críticas pela doutrina. Talvez por ter sido criada durante um período de grande pressão social devido o episódio envolvendo a atriz global Carolina Dieckmann que teve seu e-mail invadido e suas fotos íntimas divulgada na rede, e até aquele momento não havia previsão legal dessas condutas na legislação.

Sendo assim a lei 12.737/12 dispõe sobre a tipificação criminal de delitos informáticos, acrescentando dois artigos o 154-A E 154-B ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Os bens jurídicos por ela tutelados são a intimidade, a vida privada e o sigilo de dados constantes de dispositivo informático.

A ação típica descrita no caput do artigo 154-A dispõe na seguinte forma:

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. (BRASIL. Lei nº 12.737, de 30 novembro de 2012, 2012).

Depreende-se do texto legal duas finalidades que não são cumulativas, primeiramente é a conduta de invadir dispositivo informático, mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações. A segunda é com relação a invadir dispositivo informático para instalação de vulnerabilidades para obter vantagem ilícita.

A primeira análise levantada neste artigo é com relação à conceituação (não expressa pelo legislador) do objeto material do delito, a expressão “dispositivo informático”. Segundo entendimento de Mirabete e Fabbrini entende-se por dispositivo “qualquer aparelho, mecanismo ou componente construído para uma função especial”; enquanto informática “é a

ciência que estuda o tratamento da informação mediante o uso de computador ou outros dispositivos de processamento de dados”²⁷ (MIRABETE; FABBRINI, 2014).

Sendo assim infere-se que dispositivo informático, no tipo em exame é qualquer sistema ou aparelho que viabiliza, por meio eletrônico, o armazenamento, processamento ou transferência de dados ou informações. Portanto abrangem neste conceito os computadores de qualquer espécie, tais como computadores domésticos, notebooks, tablets, aparelhos celulares, etc., seus componentes e periféricos.

É importante destacar que para configuração do ilícito penal o dispositivo informático tem que ser alheio, ou seja, de titularidade de terceiro (pessoa distinta daquela que figura como sujeito ativo da conduta). Assim como, é explícito na lei, a irrelevância do dispositivo estar ou não conectado à rede.

Ainda neste contexto, outro ponto polêmico a ser discutido é com relação ao verbo do tipo “invadir” que conforme lição de Mirabete e Fabbrini é entrar, ingressar, penetrar em seu software de forma a ter acesso ao conteúdo informatizado, de qualquer natureza, como o sistema operacional, sistemas ou aplicativos, bancos de dados, e-mails, documentos, senhas e etc.²⁸

O núcleo do tipo, invadir, pressupõe a utilização de força, artimanha, violação indevido de mecanismo de segurança, desrespeito à vontade do proprietário do equipamento, ultrapassar o limite de autorização fornecida pelo titular do equipamento. É o tipo comissivo, em que o agente realiza a conduta proibida.²⁹

É notório que conforme redação do novo artigo só restará configurada o delito se o agente acessar o sistema de informática à força, seja na hipótese de a invasão ocorrer mediante acesso online, pela internet ou outra rede, como também mediante o acesso físico direto do agente a dispositivo informático.

Ainda neste sentido, para configuração do tipo penal a ação de invadir está vinculada no tipo à violação indevida de mecanismo de segurança. Portanto, exige-se que o dispositivo esteja dotado de algum aparato, físico ou não, instalado com intuito de evitar o acesso não autorizado ao seu conteúdo, como chaves, senhas, antivírus e etc., e que a invasão supere esse mecanismo de proteção.

Conforme lições de Rogério Greco:

²⁷ MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**: Parte Especial arts. 121 a 234-B do CP. 31. ed. São Paulo: Atlas, 2014.

²⁸ *Ib.* Idem.

²⁹ Lei Carolina Dieckmann - Lei nº. 12.737/12 art. 154-a do Código Penal. Disponível em: <<http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal>>. Acesso em: 16 de out 2014.

Por mecanismos de segurança podemos entender todos os meios que visem garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de login e senhas que visem identificar e autenticar o usuário, impedindo que terceiros não autorizados tenham acesso às informações nele contidas. Entendemos que essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto pelo art. 154-A do diploma repressivo quando, também, mesmo indevidamente, ingresse em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois que inexistente.³⁰ (GRECO, [201-?], p.2)

Sendo assim, se o agente invadir um dispositivo e o mesmo não tiver nenhum mecanismo de segurança (mesmo sem mecanismo de segurança não é dado a ninguém o direito de invadir computador alheio, a não ser que tenha permissão expressa ou tácita do proprietário), será o indiferente penal. Portanto, será afastado da tutela jurisdicional o dispositivo desprotegido, assim mantido por desejo do titular, por desinteresse, negligência ou mesmo falta de informação, não adotou ele qualquer cautela para evitar aquele acesso.

Portanto para a configuração da conduta presente no tipo penal, é fundamental o dolo, a consciência de agir indevidamente. Exige-se também, como elemento subjetivo do tipo que o agente atue com uma das finalidades previstas no texto legal, ou seja, visando a obtenção, a adulteração ou a destruição de dados ou informações existentes no dispositivo sem expressa autorização do titular.

A segunda finalidade proposta pelo caput do artigo em comento é com relação à invasão do dispositivo para instalação de vulnerabilidade. Conforme nos ensina Mirabete e Fabbrini instalar vulnerabilidade é inserir ou infiltrar algum mecanismo ou programa capaz de tornar o conteúdo do dispositivo mais suscetível a acessos não autorizados ou a ações que permitam a inserção, alteração ou destruição de dados³¹. São exemplos mais conhecidos de vulnerabilidade os vírus, cavalo de tróia e etc.

Vulnerabilidade pode ser ainda entendida segundo o Centro de Estudos, Respostas e Tratamento Incidentes de Segurança no Brasil:

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração

³⁰ GREGO, Rogério. **Comentários sobre o crime de Invasão de Dispositivo Informático Art. 154-A do Código Penal**. [201-?]. Disponível em: <<http://www.rogeriogreco.com.br/?p=2183>>. Acesso em: 16 out. 2014.

³¹ MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal: Parte Especial** arts. 121 a 234-B do CP. 31. ed. São Paulo: Atlas, 2014.

de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.³² (GRECO, p. 2)

Ainda neste contexto a exigência especial de obter vantagem ilícita, restrita a segunda figura típica (instalar vulnerabilidade), deve ser entendida como qualquer vantagem obtida em contrariedade a normas legais, ainda que não seja um ganho patrimonial. Sendo assim, se o agente invade o dispositivo com o propósito de destruir informações por mero espírito competitivo de obter dados do titular do dispositivo por pura curiosidade ou desejo de bisbilhotar e etc., será considerada um fato atípico para o Direito Penal.

No tocante ao § 1º, incriminan-se as ações nele descritas por serem viabilizadoras ou facilitadoras da prática do crime de invasão de dispositivo informático. Dispõe assim da seguinte forma: “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”.

Portanto, o legislador pátrio teve o intuito de equiparar tais condutas àquelas tipificada no caput, buscando-se incriminar, desta forma, a conduta daquele agente que desenvolve, difunde, distribui de forma gratuita ou onerosa o software malicioso. Fatos que a princípio não passariam de meros atos preparatórios.

Com relação ao § 2º majorou a pena base do delito, caso de a invasão resultar prejuízo econômico, essa causa de aumento refere-se exclusivamente ao disposto no caput e § 1º do art. 154-A, punindo a lei mais severamente quando a invasão atingir a esfera patrimonial. Sendo assim, “Entende-se por prejuízo econômico aquele que resulta em perda material ou financeira. Desta forma, se o prejuízo for exclusivamente de caráter moral, não haverá incidência dessa causa de aumento”³³.

O § 3º dispõe que, “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, a pena-base será a de reclusão, de seis meses a dois anos, e multa, se a conduta não constituir crime mais grave”.

³²GRECO, Rogério. **Comentários sobre o crime de Invasão de Dispositivo Informático Art. 154-A do Código Penal**. [201-?]. Disponível em: <<http://www.rogeriogreco.com.br/?p=2183>>. Acesso em: 16 de out. 2014.

³³ Novo crime: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: <vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em: 16 de out. 2014.

O parágrafo acima citado traz conduta típica qualificada, ou seja, com um preceito secundário exclusivo, diverso do caput. O primeiro resultado descrito é a obtenção pelo agente do conteúdo de comunicações eletrônica privadas. Portanto, estão abrangidos os conteúdos de comunicação eletrônicas de todas as espécies como e-mails, mensagens de texto etc.

Ao exigir que a comunicação eletrônica seja privada, a lei não está se referindo ao conteúdo da mensagem, mas a natureza da forma de comunicação, que possibilita o envio da mensagem ao seu destinatário em caráter privado. Sendo assim, o crime não é qualificado na hipótese de se realizar a comunicação por meio que permita o acesso público ao seu conteúdo como, por exemplo, na hipótese de interceptação telefônica em virtude de ordem judicial para investigação e instrução criminal, na forma prevista na lei nº 9.296/96.

Qualifica o crime também, o acesso de segredos comerciais ou industriais, protegendo mais rigorosamente esses segredos pelo risco dos danos que a sua divulgação ou revelação podem causar ao seu titular. Com a mesma finalidade é prevista como resultado qualificador a obtenção de informações que são definidos por lei como sigilosas.

Em fim, a última circunstância qualificadora é a de lograr o agente o controle remoto³⁴ não autorizado do dispositivo invadido. A punição mais severa justifica-se pelo fato da instalação de um mecanismo, programa ou vírus que permita o controle do dispositivo à distância, possibilita que o agente monitore o acesso a conteúdo por tempo indeterminado, agravando-se a lesão ao bem jurídico tutelado.

Nos termos do parágrafo 4º, prevê uma causa de aumento de pena exclusivo para o crime previsto § 3º. Sendo assim a pena aumenta de um a dois terços se houver "divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, se o fato não constitui crime mais grave."

Por fim, no seu parágrafo 5º, do texto legal prevê causas de aumento para os casos em que a invasão de dispositivo informático incidir contra autoridade selecionada expressamente pelo legislador, quais sejam: Presidentes da República, do Superior Tribunal Federal, da Câmara, do Senado, das Assembléias Legislativas, Governadores, Prefeitos e dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

³⁴ Acesso remoto com manipulação de dados presentes em dispositivos informáticos, tudo feito a distância.

Conforme leciona Fernando Capez a tutela específica de maior gravame justifica-se por força dos cargos e funções públicas de alta relevância exercidos pelos agentes arrolados no § 5º (CAPEZ, 2013) ³⁵.

No texto do art. 154-B quis o legislador tratar Sobre o procedimento processual adequado na ação penal, a qual nesse tipo de crime, em regra, está condicionada a representação da vítima, salvo se o crime for cometido contra a administração pública.

A lei 12.737/12 também atingiu o artigo 266 do Código Penal, que este teve sua redação alterada/ampliada passando a versar sobre a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

A modificação referida no artigo 266 do CP se justifica pela inserção de um parágrafo primeiro ao texto legal, circunstância que ampliou a aplicabilidade do artigo, que passou a estabelecer: “§1º. Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.”

É importante para uma melhor compreensão, uma análise de forma pormenorizada das informações presentes no dispositivo supracitado. Conforme o advogado Rodrigo Alves Zaparoli³⁶:

Entende-se por serviço telemático aquele formado pela união de tecnologias de transmissão de dados proveniente de recursos das telecomunicações (v.g.: telefonia, satélite, fibras ópticas, entre outros) com recursos atrelados à informática (v.g.: computadores, softwares, entre outros), junção esta que permite o processamento e a transmissão de grande quantidade de dados em diversos formatos de modo instantâneo, destacando-se textos, sons e imagens. A título exemplificativo, podemos citar alguns *softwares* de destaque nesse segmento, são eles: *MSN*, *Skype*, *WhatsApp*, entre outros. (ZAPAROLI, 2013, p. 2)

Ainda com relação às modificações do artigo 266 do CP, a Lei nº 12.737/12 inseriu o parágrafo segundo ao dispositivo narrado, que apenas majorou a pena prevista em lei no caso do crime vinculado ao artigo 266 CP ter sido realizado por ocasião de calamidade pública. Na qual determina: “§ 2º. Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.”

A última alteração prevista com a nova legislação em comento atingiu o dispositivo 298 do CP que dispõe da seguinte forma: “Art. 298 - Falsificar, no todo ou em parte,

³⁵ CAPEZ, Fernando. **Curso de Direito Penal**. 13. ed. São Paulo: Saraiva, 2013.

³⁶ ZAPAROLI, Rodrigo Alves. Publicação de artigo jurídico. Juris way. Abril de 2013. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=10576>. Acesso em: 17 de out. 2014.

documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa.

Nesse caso o legislador pátrio fez uma simples ampliação ao artigo citado, pois equiparou a figura do cartão magnético bancário a um documento particular, nos moldes do que demonstra o parágrafo único inserido ao artigo 298 do Código Penal, na qual prevê: “Parágrafo único: Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.”

O legislador também se preocupou com a utilização de tecnologias incorporadas aos costumes da sociedade de forma a auxiliar o acesso do cidadão aos serviços das redes bancárias, equiparação o cartão magnético bancário, seja ele de débito ou crédito ao patamar de documento particular, viabilizando assim a aplicação da sanção prevista pelo artigo 298 CP.

Dessa forma, observa-se que apesar das falhas o legislador pátrio conseguiu um expressivo avanço com as alterações legislativas realizadas, pois conforme abordado no início do presente artigo jurídico, infelizmente a legislação não acompanhou na mesma proporção e velocidade as transformações da sociedade, situação esta que acaba causando verdadeira desarmonia entre a realidade vivida e o amparo legislativo que deveria acompanhá-la.

6 MARCO CIVIL DA INTERNET

O marco civil da internet - Lei 12.965/2014 é a demonstração de um avanço significativo para a legislação brasileira. Ainda não tínhamos em nosso ordenamento uma carta de direitos digitais, um estatuto dos usuários da internet, ficou conhecido como a “constituição da internet”.

Elaborado pelo ministério da justiça com sugestões da sociedade civil e da academia. O projeto de lei do marco civil da internet foi sancionado pela presidente Dilma Rousseff em 23 de abril de 2014 e converteu-se na Lei 12.965/14³⁷. A lei foi publicada no DOU em 24 de abril de 2014 e passou a vigorar após 60 dias de vacância em 23 de junho de 2014.

O Marco Civil da Internet dispõe de 32 artigos que tratam de princípios, garantias, direitos e deveres para o uso da Internet no nosso país, conforme estabelece em seu art. 4º,

³⁷ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 de out. 2014.

inciso I, que a disciplina do uso da Internet no Brasil que tem entre os seus objetivos, o de promover o direito de acesso à Internet a todos os cidadãos.

Os pontos principais do marco civil da internet baseiam-se na liberdade de expressão, a neutralidade da rede e a proteção a vida privada dos usuários. Com relação aos direitos fundamentais a liberdade de expressão e a proteção a vida privada não há nenhuma inovação, pois ambos já estavam consagrados na constituição 88 e em tratados como, por exemplo, no “Pacto de São José da Costa Rica”.

A novidade, portanto, é no tocante a neutralidade na internet e o regulamento estrito para o tratamento de dados pessoais no ciberespaço. Segundo o Idec (Instituto Brasileiro de Defesa ao Consumidor), a neutralidade na rede definiu-se como: “tratamento da navegação dos usuários na internet pelas operadoras de telecomunicações. A neutralidade é o princípio que determina que todos sejam tratados com igualdade, sem que haja benefício para uns e não para outros na hora de navegar ou que haja limitação para clientes específicos”³⁸.

Infere-se que o princípio da neutralidade determina que a rede deva ser igual para todos, sem distinção quanto ao seu uso. Sendo assim com a entrada em vigor do Marco Civil da Internet as operações das empresas que atuam na rede devem ser mais transparentes. Estabelece a proteção dos dados pessoais e a privacidade dos usuários, que só poderá ser disponibilizado mediante ordem judicial.

Outra inovação trazida pela lei 12.965/14 é a privacidade das comunicações. Tornou válido o sigilo de comunicação também para os emails, o que não ocorria até a sua entrada em vigor.

O Marco Civil da Internet ratifica a liberdade de expressão na rede garantida na constituição, no entanto, houve uma grande mudança com relação à retirada de conteúdos do ar. Antes de sua entrada em vigor, não havia uma regra clara sobre este procedimento, a partir de agora a retirada de conteúdos do ar só será feita mediante autorização judicial, com exceção dos casos de “pornografia de vingança”. Pessoas vítimas de violações da intimidade podem pedir a retirada de conteúdo, de maneira direta, aos sites ou serviços que estejam acolhendo este conteúdo.³⁹

³⁸ **Neutralidade da rede: entenda o significado e a importância do conceito.** Disponível em: <<http://www.idec.org.br/consultas/dicas-e-direitos/neutralidade-da-rede-entenda-o-significado-e-a-importancia-do-conceito>>. Acesso em: 18 de out. 2014.

³⁹ Marco civil entra em vigor. Pensando direito. Disponível em: <<http://www.cut.org.br/noticias/marco-civil-da-internet-entra-em-vigor-nesta-segunda-feira-23-35a2/>>. Acesso em: 18 de out. de 2014.

No mais o marco Civil da Internet está organizado e dividido em cinco capítulos na forma seguinte:

I- disposições preliminares

II- direitos e garantias do usuário

III- da provisão de conexão e de aplicações de Internet

IV- da atuação do Poder Público e

V- disposições finais.

A nova legislação tem como alvo promover os usos legítimos da Internet, via a proteção à intimidade dos usuários e à liberdade de expressão. Por fim o Marco Civil da Internet é um grande avanço para o regramento brasileiro, é um indicador de que o ciberespaço possui limites e nesse ambiente podem-se reclamar direitos sonegados ou violados e exigir a efetivação de deveres, sempre que estejam em discussão bens jurídicos fundamentais para a vida, na sociedade digital.

7 CONCLUSÃO

Conforme abordado neste artigo, a internet é considerada um grande avanço para a sociedade, e se tornou um instrumento de grande magnitude para a quebra de fronteiras e paradigmas, principalmente com relação ao acesso à cultura, à informação, à livre manifestação, assim como para a realização de negócios jurídicos, como compra, transações bancárias, vendas de produtos, anúncios etc.

Diante a grande evolução tecnológica surgiu também maliciosos que utilizam a tecnologia, em particular a internet, para a prática de condutas delituosas. Neste sentido o Direito Penal veio atuar com o objetivo de reprimir a criminalidade virtual. Era perceptível que a legislação brasileira não era suficiente para punir os crimes praticados através de dispositivos de informática, daí o surgimento da Lei nº 12.737/12, que passou a tipificar, na seara penal, a prática de infrações cometidas no ciberespaço.

Portanto, apesar da boa intenção do legislador, alguns dispositivos da nova lei falharam em sua qualidade técnica, em especial a redação dada ao caput do art. 154-A do CP, pela inércia do legislador em explicar conceitos básicos no tipo penal, assim como, por ter em seu verbo nuclear a expressão “invadir”, que significa entrar à força, o que não é a realidade do modus operandi de grande parte dos crimes virtuais, nos quais o agente se utiliza de artimanhas para obter êxito em seu desiderato criminoso.

No entanto, o legislador pátrio, apesar da morosidade no processo legislativo, agiu acertadamente e de maneira oportuna ao tipificar os delitos informáticos, representando a Lei nº 12.737/12 um avanço na legislação, que veio conforme a aflição social de evolução tecnológica, já que o mundo virtual criou um novo bem jurídico merecedor de tutela, o dispositivo informático.

Outro ponto importante e digno de comemoração foi a chegada do Marco Civil, pois a lei tem como objetivo a proteção dos direitos à intimidade, à liberdade de expressão e à neutralidade da Internet. O Marco Civil é também mais um indício de que o ciberespaço não é “terra-de-ninguém” e que neste espaço podem-se reclamar direitos sonegados ou violados, assim como exigir o cumprimento de deveres, sempre que estejam em questão bens jurídicos fundamentais para a vida, na sociedade digital.

E por fim cito uma frase que os antigos romanos já diziam: onde está o homem, aí está a sociedade; onde está a sociedade, aí está o Direito (*Ubi homo ibi societas; ubi societas, ibi jus*). Esta é uma imortal lição do jurista Ulpiano, que, tendo morrido em 223 d.C., jamais conheceu a Internet. Mas sabia navegar⁴⁰.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Juarez de Oliveira, 2006.

ARAS, Vladimir. **Crimes de Informática**: uma nova criminalidade. 2001. Disponível em: <<http://jus.com.br/artigos/2250/crimes-de-informatica/1>>. Acesso em: 15 out. 2014.

BOGO, Kellen Cristina. **A história da Internet**: como tudo começou. Disponível em: <<http://kplus.cosmo.com.br/matéria.asp?co=11&rv=Vivencia>>. Acesso em: 08 set. 2014.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 out. 2014.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal;

⁴⁰ Direito e Filosofia. Disponível em: <http://www.espacoacademico.com.br/017/17cmeireles.htm>. acesso em: 25 de out. 2014.

e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 08 out. 2014.

_____. Presidência da República – Casa Civil – Subchefia para Assuntos Jurídicos – Lei nº 12.737/12, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 15 out. 2014.

_____. Tribunal Superior de Justiça. Conflito de competência : cc 116926 sp 2011/0091691-2. Relator Sebastião Reis Júnior. Terceira Seção DJe 15/02/2013. Disponível em: <<http://stj.jusbrasil.com.br/jurisprudencia/23052425/conflito-de-competencia-cc-116926-sp-2011-0091691-2-stj>>. Acesso em: 08 de out 2014.

CAPEZ, Fernando. **Curso de Direito Penal**. 13. ed. São Paulo: Saraiva, 2013.

CERT.Br. **Cartilha de Segurança para Internet**. Disponível em: <<http://cartilha.cert.br>>. Acesso em: 06 set. 2014.

COMPUTADOR. In: Ferreira, Aurélio Buarque de Holanda. **Novo Dicionário de Língua Portuguesa**. 2. Ed. Rio de Janeiro: Nova Fronteira, 2000. p.1016.

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

DIREITO e Filosofia. Disponível em: <<http://www.espacoacademico.com.br/017/17cmeireles.htm>>. Acesso em: 25 out. 2014.

GRECO, Rogério. **Curso de Direito Penal: Parte Geral**. 14. ed. Niterói: Impetus, 2012.

GRECO, Rogério. **Comentários sobre o crime de Invasão de Dispositivo Informático Art. 154-A do Código Penal**. [201-?]. Disponível em: <<http://www.rogeriogreco.com.br/?p=2183>>. Acesso em: 15 out. 2014.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. **Boletim do IBCCrin**, São Paulo, Ed. Esp., ano 8. n. 95, out. 2000.

JESUS, Damásio de; MILAGRE, José Antonio. **Marco Civil da Internet: Comentários à Lei n. 12.965/14**. São Paulo: Saraiva, 2014.

MAGIO, Vicente de Paula Rodrigues. **Novo Crime**: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: <vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em: 16 out. 2014.

MARCO civil entra em vigor. Pensando direito. Disponível em:<<http://www.cut.org.br/noticias/marco-civil-da-internet-entra-em-vigor-nesta-segunda-feira-23-35a2/>>. Acesso em: 18 out. de 2014.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**: Parte Especial arts. 121 a 234-B do CP. 31. ed. São Paulo: Atlas, 2014.

NEUTRALIDADE da rede: entenda o significado e a importância do conceito. Disponível em: <<http://www.idec.org.br/consultas/dicas-e-direitos/neutralidade-da-rede-entenda-o-significado-e-a-importancia-do-conceito>>. Acesso em: 18 out. 2014.

NIGRI, Deborah Fisch. Crimes e segurança na Internet. **In Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, ano 4, n. 20, 2000.

NOGUEIRA, Sandro D' Amato. **Crimes de informática**. 2. ed. Leme, SP: BH, 2009.

O QUE É ARPANET. Disponível em: <<https://sites.google.com/site/sitesrecord/o-que-e-arpamet>>. Acesso em: 08 set. 2014.

SPOSITO, Rosa. A era da vigilância. **INFO SMB**, nov. 2014. Disponível em: <<http://info.abril.com.br/infosmb/edicoes/001/18-1.shl>>. Acesso em: 09 set. 2014.

SPYMAN. **Manual Completo do Hacker**. 3. ed. São Paulo: Book Express, 1999.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimento de investigação. 2. ed. São Paulo: Brasport, 2013.

ZAPAROLI, Rodrigo Alves. Publicação de artigo jurídico. **Juris way**. abr. 2013. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=10576>. Acesso em: 17 out. 2014.