Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS

FLÁVIO SILVEIRA DA SILVA

OS NOVOS CRIMES DE INVASÃO DE DISPOSITIVO INFORMÁTICO E INTERRUPÇÃO DE SERVIÇO TELEMÁTICO

Brasília
2014

FLÁVIO SILVEIRA DA SILVA

OS NOVOS CRIMES DE INVASÃO DE DISPOSITIVO INFORMÁTICO E INTERRUPÇÃO DE SERVIÇO TELEMÁTICO

Monografia apresentada como requisito parcial para a obtenção do título de Bacharel em Direito da Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília.
Orientador: Prof. Álvaro Chagas Castelo Branco

Brasília
2014

FLÁVIO SILVEIRA DA SILVA

OS NOVOS CRIMES DE INVASÃO DE DISPOSITIVO INFORMÁTICO E INTERRUPÇÃO DE SERVIÇO TELEMÁTICO

Monografia apresentada como requisito parcial para a obtenção do título de Bacharel em Direito da Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília.
Orientador: Prof. Álvaro Chagas Castelo Branco

Brasília, 30 de abril de 2014

Banca Examinadora

_____

Professor Me. Álvaro Chagas Castelo Branco
Orientador

_____

Professor Lásaro Moreira da Silva
Examinador

_____

Professor Dr. Jose Rossini Campos do Couto Corrêa
Examinador

A meu pai e irmãos, pelo carinho e incentivo nessa longa jornada.

À Lilian, cuja presença e paciência foram fundamentais para a elaboração desta obra.

AGRADECIMENTOS

Agradeço primeiramente ao professor Álvaro Castelo Branco, pelas valiosas contribuições e pela orientação durante a realização deste trabalho.

Agradeço também aos colegas de trabalho que acompanharam a jornada de uma segunda graduação, pelo apoio e pelas contribuições sempre bem-vindas, em especial, ao Agente de Polícia Federal Luciano Cardoso e aos chefes do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal, Delegado Carlos Sobral e Delegado João Vianey, pelo auxílio e discussões relacionadas à matéria pesquisada.

“Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no ar não- espaço da mente, aglomerados e constelações de dados. Como luzes da cidade se afastando...”

(William Gibson)

RESUMO

Apresenta o histórico do computador, bem como a criação e evolução da Internet e sua relação com o Direito. Define o conceito de delito informático, sua classificação e os bens jurídicos tutelados, chamando atenção para os problemas decorrentes da determinação do lugar do crime e da lei penal aplicável em crimes transnacionais. Discorre sobre alguns projetos de lei relacionados à tipificação de delitos informáticos, apresentando o contexto do tramitação do PL nº 2793/11, que se tornou a Lei nº 12.737/12. Conceitua certos termos e expressões empregados nos novos tipos penais, como, por exemplo, "dispositivo informático" e "mecanismo de segurança". Analisa o novo tipo penal de invasão de dispositivo informático, bem como a figura assemelhada de instalação de vulnerabilidade. Discorre sobre os elementos específicos do tipo, bem como sobre os problemas identificados na redação do artigo 154-A. Alerta quanto à pouca eficácia do tipo penal, decorrente dos problemas acima e das baixas penas cominadas. Analisa também o tipo penal de interrupção de serviço telemático do artigo 266, §1º, discorrendo se os bens protegidos pela norma seriam apenas os de caráter público e coletivo, como as redes de telecomunicação, ou também os de caráter privado, como os *sites* da *Web*.

Palavras-chave: Internet, Direito Penal, Delito Informático, Invasão de Dispositivo, Interrupção de Serviço Telemático, Lei nº 12.737/12

ABSTRACT

Presents the history of the computer as well as the creation and evolution of the Internet and its relationship with the law. Defines the concept of cybercrime, its classification and the protected legal interests, highlighting the problems arising from the determination of the place of crime and criminal law applicable to transnational crimes. Discusses some bills related to the definition of computer crime, presenting the context of the progress of the Bill No. 2793/11, which became Law No. 12.737/12. Conceptualizes certain terms and expressions used in new crimes, such as, "computing device" and "security mechanism". Analyze the new crime of breaking into computing device, and the similar crime of installation of vulnerability. Discusses the specific elements of the crime as well as the problems identified in the writing of Article 154-A. Warns about the ineffectiveness of the article derived from the problems above and low penalties prescribed. It also analyzes the criminal offence of interruption of telematic servisse of Article 266, §1, discussing if the legal interests protected by the Law would be only those public and collective, such as telecommunication networks , or also those of private domain, as Web sites.

Keywords: Internet, Criminal Law, Computer Crime, Break Into Device, Interrupt Telematic Service, Law No. 12.737/12

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ADSL	Asymmetric Digital Subscriber Line
ANATEL	Agência Nacional de Telecomunicações
ARPA	Advanced Research Projects Agency
CES	Consumer Electronics Show
CF	Constituição Federal
CGI	Comitê Gestor da Internet no Brasil
CNJ	Conselho Nacional de Justiça
ENIAC	Electronic Numerical Integrator and Computer
FEBRABAN	Federação Brasileira de Bancos
IBOPE	Instituto Brasileiro de Opinião Pública e Estatística
IP	Internet Protocol
MC	Ministério das Comunicações
MCT	Ministério da Ciência e Tecnologia
PJe	Processo Judicial Eletrônico
RNP	Rede Nacional de Pesquisa
TCP	Transmission Control Protocol
TJ	Tribunal de Justiça
TRT	Tribunal Regional do Trabalho
WWW	World Wide Web

SUMÁRIO

INTRODUÇÃO

O presente estudo trata de tema afeto à área de Direito Penal e sua relação com a informática, tendo em vista a Lei nº 12.737/12, de autoria do Deputado Federal Paulo Teixeira, que alterou o Código Penal, tipificando as condutas de invasão de dispositivo informático e interrupção de serviço telemático.

Esta Lei, de 30 de novembro de 2012, apresenta novidades quanto à tipificação de condutas classificadas pela doutrina como "crimes próprios" informáticos, que se refletirão nos procedimentos de investigação criminal e persecução penal.

Entretanto, antes mesmo de entrar em vigor, a Lei já colecionava várias críticas de profissionais do Direito e especialistas em informática, os quais apontavam desde o uso de termos ou expressões técnicas imprecisas até a questão das penas, consideradas por alguns como brandas e ensejadoras de impunidade.

É necessário analisar a nova Lei sob os pontos de vista técnico e legal, com a finalidade de determinar quais condutas estão abarcadas e quais condutas permaneceriam atípicas ou deveriam ser ajustadas a outro tipo penal existente.

A importância quanto à presente discussão resta comprovada, tendo em vista a contemporaneidade da Lei e os casos recentes de crimes cometidos por meio da Internet. A própria Lei passou a ser conhecida como Lei Carolina Dieckmann, por ter sido sancionada após crime cometido contra a famosa atriz de televisão.

Dessa forma, o estudo em tela tem como objetivo a interpretação e análise dos "novos" crimes de Internet definidos na Lei nº 12.737/12, quais sejam, a invasão de dispositivo informático e a interrupção de serviço telemático, com vistas a delimitar as condutas alcançadas pelos novos tipos, bem como os possíveis problemas para a persecução penal.

Para isso, adota-se como método de pesquisa o jurídico-dogmático, a fim de utilizar procedimentos de cunho instrumental para um melhor entendimento dos problemas

quanto à interpretação da Lei nº 12.737/12, recorrendo sempre que necessário à doutrina mais atual sobre o assunto.

No primeiro capítulo, o estudo se inicia discorrendo sobre os aspectos gerais relacionados ao tema, como, por exemplo, o surgimento dos computadores e da Internet, bem como a importância de tais invenções para a atual Sociedade do Conhecimento.

De forma sucinta, também são apresentados outros tipos de interação entre a informática e o Direito. É o caso da informatização do processo judicial, e dos serviços da administração pública disponíveis pela Internet, como por exemplo a entrega da declaração de imposto da renda para a Receita Federal.

A seguir, o segundo capítulo trata dos delitos informáticos, apresentando o conceito, bem como a classificação doutrinaria e bem jurídico tutelado. Nesse ponto, também é realizada breve discussão acerca do lugar do crime, tendo em vista a natureza desse tipo de delito, que possibilita ao criminoso praticá-lo à distância, inclusive estando em outro país.

Por fim, o terceiro capítulo discorre sobre os dois crimes trazidos pela Lei nº 12.737/12, quais sejam, a invasão de dispositivo informático e a interrupção de serviço telemático. Primeiramente, são apresentados alguns conceitos referentes aos termos e expressões utilizados na redação dos tipos penais, passando-se a seguir à análise dos tipos em comento.

1 ASPECTOS GERAIS

A informática atualmente é parte importante da vida em sociedade, especialmente com o advento e popularização da Internet. Utilizamos computadores para nos comunicarmos, estudarmos, para realizar compras ou outras transações financeiras e utilizar serviços oferecidos por empresas ou pelo governo.

No Brasil, o funcionamento da Internet é regulado pelo Comitê Gestor da Internet no Brasil - CGI.br, organização não governamental que conta com a participação de membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica.

Entretanto, essa regulação, por emanar de organização sem poder de polícia, e por tratar apenas dos aspectos técnicos da utilização da rede mundial, não possui natureza cogente, sendo insuficiente para coibir a atuação dos criminosos modernos.

Nada mais natural que as relações humanas estabelecidas por meio do computador também passassem a ser reguladas pelo Direito.

Com o advento da Lei nº 12.737/12, de 30 de novembro de 2012, foram tipificadas as condutas de invasão de dispositivo informático, como é o caso dos computadores, *tablets* e telefones celulares, bem como a interrupção de serviço telemático.

O caráter eminentemente tecnológico de tais condutas refletiu-se no texto da nova norma jurídica, com a utilização de termos ou expressões técnicas advindos da área de informática, o que, como veremos mais à frente, vem sendo alvo de críticas por parte de especialistas na matéria, devido à imprecisão ou ambiguidade resultantes.

Sendo assim, antes de iniciar o estudo jurídico dos novos tipos, faz-se necessário primeiramente apresentar o contexto histórico relacionado ao surgimentos dos computadores e da Internet, bem como definir os conceitos técnicos relacionados aos novos tipos penais. Com isso, será possível delimitar a abrangência de tais tipos, definindo de forma clara e inequívoca quais condutas estão abarcadas e quais ainda seriam consideradas atípicas.

1.1 O SURGIMENTO DOS COMPUTADORES

A sociedade atual tem na informação uma de suas principais riquezas. A popularização dos computadores, *smartphones* e *tablets*, bem como a Internet, contribuiu de maneira significativa para isso, pois possibilitou mais rapidez na difusão das informações em escala global.

A informação que antes demorava semanas para ser difundida, tendo em vista os meios tradicionais de comunicação, como jornais, revistas e cartas, passou a demorar dias, com o advento do rádio, televisão e telefone.

Atualmente, algo que aconteça em uma província distante da Síria passa a ser conhecido em todo mundo em questão de minutos.

Para a geração nascida no século XXI, é difícil imaginar a vida sem os computadores e a Internet. No início dos anos 90, por exemplo, uma simples transferência bancária ou consulta a saldo demandava o deslocamento do correntista à agência. A comunicação com pessoas localizadas em outros estados ou países também era algo difícil e caro.

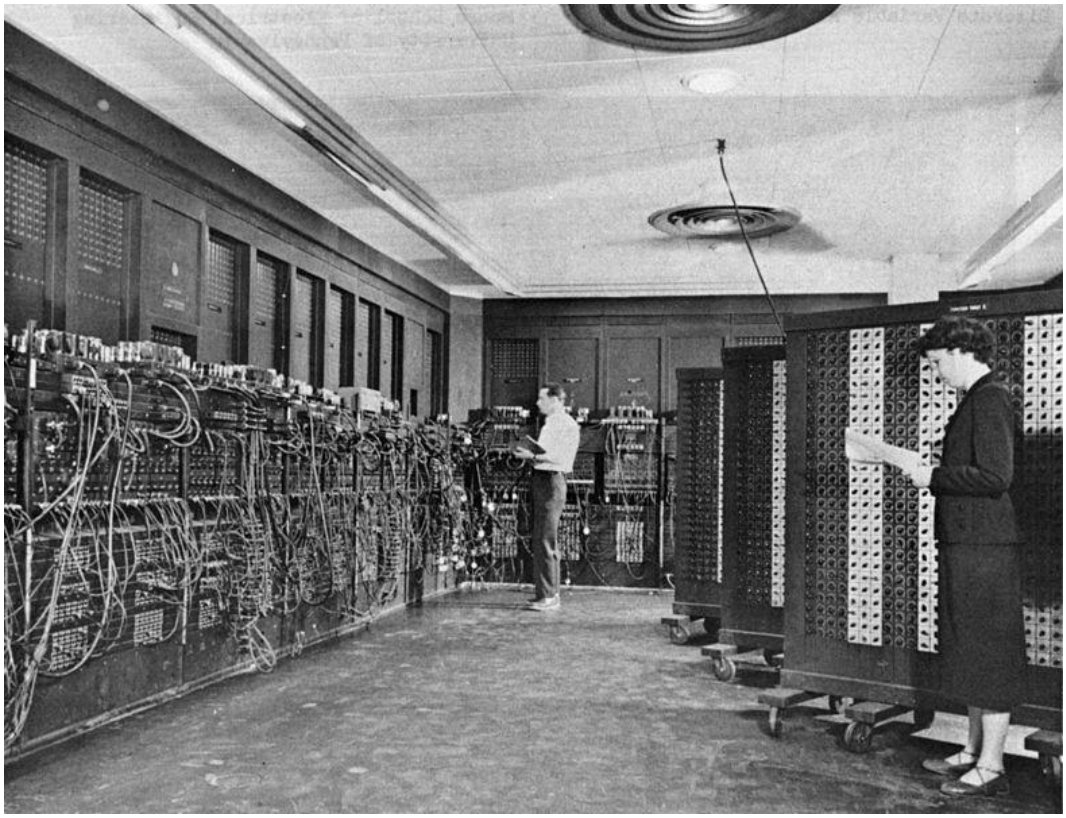
Mas, afinal, o que é um computador? Um computador nada mais é do que um dispositivo de propósito geral que pode ser programado para realizar uma sequência de operações lógicas ou aritméticas sobre um conjunto de dados de entrada (*input*), gerando uma saída (*output*). É o que conhecemos como processamento de dados. Geralmente, é composto pelas seguintes partes: dispositivos para entrada dos dados, como teclado e mouse; dispositivos para saída dos dados, como monitor e impressora; unidades de armazenamento persistente, como discos rígidos e ópticos (CDs, DVDs); memória e unidade central de processamento (FRAGOMENI, 1986, p. 125).

Não há como falar da história do computador sem relacioná-la ao ato de calcular (computar). Na Antiguidade, por exemplo, os cálculos eram realizados na contagem dos rebanhos e das colheitas, além de serem essenciais nas transações comerciais. Desde aquela época, o homem tem inventado dispositivos que o auxiliem na tarefa de calcular, como o ábaco, por volta de 3.500 a.C, e a calculadora mecânica de Pascal, em 1642 (COSTA, 1997; ROSSINI, 2004, p. 23-24).

Os computadores eletrônicos modernos surgiram apenas na primeira metade do século XX, impulsionados pelo advento da 2ª Guerra Mundial, com o objetivo de auxiliar no cálculo de trajetórias balísticas (CASTRO, 2003, p. 2).

O ENIAC (*Electronic Numerical Integrator and Computer*), construído em 1946, é considerado o primeiro computador digital eletrônico de propósito geral da história. O projeto foi desenvolvido por John Mauchly e John Presper Eckert da Universidade da Pensilvânia, e financiado pelo Exército norte-americano, custando aproximadamente quinhentos mil dólares (equivalente a seis milhões de dólares atuais). O computador possuía 17.468 válvulas e ocupava uma área de 180 m^2, pesando cerca de 30 toneladas. Sua velocidade, entretanto, era inferior à de uma calculadora atual (GUIA DO HARDWARE, 2011).

Figura 1 - O ENIAC em funcionamento



Fonte: http://en.wikipedia.org/wiki/File:Eniac.jpg

A evolução dos computadores geralmente é apresentada em gerações sucessivas, de acordo com os avanços tecnológicos. Segundo Gilberto Filho e Eduardo de Santana (2013, p. 10-16), existem cinco gerações de computadores:

- Primeira Geração (1946-1954): computadores como o ENIAC, que utilizavam **válvulas**, ocupando grandes dimensões. Devido ao uso de válvulas, apresentavam consumo elevado de eletricidade e geravam bastante calor. Com isso, as válvulas também queimavam com frequência, o que exigia reparos constantes.
- Segunda Geração (1955-1964): a válvula foi substituída pelo **transistor**. O transistor "revolucionou a eletrônica em geral e os computadores em especial", resultando em computadores menores, que "consumiam menos energia, geravam menos calor e eram mais rápidos e confiáveis".
- Terceira Geração (1964-1977): foi marcada pela criação e popularização dos **circuitos integrados,** feitos de silício. Esses circuitos, também conhecidos como **microchips**, permitiram o surgimento de computadores cada vez menores, já que um único circuito podia possuir centenas de transistores.
- Quarta Geração (1977-1991): nessa geração, presenciamos o surgimento dos processadores modernos, como os fabricados pela empresa INTEL, e de sistemas operacionais como MS-DOS, Windows e UNIX. Nessa fase, deu-se a popularização dos computadores pessoais, que se tornaram mais acessíveis ao usuário doméstico, por serem mais baratos, confiáveis e rápidos, e com uma maior capacidade de armazenamento. Também houve a expansão da Internet, devido ao surgimento da tecnologia WWW.
- Quinta Geração (1991 — ??): os computadores possuem processadores com milhões de transistores e discos rígidos com capacidade superior a 1 *terabyte* (1024 gigabytes). Essa geração foi marcada pela **inteligência artificial** e pela **conectividade à Internet**. Deu-se também o início da computação móvel, com o surgimento de *notebooks*, *palmtops* e telefones celulares.

Cada geração foi marcada por uma inovação, que rompeu com os paradigmas da geração anterior, permitindo construir computadores cada vez menores, mais rápidos e baratos. Embora muitos autores apresentem apenas as cinco gerações acima, poderíamos dizer que estamos vivenciando o início da Sexta Geração dos computadores.

Com a miniaturização dos componentes eletrônicos, temos em nossas mãos *smartphones* e *tablets* com poder de processamento superior ao de computadores de alguns anos atrás. Queremos que nossos dispositivos nos acompanhem onde estivermos, e se ajustem às nossas preferências e necessidades, atuando de forma mais inteligente. Além disso, queremos que estejam conectados entre si e à Internet, permitindo o controle e acesso de qualquer lugar do mundo.

Uma grande inovação dessa geração é a dos dispositivos vestíveis, como aponta a maior feira de produtos eletrônicos dos Estados Unidos, a *Consumer Electronics Show* – CES, realizada em janeiro de 2014 na cidade de Las Vegas (CAPANEMA, 2014). É o caso dos relógios de pulso inteligentes, os quais se conectam ao telefone celular e permitem a leitura de mensagens, realização de ligações e outros comandos sem tirar o telefone do bolso.

Outro exemplo é o dispositivo Glass, criado pela empresa Google, o qual possui o formato de óculos, apresentando em tempo real informações sobre o local onde o usuário está, além de permitir a realização de ligações telefônicas e tirar fotografias, tudo pelo comando de voz do usuário.

1.2 A REVOLUÇÃO DA INTERNET

Antes de apresentar o referencial teórico relativo aos crimes que serão objeto da pesquisa, dispostos nos artigos 154-A e 266 do Código Penal, é necessário também falar do contexto no qual tais crimes se inserem, já que, em muitos casos, estes são cometidos pela Internet.

O embrião do que hoje conhecemos como a Internet surgiu na década de 60, durante a Guerra Fria, como uma rede experimental de caráter militar desenvolvida pela agência norte-americana ARPA (*Advanced Research Projects Agency*), com o objetivo de

manter as comunicações dos Estados Unidos em funcionamento em caso de ataque do inimigo (COSTA, 2011, p. 22).

Por ter sido desenvolvida pela ARPA, a rede foi inicialmente chamada de ARPANET, e interligava instituições acadêmicas, como a Universidade da Califórnia e o Instituto de Pesquisa de Stanford, e órgãos do governo e forças armadas (SILVA, 2003, p. 22-23).

Posteriormente, a Rede passou a interligar outros países, e foi lançada comercialmente, o que contribuiu significativamente para o seu crescimento. Um dos fatores decisivos para a popularização da rede foi a invenção da tecnologia *World Wide Web* – WWW (teia de alcance mundial), ou simplesmente *Web*, por Tim Berners-Lee, em 1990 (CHACON DE ALBUQUERQUE, 2006, p. 18).

Embora para muitas pessoas Internet e *Web* sejam sinônimos, tal assertiva não se afigura correta. A *Web* é um serviço que funciona no âmbito da Internet, sendo, portanto, um subconjunto desta. Consiste basicamente na publicação de documentos denominados páginas *Web*, contendo texto, conteúdo multimídia (imagens, sons e vídeos) e hiperlinks. O acesso é realizado por meio de programas específicos conhecidos como *browsers* ou navegadores, como o *Internet Explorer* ou o *Mozilla Firefox*. Ao clicar em um hiperlink, o usuário é direcionado a outro documento e assim sucessivamente, ato este que é conhecido como “surfar” ou “navegar” na *Web* (WORLD WIDE WEB, 2014).

Já a Internet, grafada com inicial maiúscula, refere-se ao conjunto de redes de computadores geograficamente distribuídas, interligadas entre si, bem como aos serviços disponíveis por meio dessas redes.

Segundo Omar Kaminski (2005, p. 37), a Rede das redes é composta por milhares de redes de computadores e milhões de usuários individuais distribuídos pelo globo, não sendo possível mensurar suas dimensões, devido à inexistência de ponto central de controle e ao seu crescimento exponencial.

A Rede Mundial de Computadores chegou ao Brasil em 1988, por meio da Rede Nacional de Pesquisa - RNP, mas sua utilização era restrita a órgãos de governo e à comunidade acadêmica. Apenas no final de 1994, foi liberada a operação comercial da Internet no Brasil (CASTRO, 2003, p. 3).

A Norma nº 004/95-ANATEL, aprovada em 31 de maio de 1995 pela Portaria nº 148 do Ministério das Comunicações, é considerada o marco inicial do funcionamento da Internet comercial no Brasil e tinha por objetivo regular o uso de meios da rede pública de telecomunicações para o provimento e utilização de serviços de conexão à Internet (QUADROS, 2004, p. 237).

Tal norma define Internet como sendo o "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o '*software*' e os dados contidos nestes computadores".

O crescimento exponencial da Internet só foi possível graças à adoção de um conjunto padrão de protocolos de comunicação, denominado pilha de protocolos TCP/IP, o qual permitiu a conexão entre computadores de fabricantes e características distintas. Podemos comparar os protocolos TCP/IP a uma linguagem falada entre os computadores, que deve ser entendida pelo emissor e pelo receptor da mensagem, para que haja a comunicação (MARTINS, 2001, p. 168).

Para nos conectarmos à Internet, geralmente contratamos os serviços de entidades conhecidas como provedores de acesso, os quais podem ser pagos ou gratuitos. A conexão pode se dar de diversas formas, como, por exemplo, por meio de linha telefônica (discada ou ADSL), TV a cabo, satélite, rádio, 3G, entre outros.

Cada vez que você se conecta à Internet, seu provedor de acesso atribui ao seu computador um identificador único, conhecido como endereço IP, o qual é utilizado para o correto encaminhamento das mensagens destinadas e originadas de seu computador. Em um dado momento, não pode haver mais de uma máquina com o mesmo endereço IP conectada na Internet. Entretanto, tendo em vista a quantidade limitada de endereços IP, é comum que, em um dado momento, um provedor de acesso atribua um endereço IP a um computador, e após este se desconectar, o provedor atribua o mesmo endereço IP a outro computador.

Entre as características mais importantes da Internet, destacam-se a ausência de um controle central e a redundância de conexões e funções (TAKAHASHI, 2000, p. 133), o que faz com que ela seja altamente resiliente a problemas e tentativas de interrupção. Segundo Rita de Cássia Lopes da Silva (2003), "não há um único centro que governa ou

mesmo gerencia a Internet. As redes constituintes pertencem a alguma organização [...]". As decisões relativas à Internet dizem respeito principalmente a padrões tecnológicos a serem adotados, e não possuem força coercitiva.

Essa característica de descentralização, denominada "inteligência na periferia", constitui um dos principais traços da arquitetura da Internet, pois permite a criação de aplicações "de modo autônomo e desvinculado de mecanismo central que as aprove, certifique ou gerencie" (LUCERO, 2011, p. 44).

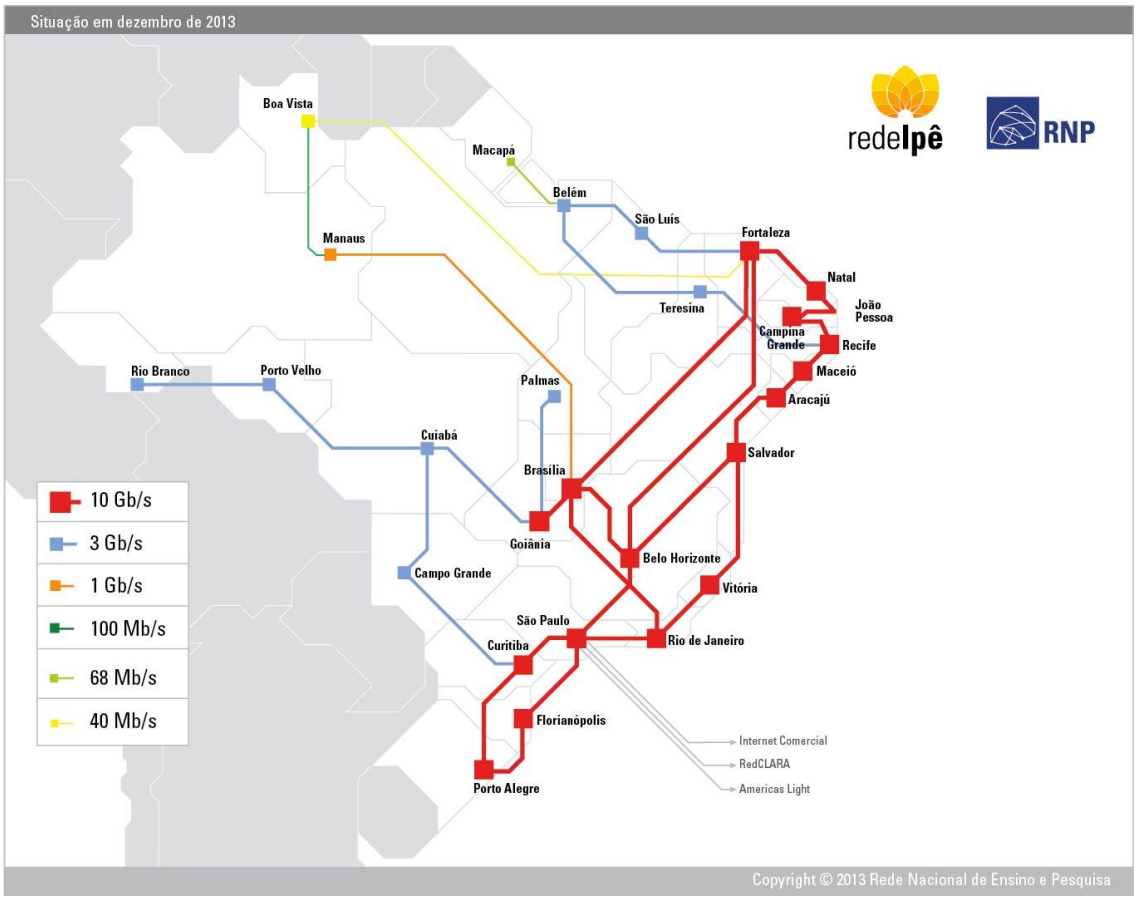
Em relação ao funcionamento da Internet, vale citar o disposto em Nota Conjunta emitida pelos Ministérios das Comunicações (MC) e da Ciência e Tecnologia (MCT) em maio de 1995, a qual estabelece que:

> "2.2 A Internet é organizada na forma de espinhas dorsais backbones, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.
> 2.3 Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da Internet no País.
> 2.4 Conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico.
> 2.5 Poderão existir no País várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada."

Podemos pensar nos *backbones* como autoestradas que ligam diferentes estados ou países, e que tem capacidade para suportar um enorme volume de tráfego. No Brasil, muitas empresas concessionárias possuem seu próprio *backbone*, como é o caso da Brasil Telecom e da Embratel (RESINA, 2006, p. 30).

Além destes, temos aqui no Brasil o *backbone* da RNP, presente em todas as 27 unidades da federação, que interliga as comunidades acadêmica e de pesquisa.

Figura 2 - Mapa do *backbone* da Rede Nacional de Pesquisa



Fonte: http://www.rnp.br/backbone/index.php

Desde então, observamos a popularização cada vez maior da informática e, principalmente, da Internet. Segundo pesquisa realizada pelo IBOPE (2013) com dados de dezembro de 2012, o Brasil ocupava a terceira posição entre os países em relação ao número de usuários ativos de Internet, com 52,5 milhões de internautas.

Muitos sistemas antes operados de forma manual passaram a ser informatizados, e a Internet, antes utilizada apenas como meio de comunicação, tornou-se um local para realização de transações comerciais.

Atualmente, as pessoas trocam mensagens instantaneamente com outras localizadas em outros estados ou até mesmo países. Além disso, as transações bancárias e a compra de mercadorias podem ser feitas com o mero apertar de um botão.

Segundo Moreira (2012), “a informática representa hoje o meio de comunicação típico e mais representativo da era globalizada”. Por meio da Internet, podemos

transmitir informações de um lugar para o outro com grande rapidez, encurtando as distâncias.

Alexandre Daoun (2001 apud COSTA, 2011, p. 51) constata, entretanto, que, além dos benefícios, a Internet "[...] também possibilitou novas ferramentas para as práticas criminosas, tanto as tradicionais, já tipificadas no Direito Penal positivo, quanto aquelas que necessitam de nova legislação [...]". Eudes de Oliveira Júnior e Pedro Oliveira (2013) compartilham de tal opinião:

> "O mundo moderno exige do direito um acompanhamento atento das mudanças ocorridas na sociedade, principalmente no que diz respeito à área da informática, que se encontra em constante evolução. Ocorre que tal evolução ao abrir caminho para novas conquistas também abre caminho para a prática de novos ilícitos. E é nessa vertente que o direito entra com o objetivo de construir barreiras sólidas contra a criminalidade virtual."

Como em qualquer meio de convívio social, com o passar dos anos a Internet também passou a presenciar condutas consideradas reprováveis, como a disseminação de vírus, envio de *spams*, invasão de sistemas, desfiguração de páginas, entre outros.

No início, muitas dessas ações eram realizadas por indivíduos com alto conhecimento da tecnologia, conhecidos como *hackers*, os quais eram motivados pela curiosidade ou pelo desejo de reconhecimento na sociedade. Com a utilização econômica da Rede, ocorreu a evolução do criminoso típico da Internet, o qual passou a ser motivado principalmente pelo lucro.

Observa-se o aumento no número de crimes cometidos por meio da Internet. Em notícia divulgada no site da Folha (GOMES, 2012), por exemplo, o prejuízo dos bancos com fraudes eletrônicas aumentou 60% de 2010 para 2011, passando de R$ 940 milhões para R$ 1,5 bilhão de reais, segundo a Federação Brasileira de Bancos - FEBRABAN. Entre os motivos para esse aumento, destacam-se a sensação de anonimato conferida pela Rede, a ausência de enquadramento legal de algumas condutas, o grau de complexidade envolvido e o caráter transfronteiriço dos crimes informáticos.

1.3 A INFORMÁTICA E OS REFLEXOS NO MUNDO JURÍDICO

Além dos reflexos vistos no campo do Direito Penal, os quais alcançam aquelas condutas de maior reprovabilidade, a popularização da informática também causou impactos em outras áreas do mundo jurídico.

É o caso, por exemplo, do desenvolvimento do Governo Eletrônico, no campo do Direito Administrativo, e da modernização do Judiciário com o processo judicial digital.

O Governo Eletrônico, segundo Luiz Fernando Martins Castro (2006, p. 327), consiste na mudança da atividade de governar, derivada dos novos meios de informação e comunicação que surgiram na segunda metade do século XX. Entre as características do Governo Eletrônico, temos o aperfeiçoamento da prestação dos serviços públicos, o tratamento da informação como riqueza pública e o alargamento do espaço democrático.

Uma definição mais abrangente é a de Jaqueline Maria Quadros (2004, p. 238), que define Governo Eletrônico como:

> "[...] a utilização, por parte do setor público, das novas tecnologias de informação e comunicação, em especial a Internet, para a prestação de melhores serviços, disseminação de informações, controle das contas públicas, redução de custos administrativos e ampliação das possibilidades de participação dos cidadãos na gestão pública".

Segundo Patrícia Peck Pinheiro (2013, p. 280), a Internet é um dos meios mais eficazes, não apenas para publicar as ações realizadas pelo governo, mas também como canal de comunicação entre governantes e cidadãos, em atenção aos princípios da publicidade dos atos públicos e probidade administrativa.

No Brasil, o Governo Eletrônico começou a se desenvolver no ano 2000, quando foi criado um Comitê Executivo com o objetivo de formular políticas, estabelecer diretrizes, coordenar e articular as ações de implantação do Governo Eletrônico.

Desde então, é cada vez maior a presença do Governo na Internet, seja em áreas como inclusão digital, prestação de serviços e divulgação de informações. Atualmente, o governo brasileiro já divulga por meio da Internet todas as compras realizadas, e oferece mais de 800 serviços *online* (PINHEIRO, 2013, p. 280).

Entre os serviços prestados pelo Governo Federal, merecem destaque aqueles relacionados à declaração de imposto de renda – pessoa física. Desde 1997, a Receita Federal passou a permitir a entrega da declaração pela Internet. Atualmente, por meio do portal eletrônico e-CAC[1], é possível, por exemplo, consultar a situação da declaração entregue, bem como obter cópia digital das declarações entregues em anos anteriores.

Temos também algumas iniciativas visando aumentar a transparência da gestão pública, permitindo o acompanhamento das atividades desenvolvidas pela Administração Pública pelo cidadão. É o caso do portal da Transparência do Governo Federal[2], lançado em novembro de 2004, para assegurar a boa e correta aplicação dos recursos públicos. Nesse sentido, a criação de uma nova modalidade de licitação denominada pregão eletrônico, instituído pela Lei nº 10.520/02, trouxe maior agilidade, economia e transparência na contratação de bens e serviços comuns (CRESPO, 2011, p. 43).

No âmbito legislativo, o *site* da Câmara dos Deputados possibilita ao cidadão o acompanhamento dos projetos de lei em tramitação na casa, bem como a participação em debates e fóruns de discussão *online*, visando incentivar a participação da sociedade no processo democrático.

Não podemos deixar de destacar as mudanças no processo eleitoral brasileiro, com o advento da urna eletrônica. Atualmente, o Brasil é o único país que possui votação eletrônica em todo o território nacional, o que permite determinar o resultado de uma eleição de forma mais ágil que a tradicional votação em papel (PINHEIRO, 2013, p.280).

O poder Judiciário também se beneficia do processo de informatização, em atenção ao princípio da celeridade processual e do acesso à justiça. Entre as mudanças proporcionadas pelas novas tecnologias, destaca-se a progressiva implantação do processo judicial eletrônico, regulamentado pela Lei nº 11.419/06.

Desde o advento desta norma, admite-se o uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais, em processos civil, penal e trabalhista, bem como nos juizados especiais, em qualquer grau de jurisdição.

---

[1] https://cav.receita.fazenda.gov.br
[2] http://www.portaltransparencia.gov.br

No *site* do Superior Tribunal de Justiça[3], define-se processo eletrônico como aquele no qual todas as peças processuais (petições, certidões, despachos, etc.) foram digitalizadas em arquivos para visualização por meio eletrônico, não havendo utilização de papel.

Segundo levantamento realizado pelo Conselho Nacional de Justiça (CNJ), até a metade do ano de 2013, o Processo Judicial Eletrônico (PJe) já contava com quase 200 mil usuários ativos, entre juízes, serventuários da Justiça, advogados e peritos, e estava em funcionamento em mais de 590 varas espalhadas pelo país, e em 31 tribunais, incluindo todos os Tribunais Regionais do Trabalho (TRTs) e os Tribunais de Justiça (TJs) de Pernambuco, Paraíba, Mato Grosso, Minas Gerais, Rio Grande do Norte, Roraima e Rio Grande do Sul (MOURA, 2013).

[3] http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=1013#1

2 OS DELITOS INFORMÁTICOS

Os computadores e, em especial, a Internet revolucionaram o processo de disseminação e democratização da informação, em uma escala nunca antes alcançada pelos meios de comunicação tradicionais, como jornais, rádio e televisão. A Rede Mundial, antes destinada apenas ao uso acadêmico, passou a ter grande relevância econômica após a permissão da exploração comercial, com o surgimento dos mais diversos serviços *online*, como é o caso do comércio eletrônico e do *home banking*.

Como toda ferramenta criada pelo homem, estas também passaram a ser utilizadas para a consecução de atividades danosas, como a disseminação de vírus de computador, as pichações de *sites* e as mensagens difamatórias enviadas por *e-mail*.

Para Spencer Toth Sydow, (2013, p. 53-54), a capacidade de mudança inerente à tecnologia da informação faz com que a sociedade atual seja vista como uma sociedade de risco *sui generis*, onde a informática é meio hábil para a prática de quaisquer condutas que violem bens jurídicos protegidos.

Marcelo Crespo (2011, p. 35), entretanto, afirma que essa ideia de "sociedade de riscos", desenvolvida pelo sociólogo alemão Ulrich Beck, deve ser interpretada com ressalvas, já que as sociedades, em qualquer época, sempre foram "de risco" e o que há, atualmente, são novos paradigmas.

De início, se argumentava quanto à impossibilidade de regulamentação externa de tais condutas, devido ao caráter descentralizado e anárquico da Internet, sem comando central. Acreditava-se na capacidade autorregulatória da Rede e de seus usuários. Também afirmava-se quanto à impossibilidade de um processo de criação legislativa voltado aos conflitos informáticos, já que a rede seria apenas um meio para a prática de velhas condutas ou um novo lugar para velhas práticas associativas (GÓIS JÚNIOR, 2005, p. 183).

Segundo Rossini (2004, p. 127), havia "[...] relutância em se permitir a intervenção do Estado na Internet, não somente com a aplicação do Direito Penal, mas de todo e qualquer ramo da Ciência do Direito", pois acreditava-se na existência da mais absoluta forma de liberdade na Internet, a qual deveria ser preservada.

Essa intervenção, antes de ser uma afronta ao princípio da liberdade de expressão, tornou-se imperiosa, na medida em que a rede se tornou terreno para a prática de variados crimes (COSTA, 2011, p. 34), o que gerou reflexos uniformes em diversos países, com a edição de normas que adaptavam certas condutas ao ordenamento Penal já existente ou criavam novos tipos penais (ROSSINI, 2004, p. 32).

O Direito Penal, de forma sucinta, pode ser definido como o ramo jurídico responsável pela seleção dos comportamentos humanos mais graves à coletividade e prejudiciais à convivência social, bem como pela cominação das sanções apropriadas (CAPEZ, 2010, p. 19).

Tendo em vista seu caráter de *ultima ratio*, com a possibilidade de privação do direito à liberdade de um indivíduo, o Estado deve obedecer a certos princípios limitadores para exercer seu poder punitivo, com destaque para o principio da legalidade ou reserva legal, consagrado pela expressão *nullum crimen, nulla poena sine lege*. Segundo esse principio, nenhum fato pode ser considerado crime e nenhuma sanção pode ser cominada se não existir lei anterior que assim defina (BITTENCOURT, 2010, p. 41).

Como bem preceitua Fernando José da Costa (2011, p. 33):

> "A conduta reprovável pela sociedade, quando devidamente tipificada pelo direito penal como criminosa, resvala na esfera dos direitos protegidos pela norma, desafiando punição estatal. Trata-se de uma resposta legal do Estado à pratica criminosa. Mesmo na internet a conduta reprovável pela sociedade deve continuar protegida pelo Estado."

Entre as condutas lesivas praticadas, algumas já existiam antes do advento dos computadores, ou seja, o bem jurídico já encontrava-se tutelado, sendo a informática utilizada apenas como meio. Nesses casos, os tipos penais já existentes em nosso ordenamento jurídico poderiam ser imediatamente aplicados, ou serem adaptados de acordo com as peculiaridades de cada conduta.

Outras condutas, entretanto, careciam de legislação específica, por afetarem bens como a integridade das informações armazenadas ou a segurança de um sistema ou rede de computador, não podendo ser punidas, devido a vedação da analogia *in malam partem* (CRESPO, 2011, p. 37). Essa carência foi parcialmente suprida com a edição da Lei nº

12.737/12, que tipificou os crimes de invasão de dispositivo computacional e interrupção de serviço telemático, os quais serão estudados mais à frente.

É tarefa do poder Legislativo regular o uso, punir o abuso e traçar diretrizes para se alcançar segurança na informática, cabendo à sociedade e aos entes governamentais e privados a efetivação de medidas de prevenção e de programas visando o uso adequado deste meio de comunicação, para que se alcance a almejada segurança (COSTA, 2011, p. 29).

Além das iniciativas legislativas individuais de cada Estado, ganham importância os acordos de cooperação e tratados internacionais, tendo em vista o caráter transnacional dos crimes informáticos.

Uma iniciativa nesse sentido foi a Convenção sobre o Cibercrime, firmada no âmbito do Conselho da Europa em 2001, na cidade de Budapeste. O teor da Convenção sugeria um rol de delitos a serem tipificados pelos países signatários, como, por exemplo, violações de direito autoral, fraudes relacionadas a computador, pornografia infantil, entre outras, bem como os procedimentos de Direito Processual necessários à persecução penal.

Embora o Brasil não seja signatário desta Convenção, há uma concordância por parte de nossos doutrinadores de que os tratados e a cooperação internacional são o caminho a ser seguido para uniformizar o combate à criminalidade informática, tendo em vista a diferença de costumes entre os povos e a inafastável soberania dos Estados (DAOUN, 2006, p. 134; ROSSINI, 2004, p. 235; GÓIS JÚNIOR, 2005, p. 188).

2.1 CONCEITO

Na literatura, este tipo de delito recebe diferentes alcunhas, denotando assim uma ausência de uniformidade por parte de nossos doutrinadores. Sendo assim, outros autores podem chamá-los de “crimes digitais”, “cibernéticos”, “de computador” ou “de informática”, “crimes de Internet” ou “virtuais”, entre outros (CRESPO, 2011, p. 47).

Neste trabalho, utilizaremos a expressão “delitos informáticos” ou de informática, por não se restringir apenas aos computadores, e por levar em consideração todo o campo da informática e não apenas a Internet.

Atualmente, além dos computadores tradicionais, existem diversos tipos de dispositivos com capacidade de processamento de dados, os quais podem ser utilizados para a prática de delitos, como, por exemplo, *smartphones* e *tablets*. Com certeza, outros tipos de dispositivo surgirão nos próximos anos, tendo em vista as características da tecnologia da informação, razão pela qual o termo "delito informático" é o mais adequado para denominar este tipo de conduta.

Cumpre ressaltar que o gênero "delito informático" denota toda conduta praticada por meio de ou contra dispositivo informático, estando este conectado ou não a uma rede de computadores. Dentro do grupo de delitos informáticos, temos os delitos telemáticos, que são praticados por meio de um dispositivo conectado a uma rede de computadores, sendo este canal de comunicação necessário para a consecução da conduta, como meio ou alvo da ação (ROSSINI, 2004, p. 110).

Quanto ao conceito de delito informático, Carla Rodrigues Araújo de Castro (2003, p. 9) define ser "[...] aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador".

Augusto Rossini (2004, p. 110) vai mais além e define "delito informático" como sendo:

> "[...] aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade."

A professora Ivete Senise Ferreira (2001, p. 210), com excepcional clareza e objetividade, define crime informático como sendo "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

2.2 BENS JURÍDICOS TUTELADOS

Bens (ou objetos) jurídicos, na teoria do Direito Penal, são todos aqueles valores da vida humana mais caros à sociedade, os quais, devido a sua maior importância,

merecem proteção pelo Direito, já que possuem um sentido social próprio, anterior à própria norma penal incriminadora (BITENCOURT, 2010, p. 306).

Esse é um conceito do Direito Penal Moderno, visando assegurar e, ao mesmo tempo, limitar a atuação do ramo mais radical do Direito, de forma que a criação de novos tipos penais seja a última alternativa de intervenção do Estado (ROSSINI, 2004, p. 125).

Assim, segundo Marcelo Crespo (2011, p. 56), temos as condutas que atingem os valores já protegidos por nosso ordenamento jurídico, como a vida, o patrimônio, a fé pública, bem como as condutas cujo alvo são as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

Nas condutas praticadas antes do advento dos computadores, é evidente que o bem jurídico atingido será o mesmo já protegido na norma penal, pois a informática nesses casos é utilizada apenas como meio para a prática da conduta. Sendo assim, uma publicação de mensagem difamatória em um *site* atinge a honra, enquanto o furto de valores da conta corrente de um individuo, realizado por meio da Internet atinge o patrimônio.

Quanto aos "novos" crimes informáticos, que se dirigem contra um sistema informático ou rede de computadores, pode-se pensar, a principio, que não é possível identificar o bem ou interesse tutelado, devido à diversidade de condutas possíveis.

Tal dificuldade decorre do fato de tais condutas terem como objeto material um dispositivo ou sistema informático, bem como uma rede de computadores, e, por conseguinte, os dados e informações intangíveis ali armazenados ou transmitidos.

Augusto Rossini (2004, p. 129), em seu estudo sobre os crimes telemáticos, afirma existir um bem jurídico permanente nesse tipo de conduta, o qual chama de "Segurança Informática", cuja existência é independente dos bens jurídicos individuais e coletivos presentes numa conduta típica praticadas pela Internet.

O autor, em consonância com o preâmbulo da Convenção sobre o Cibercrime de Budapeste, estabelece que esse bem jurídico é composto por três elementos: "integridade" (a informação deve ser fidedigna e completa), "disponibilidade" (a informação

deve estar disponível ao usuário no momento que este necessite) e “confidencialidade” (a informação só deve ser acessível aos usuários autorizados).

A afronta a cada um desses elementos pode trazer sérios prejuízos à instituição proprietária ou detentora daquela informação, bem como aos demais usuários. Esses prejuízos podem ser tanto financeiros, quanto para a imagem e credibilidade da instituição, razão pela qual muitos crimes informáticos ainda não são comunicados às autoridades policiais competentes.

A modificação não autorizada de um documento, como, por exemplo, uma sentença publicada em diário de justiça eletrônico, é uma afronta à integridade da informação.

A disponibilidade da informação é o elemento atingido no caso dos ataques de negação de serviço contra *sites* da Internet. Para as instituições bancárias, por exemplo, esse tipo de ataque traz prejuízos da monta de milhares de reais, já que enquanto o *site* estiver indisponível, os correntistas não poderão realizar transações *online*.

Por fim, o acesso e divulgação não autorizados de determinada informação constituem grave afronta à confidencialidade, como por exemplo, nos episódios de espionagem informática divulgados recentemente, envolvendo a Agência de Segurança Nacional norte-americana – NSA.

Marcelo Crespo (2011, p. 57) afirma que o meio de prática das condutas não deve ser o único aspecto levado em consideração, “[...] devendo se constituir em torno da afetação da informação como bem jurídico protegido, primordial e basicamente, ainda que não de forma exclusiva”.

Sendo assim, segundo o mesmo autor, é necessário se pensar em novos paradigmas sobre os bens jurídicos dos delitos informáticos, visto que esses crimes são pluriofensivos, na medida em que “[...] há a proteção de bens jurídicos tradicionais, mas, ao mesmo tempo, proteção de novos interesses derivados da sociedade de risco e de informação”.

Sabemos que a informação constitui uma das maiores riquezas da sociedade contemporânea, razão pela qual esta é conhecida como a Sociedade da Informação ou do Conhecimento. Nos dispositivos informáticos, a informação encontra-se armazenada ou pode

ser transmitida para outros dispositivos, sendo essencial que se garanta a sua integridade, confidencialidade e disponibilidade, caso contrário, ela não teria valor algum.

Por conseguinte, conclui-se que a informação é o bem jurídico tutelado nos crimes cometidos contra os sistemas e dispositivos informáticos, e redes de computadores, informação esta que deve ser protegida em seus três aspectos elementares, quais sejam, integridade, confidencialidade e disponibilidade.

2.3 CLASSIFICAÇÃO

Os crimes informáticos geralmente são classificados pela doutrina de acordo com a natureza do bem jurídico ofendido. Existem condutas que não existiam antes do surgimento da informática, que tem como alvo o próprio dispositivo ou sistema informático, como é o caso das invasões de sistemas, dos ataques de negação de serviço contra *sites* e das modificações não autorizadas de sistema de informações por funcionário público.

Já em outros casos, a informática é utilizada apenas como um outro meio para a consecução do crime, o qual atinge bem jurídico diverso, muitas vezes já tutelado pelo ordenamento jurídico, como, por exemplo, quando alguém publica uma mensagem difamatória contra outra pessoa em uma rede social ou *blog*, ou no compartilhamento de imagens contendo pornografia infantil pela Internet.

Segundo a professora Ivete Senise (2001, p. 211), esse tipo de crime, onde a informática é utilizada apenas como meio, consiste na "[...] utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à liberdade individual, à honra, ao patrimônio publico ou privado, etc".

Augusto Rossini (2004, p. 122) classifica os delitos informáticos em:

> "Delitos Informáticos Puros, aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, sendo que a informática é composta principalmente do 'software', do 'hardware' (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. A conduta (ou ausência dela) visa exclusivamente ao sistema informático do sujeito passivo [...]. São exemplos [...] as condutas dos 'hackers' e 'crackers' - ainda não tipificadas no Brasil [...]. E há os Delitos Informáticos Mistos, em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático. Alguns de seus exemplos são o estelionato, a ameaça e os crimes contra a honra [...]."

De maneira mais concisa, Rita de Cassia (2003, p. 60) propõe uma classificação que será a adotada no presente trabalho:

> "Os crimes informáticos comuns (impróprios ou impuros) seriam todos aqueles crimes que possam ser considerados tradicionais e que tenham sido realizados, opcionalmente, com a utilização do computador, como meio para a sua prática. Por outro lado, as ações lesivas, tendo o sistema informático como objeto material, são os crimes informáticos autênticos (ou próprios) que se dirigem aos dados armazenados."

Os crimes impróprios, portanto, encontram-se tipificados, não demandando alterações em nosso ordenamento jurídico. Contudo, alguns doutrinadores defendem a necessidade de adaptações legislativas, visando agravar a pena de tais condutas quando praticadas por meio da informática, e, em especial, da Internet, tendo em vista o maior potencial lesivo proporcionado pela Rede Mundial de computadores.

Por outro lado, os crimes próprios, como os que serão objeto de estudo neste trabalho, muitas vezes permaneciam impunes, devido à quase inexistência de tipos penais específicos e à divergência do Judiciário quanto à classificação de tais condutas nos tipos existentes.

Antes das alterações trazidas pela Lei nº 12.737/12, tais condutas já eram observadas com frequência, como, por exemplo, nos recentes ataques a *sites* do Governo brasileiro, ocorridos no ano de 2012. Na ocasião, alguns *sites* foram invadidos ou pichados, passando a exibir mensagens de protesto inseridas pelos criminosos. Outros *sites* tiveram seu serviço interrompido por ataques de negação de serviço, impedindo o acesso dos usuários legítimos.

A necessidade de legislação específica para o assunto, tanto na esfera penal quanto na processual penal, era opinião compartilhada por muitos especialistas da área, entre os quais destacamos Gabriel Inellas (2009, p. 10) e Augusto Rossini (2004, p. 251).

Segundo Rodrigo Colares (2002), havia "[...] ilícitos perfeitamente enquadráveis no Código Penal pátrio e legislação extravagante, quais sejam aqueles em que a Internet, ou outro ambiente eletrônico, informático ou computacional, é tão-somente o seu meio de execução, estando a tipificação perfeita ao ato proferido [...]". Entretanto, para o autor:

> "[...] há aquelas condutas em que o objeto da ação lesa direito relativo a bens ou dados de informática e estes em sua maioria não encontram tipificação em nosso ordenamento jurídico; são os chamados crimes informáticos, nada obstando que um crime informático seja perpetrado pelo meio eletrônico – o que, aliás, corriqueiramente acontece. É o caso do acesso indevido de hackers a computador de terceiro, que atualmente não encontra amparo criminal, mas às vezes se tenta qualificar, para esfera cível, como invasão de privacidade; em que se pese, existem opiniões contrárias."

Sendo assim, o presente estudo tratará da análise crítica de dois delitos classificados como crimes próprios, quais sejam, a invasão de dispositivo informático e a interrupção de serviço telemático. Esses crimes, como veremos no próximo capitulo, atingem de forma imediata dispositivo informático ou serviço telemático, respectivamente, e de forma mediata, a informação como bem jurídico tutelado pelo Direito Penal.

2.4 LUGAR DO CRIME

O lugar dos delitos informáticos, bem como a lei penal aplicável, são pontos de grande debate entre os estudiosos e juristas, em decorrência das próprias características deste tipo de delito, que não respeita fronteiras físicas, sendo muitas vezes transnacional. Essa discussão envolve não apenas elementos do Direito Penal, mas também aqueles do Direito Processual Penal (ROSSINI, 2004, p. 171).

Quanto ao lugar do crime, podemos ter os delitos informáticos a distância e os delitos plurilocais. No primeiro caso, os atos de execução ocorrem em um país e o resultado se dá em outro, enquanto no segundo caso, os atos de execução e o resultado ocorrem em locais diferentes de um mesmo país.

Dessa forma, o correto entendimento do lugar de um crime informático é fundamental para determinar a lei penal aplicável, se de um país ou do outro, bem como a competência territorial para conhecer e julgar os delitos telemáticos.

Sabemos que a aplicação da lei penal no Brasil decorre primariamente do princípio da territorialidade, conjugado com o princípio da soberania, ou seja, no território brasileiro se aplica a lei penal vigente em nosso país. Entretanto, em determinadas situações, a lei penal de um país pode alcançar ações praticadas fora de seu território (BITENCOURT, 2010, p. 198).

O Brasil adotou, para a aplicação da lei penal no espaço, a teoria pura da ubiquidade, consagrada no art. 6º do Código Penal, segundo a qual considera-se o crime praticado no lugar onde se deu a conduta, bem como no lugar do resultado, ou ainda no lugar do bem jurídico atingido (BITENCOURT, 2010, p. 202).

Por força dessa teoria, vários países podem se julgar competentes para julgar um crime informático de caráter transfronteiriço, o que pode levar a conflitos de jurisdição de difícil solução, sendo necessário, então, coordenar os esforços relativos à investigação, julgamento e punição de tais crimes (CHACON DE ALBUQUERQUE, 2006, p. 64-65).

No caso dos crimes informáticos, devemos também levar em consideração a ideia de ciberespaço.

Segundo Kaminski (2005, p. 40), apresentando definição da Unesco, o ciberespaço pode ser visto como um ambiente artificial, criado pelo homem com o uso da tecnologia, onde é possível se expressar, transmitir informações e realizar transações econômicas. É composto por dois elementos, um subjetivo e outro objetivo. O elemento subjetivo consiste nas pessoas de todos os países, todas as culturas e linguagens e todas as idades e profissões, que fornecem e requisitam informações. O elemento objetivo, por sua vez, consiste na rede global de computadores interconectados por infraestruturas de telecomunicações, que possibilitam que essas informações fornecidas e requisitadas sejam processadas e transmitidas digitalmente.

De forma resumida, é possível conceituar ciberespaço como um ambiente virtual, palco de relações jurídicas das mais diversas, que rompe com a concepção tradicional de território. Nesse ambiente, pessoas localizadas em diferentes países, sujeitas a diferentes ordenamento jurídicos, podem se relacionar de forma instantânea.

Quando tais relações constituem ilícitos penais, como então determinar a lei penal aplicável e a competência territorial, haja vista que o criminoso praticou a conduta por meio do ciberespaço?

Esse aparente conflito entre o princípio da territorialidade do Direito Penal e a ausência de fronteiras do ciberespaço é esclarecido por Augusto Rossini (2004, p. 172), para quem:

> "A pessoa humana que se insere no Ciberespaço para a prática de ilícitos penais, apesar de interagir no espaço virtual, ocupa um espaço físico, absolutamente concreto e palpável, o mesmo espaço que é ocupado por qualquer outro ser vivo na face da Terra. Pode-se afirmar que 'a pessoa não é virtual'."

Entretanto, pode ser tecnicamente impossível determinar em que lugar os dados se localizavam, antes de serem alterados, já que os dados podem trafegar por diferentes países, não se podendo precisar o lugar onde as consequências ou os efeitos do crime se tornaram manifestos pela primeira vez (CHACON DE ALBUQUERQUE, 2006, p. 65).

Além disso, tendo em vista a facilidade em se criar perfis e contas de *e-mail* falsos pela Internet, geralmente é muito difícil determinar imediatamente a verdadeira identidade de um usuário do ciberespaço, já que estes são conhecidos apenas por um apelido (*nickname*), endereço de *e-mail* ou perfil de rede social.

Como, então, localizar e punir um criminoso que se insere nesse ambiente virtual para a prática de crimes contra outros usuários ou sistemas informáticos?

Para tentar determinar o endereço no mundo real de um usuário da Internet, quando este comete um crime informático, é necessário primeiramente obter o endereço IP utilizado por seu computador durante a conexão. Como já explicado anteriormente, cada vez que nos conectamos na Internet, nosso provedor de acesso fornece um endereço IP que passa a identificar o dispositivo (computador, *tablet*, *smartphone*, etc) durante aquela conexão.

Após a prática de um delito pela Internet, o endereço IP do criminoso muitas vezes ficará guardado em registros de acesso do computador da vítima, no caso dos delitos próprios, ou do sistema utilizado como meio para a consumação do crime, no caso dos delitos impróprios. Sendo assim, o primeiro passo durante uma investigação de crime informático consiste em obter o endereço IP utilizado pelo criminoso.

Quando um usuário divulga mensagem ofensiva à honra de outrem, por exemplo, por meio de um serviço localizado em outro país, como é o caso das redes sociais Facebook e Twitter, pertencentes a empresas norte-americanas, faz-se necessário requisitar a preservação e fornecimento do endereço IP do autor da mensagem por meio de carta rogatória ou outros mecanismos de cooperação internacional, o que infelizmente demanda bastante

tempo, colocando em risco a eficácia da investigação (CHACON DE ALBUQUERQUE, 2006, p. 67).

Para piorar, temos casos mais complexos, onde um crime é praticado parcialmente em diversos países. Uma pessoa localizada nos Estados Unidos, por exemplo, pode invadir um computador na França e utilizá-lo como intermediário para invadir outro computador no Brasil, transferindo os dados obtidos para um servidor em Hong Kong, com o objetivo de auferir vantagem ilícita.

Considerando a volatilidade dos vestígios digitais, que podem se perder em um curto intervalo de tempo, e sua importância para a investigação dos delitos informáticos, reputa-se urgente o aperfeiçoamento dos mecanismos de cooperação internacional, especialmente quanto à celeridade na preservação e fornecimento de dados relacionados a uma investigação em andamento, bem como ao auxílio para a produção de provas (CRESPO, 2011, p. 118).

Quando o criminoso está no Brasil e se utiliza apenas de sistemas, redes e serviços estabelecidos em nosso país, em tese tudo se torna mais simples. Nesse caso, basta que se oficie à autoridade judiciária competente, para que determine ao provedor de acesso ou à empresa responsável pelo serviço que informe os dados de registro referentes aquele endereço IP.

Entretanto, devido à natureza de funcionamento da Internet, não é possível prever o caminho que os dados irão tomar e quais os servidores serão utilizados para que uma mensagem chegue a seu destino (COSTA, 2011, p. 131).

Quanto às regras de competência territorial, o art. 70 do Código de Processo Penal determina que a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução. Já a competência no caso de infrações de menor potencial ofensivo, pelo art. 63 da Lei nº 9.099/95 será a do lugar em que for praticada a infração penal.

O lugar de consumação do crime, pela regra do art. 70 do CPP, deve ser determinado de acordo com o tipo de crime, se material, formal ou de mera conduta. No caso dos crimes materiais, considera-se consumado o crime no lugar onde se produziu o resultado.

Já os crimes formais e de mera conduta, que não dependem da efetivação de resultado externo, se consumam no lugar onde foi praticada a infração (ROSSINI, 2004, p. 177).

Embora não faça parte do escopo do presente trabalho, cumpre ressaltar que a regra processual de competência quanto ao lugar onde se produziu o resultado, no caso do crimes materiais cometidos pela Internet, pode conduzir a investigações ineficientes, já que em muitos casos o autor do crime estará localizado em cidade diversa da vítima, dificultando a coleta de provas.

Nas fraudes bancárias eletrônicas, por exemplo, um criminoso ou organização criminosa, por meio da Internet, subtrai valores das contas correntes de vítimas de diferentes regiões do país, os quais são transferidos para contas de beneficiários (“laranjas”) ou utilizados para pagamento de títulos bancários de terceiros. Segundo a regra do art. 70 do CPP, teríamos diversas investigações em andamento para os atos praticados por uma mesma organização criminosa, ocasionando maior dispêndio dos recursos públicos e maior chance de impunidade.

3 A NOVA LEI Nº 12.737/12 DE CRIMES INFORMÁTICOS

Com a crescente utilização da Rede para fins ilícitos ou prejudiciais a terceiros, surgiram no Brasil diversas iniciativas legislativas com o intuito de criminalizar as condutas praticadas contra sistemas ou dispositivos informáticos. Entre elas, tivemos o Projeto de Lei – PL nº 84/99, de autoria do Deputado Luiz Piauhylino, o qual tramitou no Senado e na Câmara sob a relatoria do Deputado Eduardo Azeredo, e o PL nº 76/2000, de autoria do Senador Renan Calheiros.

Tais projetos foram extremamente criticados, entre outros motivos, devido às imprecisões técnicas dos textos, à grande abrangência dos tipos penais, que possibilitariam a criminalização de condutas triviais praticadas na Internet, e também à tipificação de condutas já tuteladas pelo Direito Penal, em desacordo ao princípio da intervenção penal mínima.

A tramitação do PL nº 84/99, por exemplo, demorou 13 anos, originando a Lei nº 12.735/12, também conhecida como Lei Azeredo, que não será objeto de estudo do presente trabalho.

O PL nº 84/99 inicialmente apresentava 18 artigos versando sobre princípios, definições e tipos penais inovadores referentes às condutas de dano informático, acesso indevido, alteração de dados, produção de *malwares*, entre outros (SYDOW, 2013, p. 273).

Entretanto, foi drasticamente modificado, sendo sancionado com apenas 4 artigos, relacionados à adequação de setores especializados de investigação de crimes informáticos nas polícias judiciárias e às medidas cautelares em crimes de preconceito.

Já a Lei nº 12.737/12 originou-se do PL nº 2793/2011, apresentado pelo Deputado Federal Paulo Teixeira em 29 de novembro de 2011, o qual tramitou de forma célere nas casas legislativas, sendo publicada em 03 de dezembro de 2012.

Conhecida no jargão popular como “Lei Carolina Dieckmann”, por ter sido aprovada após os incidentes que resultaram na obtenção e divulgação não autorizada de fotos

íntimas da atriz na Internet, a lei tipificou, entre outros, os crimes de invasão de dispositivo informático, com a adição do art. 154-A, e interrupção de serviço telemático, com a alteração do art. 266, ambos do Código Penal.

Antes dela, havia a necessidade de adequar as condutas aos tipos penais pré-existentes, como, por exemplo, o crime de dano, o que nem sempre se dava de forma perfeita, podendo resultar no arquivamento da investigação policial pela autoridade judiciária, caso esta não julgasse adequado o enquadramento dado à conduta lesiva (CABETTE, 2013).

Era flagrante a necessidade de uma legislação adequada sobre o tema, de forma a se evitar a constante afronta ao princípio da reserva legal, bem como os casos de impunidade de condutas relevantes sob o ponto de vista penal (MOREIRA, 2012).

O PL nº 2793/11, em sua justificativa, pugnava pela "criação de tipos penais aplicáveis à condutas praticadas na Internet mas apenas aquelas estritamente necessárias à repressão daquelas atividades socialmente reconhecidas como ilegítimas e graves".

Segundo seus autores, procurou-se, em comparação com outros PLs, "[...] excluir as definições pretensamente exaustivas, as quais não significavam ganho em precisão e clareza da legislação penal [...]", utilizando-se para isso de terminologias que encerrassem as condutas a serem criminalizadas de forma adequada.

Entretanto, o novo texto legal ainda é objeto de discussão entre juristas, tendo recebido diversas críticas quanto às diferentes interpretações possíveis e à imprecisão dos conceitos técnicos envolvidos. Luiz Flávio Gomes (2013), por exemplo, assinala 104 conceitos passíveis de interpretação na nova lei.

Tal opinião não é unânime, pois, como afirma Marília Monteiro (2012), o diferencial da nova lei é "a sua precisão na identificação dos tipos penais em respeito ao princípio da vedação da norma penal em branco".

As críticas também dizem respeito à celeridade vista na tramitação do PL nº 2793/2011, apontada por muitos como decorrente da pressão da opinião pública após o incidente envolvendo a atriz Carolina Dieckmann (VIEIRA, 2013).

De qualquer forma, com a aprovação da referida Lei, foram realizadas alterações em nosso Código Penal, o qual passou a tipificar os crimes de invasão de dispositivo computacional e de interrupção de serviço telemático, cuja análise será o objeto dos próximos tópicos.

3.1 CONCEITOS TÉCNICOS ENVOLVIDOS

Para o desenvolvimento do presente capítulo, é necessário definir certos termos e expressões que serão tratados mais à frente, os quais tem relação com a área da computação, e devem ser bem compreendidos para estabelecer o alcance dos tipos penais definidos na Lei nº 12.737/12.

3.1.1 Dispositivo informático

Para definir a expressão "dispositivo informático", é necessário primeiramente saber o que vem a ser dispositivo, bem como qual o conceito de informática.

Dispositivo, segundo a definição do Dicionário Houais (2009, p. 696), seria "o conjunto de componentes físicos ou lógicos que integram ou estão conectados a um computador, e que constituem um ente capaz de transferir, armazenar ou processar dados".

Em um contexto geral, não apenas o conjunto de componentes, mas até mesmo o computador ou equipamento assemelhado pode ser considerado um dispositivo (THING, 2003, p. 226).

Dessa forma, podemos definir dispositivo como sendo qualquer equipamento, aparelho, instrumento ou componente, tanto físico quanto lógico, projetado para um função específica (FRAGOMENI, 1986, p. 187).

Já informática, segundo o Dicionário Houaiss (2009, p. 1082), é a ciência que se dedica ao tratamento da informação mediante o uso de computadores e outros dispositivos de processamento de dados, incluindo desde os recursos lógicos, como os *softwares*, linguagens e algoritmos, até os recursos físicos, como processadores, periféricos e demais componentes (FRAGOMENI, 1986, p. 314).

A origem da palavra vem do francês *informatique*, cunhado em 1962 pelo engenheiro francês Phillipe Dreyfus, como um acrônimo das palavras “informação” e “automática”, ou seja, refere-se ao tratamento automático de informações (ROSSINI, 2004, p. 42).

O conceito de dispositivo, de forma genérica, nos remete à ideia de algo físico, palpável, ou seja, o *hardware* que compõe um equipamento computacional, como é o caso das placas, chips, discos, monitores, teclados, mouse e impressora.

Entretanto, se fossemos pensar apenas na ideia de *hardware*, o conceito de “dispositivo informático” estaria incompleto, pois este seria incapaz de processar e tratar as informações de forma automática. Para que isso ocorra, faz-se necessária a presença de uma parte lógica (*software*), a qual é indissociável da parte física, sob pena desta não ter utilidade, como é o caso, por exemplo, do sistema operacional e dos aplicativos instalados no dispositivo.

Sendo assim, considera-se “dispositivo informático” o conjunto formado pelo equipamento, bem como os sistemas nele instalados, que processe ou armazene informações de forma automatizada, não se restringindo apenas a computadores e notebooks, mas podendo abarcar invenções mais recentes, como os *tablets*, *smartphones* e *pendrives*.

3.1.2 Mecanismo de segurança

Segurança, de forma geral, pode referir-se tanto a um estado ou condição de quem ou do que está livre de perigos e assegurado de danos e riscos eventuais, quanto a um dispositivo cuja função é evitar o perigo, acidentes, danos e perdas (HOUAISS; VILLAR, 2009, p. 1722).

Já no campo da informática, segurança pode ser definida como a prevenção do acesso ao uso de dados ou programas sem autorização (FRAGOMENI, 1986, p. 580).

Essa prevenção pode se dar por meio de diferentes mecanismos, os quais podem ser extrínsecos ou intrínsecos ao dispositivo informático.

No caso dos mecanismos extrínsecos, temos por exemplo a adoção de uma política de segurança da organização, a qual pode determinar a periodicidade da instalação

das atualizações de segurança lançadas para um sistema operacional, visando corrigir alguma vulnerabilidade recentemente descoberta, e a realização de cópias de segurança (*backups*) dos dados importantes (CERT.br, 2012, p. 48-53).

Os mecanismos intrínsecos, por sua vez, são inerentes ao próprio dispositivo, como é o caso das senhas de autenticação, uso de criptografia, programas do tipo antivírus ou *firewall*, os quais muitas vezes são oferecidos com o próprio sistema, mas podem ser desabilitados pelo usuário.

Devemos ter em mente que nenhum mecanismo de segurança protege contra todos os riscos, pois a cada dia, surgem novas ameaças no campo da informática, cada vez mais complexas e com alto poder de disseminação, as quais não são detectadas imediatamente.

Sendo assim, mesmo um computador que possua vários desses mecanismos em funcionamento ainda pode ser alvo de um crime informático, como por exemplo um novo vírus cuja "vacina" ainda não tenha sido produzida pela empresa fabricante do *software* antivírus.

Como veremos mais à frente, a caracterização da violação de mecanismo de segurança é importante, pois caso não se verifique tal violação, a conduta de invasão de dispositivo informático restará atípica.

Entretanto, a expressão "mecanismo de segurança" deve ser interpretada de acordo com a conduta criminosa praticada. Por exemplo, não há que se falar em violação indevida de mecanismo de segurança quando uma pessoa não autorizada manuseia um computador que não possui senha de acesso e obtém, adultera ou destrói os dados ou informações ali contidas.

Caso a mesma pessoa consiga o acesso ao computador sem senha por meio da rede de computadores, ao explorar uma falha de segurança do sistema operacional, vemos que a existência de senha seria irrelevante para a consecução do delito, caracterizando assim violação indevida de mecanismo de segurança intrínseco ao sistema operacional.

Nesses casos, será fundamental a presença do especialista de informática ou perito criminal com formação na área, que poderá determinar como se deu o acesso indevido e, caso existente, qual o mecanismo de segurança violado.

3.1.3 Vulnerabilidade

Vulnerabilidade, segundo o Dicionário Houaiss (2009, p. 1961) é a qualidade ou estado do que é ou se encontra vulnerável, sujeito a ser atacado.

No campo da informática, uma vulnerabilidade é uma fraqueza intrínseca existente em um sistema ou dispositivo, em geral decorrente de erros no projeto ou na programação lógica, podendo comprometer a segurança do sistema e ser explorada por um agente mal-intencionado. O ato de explorar a vulnerabilidade, bem como o código ou programa que realiza tal tarefa são conhecidos pelo termo em inglês *exploit* (THING, 2003, p. 311).

A Cartilha de Segurança do CERT.br (2012, p. 18) traz o seguinte conceito:

> "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 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."

Quando uma nova vulnerabilidade é descoberta, seja em um sistema operacional ou em um *software* específico, o fabricante daquele produto desenvolve um "reparo" ou "remendo" (*patch*) em resposta, sendo responsabilidade do usuário do dispositivo efetuar a instalação dessa correção. Entretanto, pode ser difícil manter o dispositivo sempre atualizado, tendo em vista a velocidade da descoberta de novas vulnerabilidades (THING, 2003, p. 311-312).

3.1.4 Serviço telemático

Antes do advento das redes de computadores, e, em especial, da Internet, os serviços oferecidos por determinado computador eram acessíveis apenas aos usuários que

pudessem interagir fisicamente com aquele equipamento. Como já explicado anteriormente, a Internet foi criada devido à necessidade do governo norte-americano de manter suas comunicações em caso de guerra ou ataque, o que levou à popularização das redes de computador e ao desenvolvimento da telemática.

Telemática, também denominada teleinformática, consiste na conjugação da informática e dos meios de telecomunicação, ou seja, é a ciência que provê a infraestrutura necessária à troca de informações entre computadores e demais dispositivos informáticos, os quais geralmente interagem por meio de redes de telecomunicação (ROSSINI, 2004, p. 42-43).

O termo diz respeito não apenas à infraestrutura e aos protocolos necessários à comunicação entre computadores, mas também aos próprios serviços informáticos fornecidos por meio de redes de telecomunicações (HOUAISS, VILLAR, 2009, p. 1823), como por exemplo um serviço de *e-mail* interno de uma empresa ou um *site* acessível pela Internet.

Com a telemática e a informatização, serviços que antes eram prestados apenas de forma presencial passaram a ser realizados à distância, como, por exemplo, os serviços bancários (*home banking*), o comércio eletrônico, atividades de educação e até mesmo telecirurgias, onde o médico cirurgião pode estar a milhares de quilômetros de distância do paciente e operar um robô por meio da Internet.

Conforme visto no segundo capítulo, a interrupção de um serviço afeta a disponibilidade da informação, e geralmente ocorre pela sobrecarga de acessos, ou seja, quando um número elevado de usuários solicita o serviço ao mesmo tempo. Pode resultar em sérios prejuízos, seja na esfera econômica, como por exemplo nos *sites* bancários e de comércio eletrônico, ou até mesmo à vida e integridade física, no caso das cirurgias à distância.

A interrupção pode se dar pelo aumento repentino de acessos legítimos, como é o caso dos *sites* de companhias aéreas quando anunciam uma promoção de passagens, ou por ação criminosa, quando um individuo mal-intencionado realiza um ataque de negação de serviço, causando lentidão e até mesmo interrompendo o acesso a um *site* ou serviço da Internet.

3.2 ANÁLISE DO DELITO DE INVASÃO DE DISPOSITIVO INFORMÁTICO

O artigo 154-A, *caput*, do Código Penal, acrescido pela Lei nº 12/737/12, tipifica a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, que ocorra 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.

Nos termos do artigo 154-A, §1º, pratica o mesmo crime quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta acima definida.

Nos dois casos, a pena varia de três meses a um ano de detenção, e multa, podendo ser majorada de um sexto a um terço se da invasão resultar prejuízo econômico.

A forma qualificada definida no 154-A, §3º exige 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, sendo a pena de seis meses a dois anos de reclusão e multa, caso a conduta não constitua crime mais grave.

Além disso, a pena nesses casos pode ser aumentada de um a dois terços, se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

A pena também pode ser aumentada de um terço à metade se o crime for cometido contra pessoas que ocupam altos cargos públicos, como Presidente da República, governadores, prefeitos, Presidente do STF, da Câmara dos Deputados, entre outros.

Para Guilherme Nucci (2014, p. 814), o tipo penal definido no *caput* do artigo 154-A pode ser classificado como:

> "[...] crime comum (pode ser cometido por qualquer pessoa); formal (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira

> determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; unissubjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos); admite tentativa.

A tutela jurídica, tendo em vista a localização do tipo em nosso Código Penal, se voltaria à proteção da liberdade individual de forma mediata, e, de forma imediata, à inviolabilidade dos segredos, aqui entendida como proteção à intimidade, à vida privada, à honra e à inviolabilidade das comunicações, entre outros (NUCCI, 2014, p. 811).

Tal posicionamento é semelhante ao adotado por Cabette (2013), para quem a tutela seria individual, não se destinando ao sistema informático e sim à pessoa atingida pela conduta lesiva, alcançando inclusive o direito à privacidade, garantido no art. 5º, X de nossa Carta Magna.

Spencer Toth Sydow (2013, p. 288), de maneira diversa, afirma ser a tutela coletiva, voltada à proteção da segurança telemática, ou seja, protege "[...] a confidencialidade dos arquivos existentes nos dispositivos informáticos", bem como "[...] a integridade dos dados e sua disponibilidade, todos em conjunto".

Já que a lei destina-se à tipificação dos delitos informáticos, a interpretação desta deve se dar não apenas de forma literal, mas também teleológica, tendo em vista a finalidade da norma, em conjunção com os conceitos da Computação e Tecnologia da Informação.

O verbo núcleo do tipo, que no Projeto de Lei original era "devassar", foi substituído por "invadir", definido como o ato de "[...] entrar sem autorização do proprietário" (BRITO, 2013), ou também "[...] violar, transgredir, entrar à força em algum lugar" (NUCCI, 2014, p. 812).

Ao procurar o significado do verbo em um dicionário, verificamos que este é geralmente associado ao uso de força ou violência. Entretanto, no contexto da nova lei, vemos que o verbo invadir, comumente usado na área de Segurança da Informação, representa o ato de acessar um dispositivo ou sistema informático de forma indevida, sem o consentimento do titular daquele dispositivo, aproveitando-se de falha de segurança ou técnicas de engenharia social.

O objeto material alvo da conduta tipificada no *caput* do artigo em análise consiste em dispositivo informático alheio, sendo, portanto, atípica a invasão de um usuário a seu próprio computador, como, por exemplo, quando este esquece a senha de acesso.

O conceito de dispositivo informático, como já discutido, abarca não apenas os computadores, mas, segundo Cabette (2013), também outros aparelhos "[...] que tenham capacidade de armazenar dados ou informações passíveis da violação prevista no tipo penal" do artigo 154-A (*tablets*, *netbooks*, *notebooks*, *smartphones*, etc), bem como os sistemas e *softwares* instalados nesses equipamentos.

O elemento normativo do tipo exige que a invasão se dê mediante violação indevida de mecanismo de segurança, ponto bastante criticado por especialistas da ciência do Direito e da Informática.

Por ser um termo técnico, o significado de "mecanismo de segurança" é passível de diferentes interpretações. Cabette (2013), por exemplo, afirma que é necessário que o dispositivo, seja este um computador, *tablet*, celular, etc, possua senha, *firewall*, antivírus ou ferramentas semelhantes instaladas e ativas no momento do crime.

Guilherme Nucci (2014, p. 813-814) considera o elemento normativo acima como o "[...] calcanhar de Aquiles do tipo em comento", já que a invasão de dispositivo que não possua mecanismos de segurança ou que tenha ocorrido sem violar nenhum dos mecanismos existentes restaria atípica. Além disso, é inapropriado se falar em "violação indevida", pois o verbo "invadir" já possui uma forte conotação de transgressão, de forma que, se a violação fosse devida, seria mero exercício regular de direito ou estrito cumprimento do dever legal, por exemplo.

Entretanto, não podemos, como operadores do Direito, realizar uma valoração fático-jurídica simplista, caracterizando uma conduta como atípica apenas pela ausência dos mecanismos de segurança mais usuais (senhas, *softwares* antivírus, *firewalls*, etc).

Um dispositivo conectado ou não a uma rede de computadores não pode, de maneira trivial ao homem médio, ser invadido, mesmo que não possua nenhum mecanismo de segurança extrínseco instalado. Pelo fato de os sistemas operacionais possuírem mecanismos intrínsecos de segurança, os quais geralmente se encontram habilitados por padrão, na maioria

dos casos apenas um perito criminal ou especialista de informática será capaz de determinar como se deu a invasão e qual o mecanismo de segurança violado.

Os sujeitos ativos e passivos do delito de invasão podem ser qualquer pessoa, sendo que o sujeito passivo pode ser inclusive pessoa jurídica que tenha seu sistema ou dispositivo invadido. Para Cabette (2013), o usuário não precisa ser o proprietário ou titular do dispositivo. Assim, usuários de *lan houses*, por exemplo, estariam amparados pela nova lei.

O crime de invasão de dispositivo também admite a forma tentada, quando uma pessoa utiliza seus conhecimentos e ferramentas para violar mecanismo de segurança, mas falha em alcançar o resultado "por motivos alheios à sua vontade seja porque é fisicamente impedida, seja porque não consegue, embora tente violar os mecanismos de proteção" (CABETTE, 2013).

O crime de invasão prevê apenas a modalidade dolosa, não se exigindo que o computador esteja conectado em rede de computadores, seja a Internet ou rede local.

A expressão "instalar vulnerabilidades" também é bastante criticada, devido à imprecisão técnica quanto ao termo e à redação utilizada por nosso legislador, que resulta em ambiguidade na leitura do tipo penal.

Primeiramente, quanto à imprecisão técnica, cumpre esclarecer que a ação de instalar, no âmbito da informática, refere-se geralmente a código ou aplicativos, sendo tecnicamente incorreto dizer que uma vulnerabilidade foi instalada. Conforme já explicado, a existência de uma vulnerabilidade em um dispositivo ou sistema informático muitas vezes é um fato desconhecido de seus usuários e do próprio fabricante. Tal condição pode ser explorada por um agente mal-intencionado, resultando na execução de ações maliciosas.

Em relação à ambiguidade presente no *caput* do tipo penal, o legislador não deixa claro se o ato de instalar vulnerabilidade constitui conduta típica alternativa à ação de invadir dispositivo, ou se ela constitui finalidade especial de agir da invasão, juntamente com o ato de obter, adulterar ou destruir dados ou informações.

Certos autores defendem tratar-se de tipo penal misto alternativo. Para Nucci (2014, p. 812) e Cabette (2013), por exemplo, pratica o crime descrito no *caput* do

artigo 154-A quem invade dispositivo ou instala vulnerabilidades, sendo considerado crime único a prática de uma ou de ambas as condutas.

Outros autores, como Rogério Greco (2013), Spencer Sydow (2013, p. 289) e Marcelo Crespo (2013, p. 9), entendem ser o crime de ação única, possuindo diversos elementos subjetivos específicos, quais sejam, a finalidade de **obter**, **adulterar** ou **destruir** dados ou informações, sem autorização expressa ou tácita do titular do dispositivo, ou a finalidade de **instalar vulnerabilidades para obter vantagem ilícita**.

No Projeto de Lei original, o artigo 154-A, *caput*, apresentava o seguinte texto:

> "Devassar dispositivo informático alheio, conectado ou não a 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, instalar vulnerabilidades ou obter vantagem ilícita."

Observa-se de plano que a intenção do legislador inicialmente era de que a instalação de vulnerabilidades constituísse finalidade específica do crime de invasão, tese que pode ser confirmada com a leitura da justificativa do Projeto de Lei:

> "[...] estabelece a necessidade de intenção específica de 'instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações não autorizados' - ou seja, pune-se apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável e não se confundir com atividades legítimas da Internet, excluindo-se assim, mais uma vez, os casos de mero acesso a informações, ou os casos de obtenção de informações que, por sua natureza, não seriam passíveis de restrição de acesso, em um primeiro momento, era de que a instalação de vulnerabilidades para obter vantagem ilícita constituísse elemento subjetivo específico do tipo, assim como a obtenção, adulteração ou destruição de dados ou informações o são."

Com a modificação do texto original, entende-se que o legislador optou por ampliar o espectro de condutas puníveis, tratando-se, portanto, de tipo penal misto alternativo, já que em muitos casos a instalação de vulnerabilidades pode ocorrer sem que antes tenha havido a invasão do dispositivo.

Como exemplo, podemos citar os *spams*, que são mensagens de *e-mail* indesejáveis, contendo arquivos anexos com programas maliciosos, que podem infectar o

computador do destinatário, caso este os execute inadvertidamente, consumando assim o ato de “instalar vulnerabilidade”.

Desde que o usuário não execute o arquivo malicioso constante do *e-mail*, podemos classificar tal conduta como mero ato preparatório. Entretanto, uma vez que o usuário tenha executado o arquivo, podemos estar diante de um crime consumado ou de uma tentativa, dependendo se o arquivo tenha sido instalado com êxito ou não, quando, por exemplo, ocorre a detecção por programa antivírus.

Sendo assim, o crime definido no artigo 154-A, *caput*, é de ação múltipla, devendo o autor do delito ter a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, no caso da ação de invasão de dispositivo, ou obter vantagem ilícita, no caso da ação de instalação de vulnerabilidades.

A intenção do legislador, segundo a justificativa do PL, foi punir apenas as condutas que resultassem em dano ou quando o objetivo do agente fosse efetivamente censurável, evitando-se assim punir atividades legítimas praticadas pela Internet.

Para Brito (2013), essa previsão do especial fim de agir trouxe “[...] uma restrição temerária ao horizonte de abrangência da norma”. Por exemplo, a conduta de um *hacker* iniciante, que pratica a invasão para aprimorar seus conhecimentos, sem, contudo, ter interesse em obter dados ou obter vantagem ilícita, não poderia ser punida:

> “É possível que nessas invasões despretensiosas, o primeiro autor deixe aberta as portas para que um segundo criminoso, sem qualquer ajuste entre os dois, agora com a intenção de obter informações, por exemplo, atue livremente, chegando ao extremo de nem mesmo responder pelo crime, já que ele não violou indevidamente a segurança, ela já estava violada.”

Um ponto importante é que o crime, por ser formal, se consuma com a simples invasão ou instalação de vulnerabilidades, constituindo mero exaurimento a eventual obtenção de dados ou informações, adulteração ou destruição, bem como a obtenção de vantagem ilícita (CABETTE, 2013).

Essa posição enfatiza o caráter protetivo do Direto Penal, em contraposição ao princípio da lesividade. Segundo Auriney Brito (2013), o Direito Penal, sendo a *ultima ratio* do Estado, deve se antecipar à lesão ou ameaça, protegendo os cidadãos antes que as condutas lesivas possam lhe causar maiores prejuízos.

No caso da figura equiparada do artigo 154-A, §1º, buscou-se coibir a produção, comercialização ou difusão de dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

Não é muito difícil localizar *sites* e fóruns da Internet direcionados à compra e venda de programas maliciosos. Em geral, esses programas permanecem invisíveis no sistema do usuário, capturando informações sigilosas, como dados bancários, e realizando ações maliciosas (envio dos dados obtidos ao *e-mail* do criminoso, por exemplo).

Como exemplo de dispositivo destinado à prática da conduta definida, temos os mecanismos conhecidos como *keyloggers*, instalados entre o computador e o teclado da vítima, que armazenam tudo que é digitado pelo usuário, possibilitando ao criminoso obter senhas e outras informações sigilosas.

Figura 3 - Exemplo de *keylogger* instalado em um computador

Fonte: http://www.coolestgizmo.com/computer-gadgets/usb-keyboard-recorder-keylogger/

Ocorre que, com a redação dada pelo legislador ao novo artigo 154-B do Código Penal, tais condutas muitas vezes não poderão ser punidas, já que a ação penal nesses delitos será condicionada à representação, exceto quando o crime for 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.

Conforme preleciona Guilherme Nucci (2014, p. 815), as condutas tipificadas não apresentam sujeito passivo determinado, destinando-se à proteção da sociedade de forma geral. Dessa forma, quando um criminoso produz um software para

invadir computadores, independentemente se esses pertencem ou não à administração, trata-se de crime de ação pública condicionada, não havendo quem possa representar, já que o sujeito passivo é a própria sociedade.

Quanto à forma qualificada do crime de invasão de dispositivo, esta pode se dar 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.

O controle remoto definido no artigo 154-A, §3º, como o próprio nome indica, ocorre com a instalação de código ou programa que permita ao criminoso o controle do dispositivo à distância. Dessa forma, o criminoso pode utilizar o dispositivo invadido como intermediário para o cometimento de outros crimes.

O acesso remoto frequentemente é associado aos ataques de negação de serviço, estudados na próxima seção, que ocorrem quando vários computadores controlados remotamente pelo criminoso sobrecarregam um site ou sistema alvo, impedindo o acesso dos demais usuários.

Em crimes informáticos cometidos contra os órgãos e entidades da Administração Pública, o inquérito policial não dependerá de representação do ofendido, podendo ser iniciado de ofício pela autoridade policial.

Muitas vezes, entretanto, apenas a área de Tecnologia da Informação (TI) do órgão ou entidade atingido pela conduta tem condições de verificar quanto à ocorrência do delito e à existência de registros ou evidências que auxiliem a determinar a materialidade e autoria.

A investigação de um delito informático, então, depende do auxílio do responsável pelo dispositivo ou sistema atingido, o qual, por sua vez, deve armazenar e fornecer à polícia todas as evidências e registros que sirvam à elucidação do crime.

Os novos crimes informáticos, por seu caráter eminentemente técnico, também trazem consequências diretas para a investigação e persecução penal. Além de contar com o auxílio dos Institutos de Criminalística, os órgãos de polícia judiciária agora precisam estruturar setores especializados na investigação desse tipo de delito.

O investigador de delitos informáticos e o perito criminal, fugindo do estereótipo comum de policial, devem ser pessoas com amplo conhecimento na área de informática, com capacidade para entender o *modus operandi* do crime, constatando a materialidade e determinando a autoria.

Outro fator de crítica é quanto às penas cominadas ao crime de invasão, considerando os prejuízos financeiros advindos, como é o caso da obtenção de segredos industriais de uma grande empresa, bem como à intimidade da vítima, na obtenção e divulgação de informações armazenadas em seu computador.

À primeira vista, poderíamos pensar ser cabível a aplicação da Lei nº 9.099/95, com o trâmite segundo o rito sumaríssimo, considerando que a maior parte das penas máximas cominadas não é superior a dois anos.

Entretanto, é provável que muitas ações sejam processadas na Justiça Comum, devido à complexidade de tais delitos e à necessidade de perícias computacionais para determinar a materialidade, o que é incompatível com os princípios da celeridade e simplicidade que norteiam os Juizados Especiais Criminais (CRESPO, 2013, p. 9).

Dessa forma, o trâmite mais lento na Justiça Comum, conjugado com a complexidade dos crimes e seu caráter transnacional, poderá resultar na ocorrência de prescrição em muitos casos.

Isso porque, em qualquer dos delitos, a pena mínima aplicada em concreto, mesmo considerando as causas de aumento de pena, será menor que um ano, operando-se a prescrição retroativa caso se passem três anos entre o recebimento da denúncia ou queixa e a publicação da sentença condenatória (artigo 109, VI, e 110 do Código Penal).

Além disso, se o autor da conduta for menor de 21 anos quando da época do crime, fato bastante comum nos crimes informáticos, estaremos diante de um caso de menoridade penal relativa (art. 115), o que reduz o prazo prescricional pela metade.

William Oliveira (2013) corrobora tal assertiva, arguindo que:

> "[...] a apuração da autoria certamente demandará exames periciais complexos, principalmente por se tratar de infração que deixa vestígios. Considerando que a pena mínima é baixíssima, não serão poucos os casos em

> que se verificará a prescrição. Quando isso não ocorrer, o autor fará jus à transação penal.”

O mesmo autor também declara ser incabível a decretação de prisão temporária, preventiva ou em flagrante, já que o autor dos fatos, assumindo o compromisso de comparecer em juízo, acabará sendo liberado.

Considerando a pena cominada ao delito, em muitos casos também não será possível utilizar-se de uma importante ferramenta de investigação de delitos informáticos, qual seja, a interceptação telemática da conexão do suspeito, haja vista a proibição de tal procedimento quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção, conforme art. 2º, III, da Lei nº 9.296/96.

Diante do quadro exposto, é possível concluir que o tipo penal em comento, embora represente uma avanço na tipificação dos delitos informáticos próprios, não resultará em maior eficácia no combate a esse tipo de delinquência, tendo em vista a complexidade de prova da materialidade, bem como as penas cominadas, que favorecerão a ocorrência de prescrição.

3.3 ANÁLISE DO DELITO DE INTERRUPÇÃO DE SERVIÇO TELEMÁTICO

Outra modificação trazida pela Lei nº 12.737/12 foi a alteração do tipo penal do artigo 266, com a inserção do parágrafo primeiro, que passou a tipificar a interrupção de serviço telemático ou de informação de utilidade pública, incorrendo também no crime quem impede ou dificulta-lhe o restabelecimento. As penas continuam as mesmas aplicadas ao *caput*, quais sejam, detenção de um a três anos, e multa.

Segundo Nucci (2014, p. 1160), a palavra “interromper” significa fazer cessar integralmente ou romper a continuidade, enquanto impedir pode ser visto como sinônimo de impossibilitar, e dificultar é o mesmo que colocar obstáculo.

O mesmo autor classifica essa nova figura típica como sendo crime comum, formal, de forma livre, comissivo, instantâneo, de perigo comum abstrato, unissubjetivo, plurissubsistente e que admite tentativa.

É interessante notar que o *nomem juris* do crime foi alterado, passando a se chamar “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”.

No caso dos serviços telemáticos e de utilidade pública, o legislador preferiu criminalizar apenas a interrupção, por considerar que a perturbação de tais serviços poderia abranger condutas inofensivas como o excesso de utilização por usuários legítimos. Entretanto, já que tais crimes admitem a tentativa, será possível punir a perturbação criminosa, quando, por exemplo, um individuo tentar sem sucesso “derrubar” um *site*, deixando-o apenas mais lento. A pena, nesses casos, será a correspondente ao crime consumado, diminuída de um a dois terços, conforme o art. 14, parágrafo único do CP.

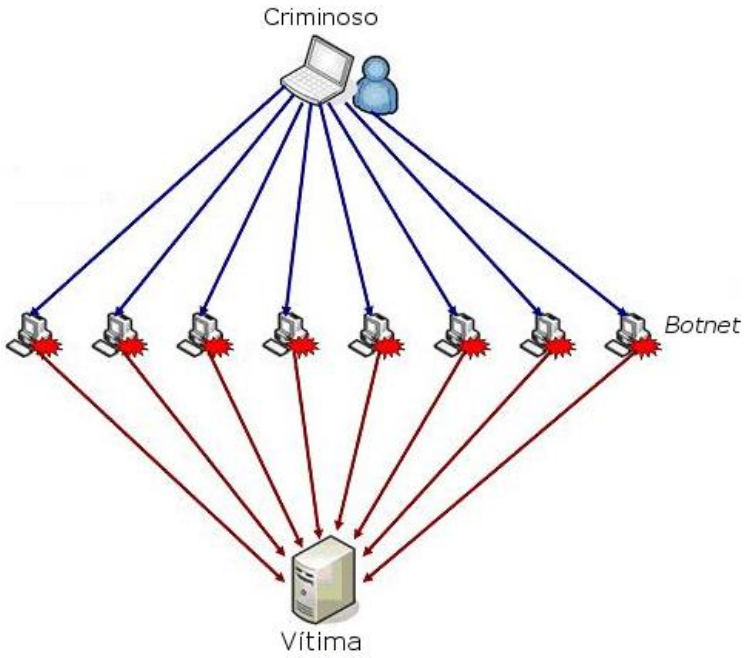
O serviço informático, embora apareça no título do crime, não foi inserido no corpo do tipo penal, provavelmente em decorrência da pressa do legislador, razão pela qual permanece atípica a sua perturbação ou interrupção (NUCCI, 2014, p. 1160).

Essa modificação do art. 266 do CP possibilitou a tipificação das condutas conhecidas como ataques de negação de serviço (*Denial of Service – DoS*) e dos ataques distribuídos de negação de serviço (*Distributed Denial of Service – DDoS*).

Em um ataque distribuído de negação de serviço, o criminoso interrompe o acesso de outros usuários a um serviço telemático (um *site* da Internet, por exemplo), por meio da sobrecarga do serviço.

Para isso, geralmente é utilizada uma grande quantidade de computadores infectados, denominada *botnet*, sobre os quais o criminoso detenha o controle remoto. Após a ordem de atacar, os computadores infectados começam a enviar grande quantidade de requisições para o serviço, causando desde lentidão até o completo travamento do serviço (ATAQUE DE NEGAÇÃO DE SERVIÇO, 2014).

Figura 4 - Exemplo de um ataque do tipo *DDoS*



Fonte: http://blog.corujadeti.com.br/que-tal-simular-um-ataque-ddos-para-testar-o-seu-weblab/

Tendo em vista os potenciais prejuízos causados por um ataque *DDoS*, existem inclusive relatos de empresas que "contratam" esses criminosos, para que ataquem o *site* de empresas rivais, prejudicando os negócios da concorrente. Essa situação caracteriza, além do crime de interrupção de serviço telemático, também o crime de concorrência desleal, definido no art. 195, III da Lei nº 9279/96, ensejando não apenas o processamento perante a esfera criminal, mas também a reparação dos danos no juízo cível.

Na justificação do Projeto de Lei, a intenção do legislador era proteger apenas os serviços essencialmente públicos, uma vez que o tipo penal insere-se no Capítulo referente aos crimes contra a segurança dos meios de comunicação e transporte e outros serviços públicos, excluindo aqueles cuja natureza, eminentemente privada, não merecesse o mesmo nível de equiparação.

Para João Felipe Jatobá (2012), houve falha na redação do art. 266, já que a proteção estende-se apenas aos serviços telemáticos e de utilidade pública:

> "Isto significa que o referido tipo penal protegerá o serviço telemático em si e os serviços de informação de utilidade pública, e não os sites considerados individualmente. O objeto material protegido são os serviços telemáticos e de informação considerados como o conjunto de equipamentos e protocolos que possibilitam a troca de informações e dados."

Entretanto, o legislador não se atentou para o significado da expressão “serviço telemático”, que tem uma abrangência maior do que a que se quis alcançar. Conforme explicado anteriormente, um serviço telemático corresponde não apenas à infraestrutura pública de telecomunicações e aos protocolos necessários à interação entre computadores, mas também aos próprios serviços informáticos fornecidos por meio dessas redes.

Spencer Toth Sydow (2013, p. 285) afirma tratar-se de norma penal em branco, já que o conceito de serviço telemático não está definido com precisão, necessitando de normativo complementar que venha a suprir a dúvida, evitando assim o alargamento excessivo da punição.

Entretanto, diante dos conceitos expostos nas seções anteriores, é possível perceber que a expressão “serviço telemático”, embora contemple diferentes tipos de serviço acessíveis por ou inerentes aos meios de telecomunicação, encontra-se delimitada, sendo possível aplicar o tipo penal em exame.

Dessa forma, o serviço de conexão de um provedor de acesso à Internet, um portal de notícias na *Web* ou um servidor de *e-mail*, entre outros, mesmo pertencentes a particulares, podem ser considerados serviços telemáticos, de forma que a sua interrupção é considerada crime, devendo ser objeto da atenção do Direito Penal.

CONCLUSÃO

A Internet é considerada uma das maiores invenções do homem, podendo ser vista ao mesmo tempo como um meio de comunicação e um lugar para o estabelecimento de relações jurídicas.

Seu uso, antes restrito aos governos e comunidades acadêmicas, foi liberado para a exploração comercial, resultando na formação de uma verdadeira Aldeia Global, onde as distâncias não existem e uma transação comercial ocorre no apertar de um botão.

Ao mesmo tempo em que propiciou o crescimento econômico e o aprimoramento das relações humanas, a Internet também despertou a atenção dos criminosos, cientes do potencial e dos ganhos que poderiam ser obtidos com essa nova ferramenta.

Nos últimos anos, presenciamos o surgimento e o aumento desenfreado dos crimes praticados pela Rede Mundial, alguns deles já tipificados em nosso ordenamento jurídico, quando a Internet é utilizada apenas como meio para atingir o bem jurídico tutelado, como a honra ou o patrimônio. Nessa toada, podemos citar, como exemplo, as difamações publicadas em *sites* de rede social e as fraudes bancárias eletrônicas, caracterizadas como furto.

No entanto, as novas condutas, classificadas pela doutrina como crimes informáticos próprios, muitas vezes ficavam impunes, devido à inexistência de tipo penal específico. Essas condutas não atingiam bem jurídico já tutelado, tendo como objetivo prejudicar o funcionamento dos sistemas ou dispositivos informáticos.

Entre as condutas assim classificadas, destacam-se a invasão de computador ou dispositivo assemelhado e a interrupção de serviço telemático. Embora a sociedade brasileira há muito já reclamasse um diploma legal específico para tipificar essas condutas, apenas em 2013, com a vigência da Lei nº 12.737/12, isso ocorreu.

Contudo, várias críticas foram feitas à edição dessa norma, algumas procedentes, conforme discutido anteriormente.

Em primeiro lugar, fica evidente que a celeridade na aprovação não trouxe maiores benefícios à persecução penal, por resultar em tipos penais cuja redação encontra-se repleta de incorreções. No presente caso, essa crítica ganha ainda mais força, já que a rapidez da tramitação foi supostamente atribuída à pressão da mídia no caso da atriz Carolina Dieckmann.

No outro extremo, como exemplo de tramitação morosa, tivemos o PL nº 84/99, que mais tarde veio se tornar a Lei nº 12.735/12, ou Lei Azeredo. Esse projeto de lei, durante os treze anos que levou para ser aprovado, sofreu tantas modificações no texto original, que, dos dezoito artigos inicialmente previstos, restaram apenas quatro, sendo que nenhum destes trata sobre crime informático.

Ao analisar a Lei nº 12.737/12, é possível identificar incorreções em ambos os artigos, algumas delas contornáveis e outras que afetam a aplicabilidade da norma penal.

Entre as incorreções, destaca-se a ambiguidade presente no texto do artigo 154-A, *caput*, do CP, que prejudica a interpretação do tipo penal, se de ação única ou de ação múltipla.

Se o intérprete concluir tratar-se de crime de ação única, o único núcleo do tipo seria "invadir dispositivo computacional". Nesse caso, os atos de "obter, adulterar ou destruir dados ou informações" e "instalar vulnerabilidades para obter vantagem ilícita" caracterizariam finalidade especial de agir do sujeito ativo.

Entretanto, considera-se que este não é o caso. Ao estudar o Projeto de Lei, verifica-se que o texto original sofreu alterações nesse trecho, sendo possível concluir tratar-se de crime misto alternativo, ou seja, o crime poderá ser praticado de duas formas, pela invasão do dispositivo ou pela instalação da vulnerabilidade.

Outro exemplo refere-se à suposta incoerência entre o delito previsto no art. 154-A, §1º, e a norma de natureza processual prevista no art. 154-B. O art. 154-A, §1º tipifica a produção, oferecimento, distribuição, venda ou difusão de dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*. Já o art. 154-B prevê que a ação penal condicionada à representação, exceto quando o crime for cometido contra a administração pública.

Aparentemente, o delito previsto no art. 154-A, §1º, por se destinar à proteção de toda a sociedade, não ensejará a persecução penal pelo Estado, já que a ação mediante representação não procederá por não possuir sujeito passivo determinado.

Além de tais erros, infere-se que na prática muitos desses crimes ficarão impunes, tendo em vista as penas cominadas e as dificuldades trazidas pelos próprios tipos penais.

Mesmo com penas não superiores a dois anos, tais crimes dificilmente serão processados perante os Juizados Especiais, tendo em vista a complexidade das condutas e a necessidade de exames periciais. No caso da invasão de dispositivo, por exemplo, tais exames deverão comprovar a existência e violação de mecanismo de segurança, detalhando o *modus operandi* do agente, o que muitas vezes pode ser inconclusivo.

Dessa maneira, o trâmite mais lento na Justiça Comum, conjugado com a complexidade dos crimes e seu caráter transnacional, poderá resultar na ocorrência de prescrição em muitos casos.

Entre as medidas que podem ser buscadas para contornar essa situação, destaca-se o aperfeiçoamento das medidas de cooperação internacional, visando agilizar os procedimentos de requisição e fornecimento de informações relacionadas a crimes informáticos, bem como o aperfeiçoamento das policias judiciárias, com a estruturação de setores especializados e treinamento de pessoal.

Além disso, a sociedade deverá contar também com a boa vontade do legislador, no sentido de eliminar as incorreções existentes no texto e aplicar penas mais adequadas, tendo em vista a gravidade de tais condutas e os prejuízos decorrentes de sua prática.

REFERÊNCIAS

ATAQUE DE NEGAÇÃO DE SERVIÇO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2014. Disponível em: <http://pt.wikipedia.org/w/index.php?title= Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o&oldid=38478997>. Acesso em: 24 mar. 2014.

BRASIL. *Lei Nº 9.099, de 26 de setembro de 1995*. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, 1995. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 17 mar. 2014.

_____. *Lei Nº 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 17 mar. 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; e dá outras providências. Brasília, 2012. Disponível em: <http:// http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 17 mar. 2014.

_____. *Projeto de Lei nº 2793/2011*. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Brasília, 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename =PL+2793/2011>. Acesso em: 17 mar. 2014.

_____. *Norma Nº 004, de 31 de maio de 2005*. Uso de meios da rede pública de telecomunicações para acesso à Internet. Brasília, 1995. Portaria nº 148, Ministério das Comunicações. Disponível em: <http://www.anatel.gov.br/hotsites/Direito_Telecomunica coes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf>. Acesso em: 17 mar. 2014.

_____. *Processo eletrônico/ petição eletrônica: perguntas mais frequentes*. Disponível em: <http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=1013#1>. Acesso em: 17 mar. 2014.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte geral 1*. 15ª ed. São Paulo: Saraiva, 2010.

BRITO, Auriney. *Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"*. Disponível em: <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em: 01 maio 2013.

CAPANEMA, Rafael. *CES aponta para futuro de computação vestível e objetos conectados*. 2014. Disponível em: <http://www1.folha.uol.com.br/tec/2014/01/1396196-ces-aponta-para-futuro-de-computacao-vestivel-e-objetos-conectados.shtml>. Acesso em: 17 mar. 2014.

CAPEZ, Fernando. *Curso de direito penal – parte geral. v.1*. 14ª ed. São Paulo: Saraiva, 2010.

CABETTE, Eduardo Luiz Santos. *Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático*. Jus Navigandi, Teresina, ano 18, n. 3493, 23 jan. 2013. Disponível em: <http://jus.com.br/revista/texto/23522>. Acesso em: 17 mar. 2014.

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. 2ª Ed. Rio de Janeiro: Lumen Juris, 2003.

CASTRO, Luiz Fernando Martins. Do governo eletrônico à ciberdemocracia. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coord.). *Manual de direito eletrônico e Internet*. São Paulo: Lex Editora, 2006. p. 326-337.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT.br. *Cartilha de segurança para Internet, versão 4.0*. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 17 mar. 2014.

CHACON DE ALBUQUERQUE, Roberto de Araújo. *A criminalidade informática*. 1ª. ed. São Paulo: Editora Juarez de Oliveira, 2006.

COLARES, Rodrigo Guimarães. *Cybercrimes: os crimes na era da informática*. Jus Navigandi, Teresina, ano 7, n. 59, 1 out. 2002 . Disponível em: <http://jus.com.br/revista/texto/3271>. Acesso em: 17 mar. 2014.

COSTA, Fernando José da. *Locus delicti nos crimes informáticos*. 2011. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/>. Acesso em: 17 mar. 2014.

COSTA, Marco Aurélio Rodrigues da. *Crimes de informática*. Jus Navigandi, Teresina, ano 2, n. 12, 5 maio 1997 . Disponível em: <http://jus.com.br/artigos/1826>. Acesso em: 17 mar. 2014.

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

_____. *Os crimes digitais e as Leis 12.735/2012 e 12.737/2012*. Boletim IBCCRIM, ano 21, n. 244, Março/2013.

DAOUN, Alexandre Jean. Crimes informáticos funcionais. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coord.). *Manual de direito eletrônico e Internet*. São Paulo: Lex Editora, 2006. p. 133-147.

FERREIRA, Ivete Senise. A criminalidade informática. In: LUCCA, Newton de; SIMAO FILHO, Abalberto (Coord.) et al. *Direito & internet: aspectos jurídicos relevantes*. Bauru: Edipro, 2001.

FILHO, Gilberto Farias de Sousa; ALEXANDRE, Eduardo de Santana Medeiros. *Introdução à computação*. João Pessoa: Curso de Licenciatura em Computação na Modalidade à Distância / UFPB, 2013.

FRAGOMENI, Ana Helena. *Dicionário enciclopédico de informática*. Rio de Janeiro: Campus, 1986.

GÓIS JÚNIOR, José Caldas. Regulamentação da Internet: legislar ou reciclar. In: KAMINSKI, Omar (Org.). *Internet legal: o direito na tecnologia da informação*. 1ª Ed. Curitiba: Juruá, 2005. p. 183-188.

GOMES, Helton Simões. *Bancos perdem R$ 1,5 bi com fraudes*. 2012. Disponível em: <http://www1.folha.uol.com.br/fsp/mercado/69329-bancos-perdem-r-15-bi-com-fraudes.shtml>. Acesso em: 17 mar. 2014.

GOMES, Luiz Flávio. *Lei "Carolina Dieckmann" e sua (in)eficácia*. Jus Navigandi, Teresina, ano 18, n. 3536, 7 mar. 2013 . Disponível em: <http://jus.com.br/revista/texto/23897>. Acesso em: 17 mar. 2014.

GRECO, Rogério. *Comentários sobre o crime de invasão de dispositivo informático: art. 154-A do Código Penal*. 2013. Disponível em: <http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 17 mar 2014.

GUIA DO HARDWARE. *A história da informática (parte 6: sistemas embarcados e supercomputadores)*. 2011. Disponível em: <http://www.hardware.com.br/guias/historia-informatica/eniac.html>. Acesso em: 17 mar. 2014.

HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.

IBOPE. *Brasil é o terceiro país em número de usuários ativos na internet*. 2013. Disponível em: <http://www.ibope.com.br/pt-br/noticias/paginas/brasil-e-o-terceiro-pais-em-numero-de-usuarios-ativos-na-internet.aspx>. Acesso em: 17 mar. 2014.

INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*. 2ª Ed. São Paulo: Editora Juarez de Oliveira, 2009.

JATOBÁ, João Felipe Brandão. *A falha da Lei nº 12.737/12: abrangência dos serviços telemáticos*. Jus Navigandi, Teresina, ano 17, n. 3444, 5 dez. 2012 . Disponível em: <http://jus.com.br/revista/texto/23172>. Acesso em: 17 mar. 2014.

KAMINSKI, Omar. Aspectos jurídicos que envolvem a rede das redes. In: KAMINSKI, Omar (Org.). *Internet legal: o direito na tecnologia da informação*. 1ª Ed. Curitiba: Juruá, 2005. p. 37-42.

LUCERO, Everton. *Governança da Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática*. Brasília: Fundação Alexandre de Gusmão, 2011.

MARTINS, Júlio César Werneck. O hackerismo e a defesa da propriedade virtual: o patrimônio da informação. In: JUNIOR, Roberto Roland Rodrigues da Silva (Org.). Internet e direito: reflexões doutrinárias. Rio de Janeiro: Lumen Juris, 2001. p. 165-190.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. Manual de direito penal, volume 1: parte geral, arts. 1º a 120 do CP. 24ª Ed. São Paulo: Atlas, 2008.

MONTEIRO, Marília. *A "Lei Carolina Dieckmann" e a mudança do paradigma da privacidade*. Disponível em: <http://observatoriodainternet.br/a-%E2%80%9Clei-carolina-dieckmann%E2%80%9D-e-a-mudanca-do-paradigma-da-privacidade>. Acesso em: 17 mar. 2014.

MOREIRA, Rômulo de Andrade. *A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário*. Jus Navigandi, Teresina, ano 17, n. 3443, 4 dez. 2012. Disponível em: <http://jus.com.br/revista/texto/23163>. Acesso em: 17 mar. 2014.

MOURA, Maísa. *Processo eletrônico já funciona em mais de 590 varas*. 2013. Disponível em: <http://www.cnj.jus.br/noticias/cnj/25427-processo-eletronico-ja-funciona-em-mais-de-590-varas>. Acesso em: 17 mar. 2014.

NUCCI, Guilherme de Souza. *Código Penal Comentado*. 14ª Ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, William César Pinto de. *Lei Carolina Dieckmann*. Jus Navigandi, Teresina, ano 18, n. 3506, 5 fev. 2013 . Disponível em: <http://jus.com.br/revista/texto/23655>. Acesso em: 17 mar. 2014.

OLIVEIRA JÚNIOR, Eudes Quintino de; OLIVEIRA, Pedro Bellentani Quintino de. *Entra em vigor a Lei Carolina Dieckmann*. Disponível em: <http://atualidadesdodireito.com.br/eudesquintino/2013/04/04/entra-em-vigor-a-lei-carolina-dieckmann/>. Acesso em: 17 mar 2014.

PINHEIRO, Patrícia Peck. *Direito digital*. 5ª Ed. São Paulo: Saraiva, 2013.

QUADROS, Jaqueline Maria. Governo eletrônico e direito administrativo. In: ROVER, Aires José (Org.). *Direito e informática*. Barueri, SP: Manole, 2004. p. 233-246.

RESINA, Jane. Desmistificação da Internet para advogados. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coord.). *Manual de direito eletrônico e Internet*. São Paulo: Lex Editora, 2006. p. 27-40.

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

SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: RT, 2003.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013.

TAKAHASHI, Tadao (Org.). *Sociedade da informação no Brasil: livro verde*. Brasília: Ministério da Ciência e Tecnologia, 2000.

THING, Lowell. *Dicionário de tecnologia* [tradução Bazán Tecnologia e Linguística e Texto Digital]. São Paulo: Futura, 2003.

VIEIRA, Victor. *Lei Carolina Dieckmann enfrentará dificuldades na prática*. 03 abr. 2013. Disponível em: <http://www.conjur.com.br/2013-abr-03/aplicacao-lei-carolina-dieckmann-enfrentara-dificuldades-tribunais>. Acesso em: 17 mar. 2014.

WORLD WIDE WEB. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2014. Disponível em: <http://pt.wikipedia.org/w/index.php?title=World_Wide_Web&oldid=38389841>. Acesso em: 17 mar. 2014.