UNIVERSIDADE DO SUL DE SANTA CATARINA

MAYUMI ARIMURA DE MELO

OS MECANISMOS UTILIZADOS NA FRAUDE ELETRÔNICA INERENTE AO *INTERNET BANKING* SEGUNDO CLAUDIO ANTÔNIO DE PAIVA SIMON: *SCAM, PHISHING* E *PHARMING*

Araranguá

2013

MAYUMI ARIMURA DE MELO

OS MECANISMOS UTILIZADOS NA FRAUDE ELETRÔNICA INERENTE AO *INTERNET BANKING* SEGUNDO CLAUDIO ANTÔNIO DE PAIVA SIMON: *SCAM, PHISHING* E *PHARMING*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade do Sul de Santa Catarina, como requisito parcial à obtenção do Bacharel em Direito.

Orientador: Prof. Dr. Diego Archer de Haro

Araranguá

2013

MAYUMI ARIMURA DE MELO

OS MECANISMOS UTILIZADOS NA FRAUDE ELETRÔNICA INERENTE AO *INTERNET BANKING* SEGUNDO CLAUDIO ANTÔNIO DE PAIVA SIMON: *SCAM, PHISHING* E *PHARMING*

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito da Universidade do Sul de Santa Catarina.

Araranguá, 13 de junho de 2013.

_____

Professor e orientador Diego Archer de Haro
Universidade do Sul de Santa Catarina

_____

Prof. Fátima Hassan Caldeira, MsC.
Universidade do Sul de Santa Catarina

_____

Prof. José Adilson Cândido.
Universidade do Sul de Santa Catarina

Dedico este trabalho à minha mãe Rose e minha avó Antonia, que sempre me deram força para que eu alcançasse meus objetivos, me apoiando da forma mais sincera possível, fazendo com que eu aprendesse com meus erros e me orgulhasse de minhas conquistas, cada uma com suas qualidades, e com a essência mais pura que já vislumbrei em minha vida, deram coragem para tornar real a pessoa que sou hoje.

AGRADECIMENTOS

Agradeço a Deus, pelos momentos de reflexão e de paz que oportunizaram a concentração e disposição necessária para que meu objetivo se tornasse realidade, além da chance de vislumbrar momentos que jamais imaginei viver em minha vida ao longo do curso.

À minha família, pelo apoio que me foi dado no decurso desta jornada, pela sua persistência quando eu tinha vontade de desistir, pela sua paciência quando eu demonstrava minhas indecisões, pelo seu carinho e amor quando eu necessitava de silêncio, pelo estímulo que me fez seguir em frente e concretizar meu ideal.

Agradeço também a uma pessoa que entrou em minha vida no decorrer do curso de Direito, e que me fez perceber que as coisas são mais simples do que parecem, e que guardam em si momentos que são inexplicavelmente eternos, sem os quais eu não poderia ter chegado ao fim do presente trabalho. Pelo amor, carinho, paciência e compreensão que esta pessoa, chamada João Paulo, proporcionou durante a elaboração desta pesquisa.

Aos meus professores, que ao longo do curso proferiram ensinamentos que não levarei somente para minha vida profissional, mas também para a pessoal, pois, tamanha determinação e conhecimento são dignos de permanecerem em minhas futuras conquistas.

À professora Fátima e ao professor e orientador Diego, pelas ideias, incentivos e exatidão na demonstração dos caminhos que deveria seguir para que, finalmente, chegasse à conclusão desta monografia.

Aos colegas de classe pela ajuda e demonstração de solidariedade na troca de materiais, nas ideias levantadas em aula, e pelos momentos vividos nestes cinco anos que jamais serão esquecidos.

E por último, mas não menos importantes, aos amigos que conquistei ao longo destes anos, Cássio, Lucas, Morgana e Thábata, que me oportunizaram momentos de alegria e de conhecimento, risadas e companheirismo, no meio da agitada vida acadêmica.

“O dinheiro é a essência alienada do trabalho e da existência do homem; a essência domina-o e ele adora-a.” (Karl Marx).

RESUMO

O presente trabalho trata do *scam*, *phishing* e *pharming*, mecanismos utilizados na fraude eletrônica que está presente no *Internet Banking*. Foram estudados os conceitos e exemplos que estão contidos no cotidiano da sociedade virtual, para proporcionar ao leitor uma leitura com maior veracidade e facilidade de compreensão. Por meio do método dedutivo de pesquisa, delimitando-se pela exploração, foi apresentada, no decorrer da leitura, a história da *internet*, visualizando a publicidade nela realizada e verificando os instrumentos utilizados naqueles mecanismos (*internet*, *World Wide Web* e correio eletrônico). Também houve a explicação sobre o que é o *Internet Banking* e a fraude eletrônica, a compreensão da tipificação das condutas efetuadas nestas fraudes antes da Lei n. 12.737/2012, observando as alterações trazidas por esta lei, bem como foram vislumbradas as condutas que a legislação brasileira está adquirindo com relação ao tema, além da análise dos mecanismos mencionados, e, por fim, foram estudados os métodos de prevenções que devem ser adotados pelos usuários da *internet*. Deste modo, foi observado que as condutas provocadas pelo *scam*, *phishing* e *pharming* eram tipificadas criminalmente em furto mediante fraude ou em estelionato antes da Lei n. 12.737/2012. Com o surgimento desta lei, este entendimento está começando a ter suas primeiras alterações. Tendo isto em vista, deve-se criar uma conscientização da população brasileira acerca das medidas preventivas, para que, desta forma, haja a diminuição da incidência da fraude eletrônica no *Internet Banking*.

Palavras-chave: fraude eletrônica; *internet banking*; *scam*; *phishing*; *pharming*.

ABSTRACT

The current paper talks about scam, phishing and pharming, mechanisms used on electronic fraud which can be found on Internet Banking. Concepts and examples that are inserted everyday in the virtual society were studied to give to the reader an easier and truthful reading for better comprehension. By deductive rearch, delimited by exploration, it was submitted, along the reading, the history of internet, viewing the advertisement done on it and checking the tools used on those mechanisms (internet, World Wide Web and the electronic mail). Also, it is explained what are Internet Banking and electronic fraud, the understanding of the typification of the behaviors on those frauds before Law # 12.737/2012 (Lei n. 12.737/2012), it can be noticed the changes brought by this law, as well as the behaviors that the Brazilian legislation is acquiring related to the theme, besides the analysis of the mentioned mechanisms, and, finally, the methods of control that should be taken by internet users were studied. It can be noticed that the behaviors caused by scam, phishing and pharming were typified criminally for theft by fraud or larceny before Law # 12.737/2012 (Lei n. 12.737/2012). With the emergence of this Law, this understading is beginning to have it's first changes. With this in mind, a awareness of the Brazilian population about those preventive measures must be created, so that in this way, there is a decreased incidence of electronic fraud in Internet Banking.

Keywords: electronic fraud; internet banking; scam; phishing; pharming.

LISTA DE ABREVIATURAS E SIGLAS

§	Parágrafo
ARPA	Advanced Research Projects Agency
Art	Artigo
BBN	Bolt Beranek and Newman
BITNET	Because It's Time Network
Bps	Bits por segundo
CAIS	Centro de Atendimento e Incidentes de Segurança
CP	Código Penal
DNS	Domain Name System
EUA	Estados Unidos da América
FAPESP	Fundação de Amparo à Pesquisa do estado de São Paulo
FEBRABAN	Federação Brasileira de Bancos
FERMILAB	Fermi National Laboratory
HEPNET	High Energy Physics Network
HTML	Hyper Text Markup Language
IBASE	Instituto Brasileiro de Análises Sociais e Econômicas
ICPs	Internet Service Providers
LAN	Local Area Network
LNCC	Laboratório Nacional de Computação Científica
NASA	National Aeronautics and Space Administration
NCSA	*National Center for Supercomputing Applications*
NPC	Network Control Protocol
NSF	National Science Fundation
NSFNET	National Science Fundation Network
RNP	Rede Nacional de Pesquisa
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal
TCP/IP	Transmission Control Protocol/Internet Protocol
TRF	Tribunal Regional Federal
UFRJ	Universidade Federal do Rio de Janeiro
UCLA	Universidade de Califórnia em Los Angeles

SUMÁRIO

1 INTRODUÇÃO

O grande avanço tecnológico dos últimos anos proporcionou à população mundial uma maior comodidade para o exercício de suas atividades. Além disso, a informação ficou mais viável, através de invenções como rádio, televisão, computador, entre outros.

Um dos meios resultantes deste avanço é a *internet*, que ultimamente vem sendo utilizada pela sociedade de forma cada vez mais comum, devido à sua facilidade de informações dispostas rapidamente ao usuário através de *sites* e *e-mails*, por exemplo.

Surgida em tempos de Guerra Fria, a *internet* tornou-se uma peça fundamental para a atualidade. Proporciona à pessoa que utiliza deste recurso assuntos que podem ser tanto de caráter estudantil, como de caráter comercial, demonstrando sua diversidade nos temas abrangidos.

As empresas, visando à obtenção de maiores lucros, mediante publicidade facilitada, acabaram aderindo a este mundo virtual, tendo em vista a economia e o maior raio de alcance aos consumidores que são demonstrados pelo mesmo, permanecendo, desta forma, por mais tempo no mercado comercial.

Contudo, nem todos se utilizam da *internet* como uma ferramenta para crescimento financeiro de boa-fé. Consequentemente, houve o surgimento da fraude eletrônica, utilizada por pessoas de má-fé com a intenção de ludibriar outrem através desta ferramenta que caiu no uso diário da população brasileira.

Com o desenvolvimento da publicidade eletrônica, as instituições financeiras acharam um lugar onde poderiam oportunizar aos seus clientes operações bancárias em seu próprio computador, como o pagamento de uma conta, ou a transferência de dinheiro entre contas bancárias, sem necessitar de seu deslocamento até o banco. Eis que então surgiu o denominado *Internet Banking*, que facilmente caiu na visão dos criminosos, objetivando a aquisição de dinheiro fácil através da supracitada fraude eletrônica.

É importante, deste modo, que a sociedade tenha conhecimento dos riscos que estão presentes na *internet* diariamente, principalmente no *Internet Banking*, por se tratar do dinheiro do cliente, sem o qual se tem sabedoria de que não haveria uma vida sem preocupações com suas necessidades vitais no mundo capitalista vivido atualmente.

Mas de que forma a fraude eletrônica age no *Internet Banking*? Como elas chegam até o usuário? Estas perguntas, caro leitor, serão respondidas no decorrer da leitura do presente trabalho acadêmico, com exemplos extraídos do dia-a-dia da população brasileira.

Mas, tal fraude utiliza-se de determinados mecanismos para se concretizarem. Claudio Antônio de Paiva Simon traz à tona, no artigo denominado como "Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil", o *scam*, o *phishing* e o *pharming*, intitulados no título do texto como fraudes, mas que, na verdade, devem ser chamados de "mecanismos", tendo em vista que eles proporcionam, como será visto, ao criminoso, a concretização do que realmente se trata uma fraude.

Referidos mecanismos são os principais responsáveis pela fraude eletrônica inerente ao *Internet Banking*. Mas afinal, como funcionam? De que forma os criminosos responsáveis pela disseminação destas fraudes são condenados? Como o usuário poderá se prevenir?

Através do método dedutivo de pesquisa, delimitando-se pela exploração, o presente trabalho explicará estes e outros temas que cercam a fraude eletrônica inerente ao *Internet Banking*, apresentando o histórico da utilização da *internet* no ambiente comercial, explicando o que é a fraude eletrônica, compreendendo o *Internet Banking*, verificando, deste modo, os mecanismos que concretizam esta fraude eletrônica no *Internet Banking*, e estudando medidas preventivas cabíveis nestes casos, através de pesquisa que traz consigo informações atuais, entendimentos doutrinários e jurisprudenciais, e exemplos práticos e facilmente identificáveis no dia-a-dia da sociedade virtual.

Para isto, este trabalho foi dividido em três capítulos, iniciando pelo surgimento da *internet* no mundo e no Brasil, visualizando conceitos importantes ao tema, como o *World Wide Web* e o correio eletrônico, entendendo a publicidade realizada no ambiente virtual, principalmente a relacionada às instituições bancárias, passando para a tipificação das condutas praticadas na fraude eletrônica antes da Lei n.º 12.737/2012, que trata sobre os delitos informáticos, e, posteriormente, abordando esta nova lei, verificando as alterações trazidas pela mesma, assim como a legislação que acompanha o meio eletrônico no Brasil com maior força, revelando, ademais, os mecanismos até aqui mencionados, e, por fim, trazendo soluções preventivas para que o usuário não seja vítima destes criminosos virtuais, como poderá ser vislumbrado na presente leitura.

2 DOS PRIMÓRDIOS DA *INTERNET* À SUA RELAÇÃO BANCÁRIA

2.1 O DESENVOLVIMENTO DA *INTERNET* E SUA CHEGADA AO BRASIL

2.1.1 O surgimento da *internet*

Em meio a Guerra Fria, a União Soviética obteve uma grande diferença em relação aos EUA na corrida espacial, colocando em órbita o primeiro satélite espacial, denominado *Sputnik*, em 1957.

Deste modo, o Departamento de Defesa dos Estados Unidos, através da NASA, criou em 1958 a ARPA, objetivando o desenvolvimento da pesquisa científica e tecnológica em bases militares. (GUIZZO, 2002, p. 16).

Em 1969, a ARPA, a fim de conectar os departamentos de pesquisa americanos, desenvolveu a rede ARPANET. Segundo Kellen Cristina Bogo (2013), esta funcionava "com um *Back Bone* [sic] que passava por baixo da terra (o que o tornava mais difícil de ser interrompido), ela ligava os militares e pesquisadores sem ter um centro definido ou mesmo uma rota única para as informações, tornando-se quase indestrutível".

O *backbone* nada mais é do que a espinha dorsal da *Internet*. Trata-se da rede principal por onde os dados de todos os clientes da Internet passam, sendo atualmente a responsável por possibilitar o envio e recebimento de dados entre países (MARTINS, 2009).

Em 1968, houve o desenvolvimento do sistema de comutação de pacotes pela empresa BBN, dando assim mais forma à ARPANET. "Em 1969, quatro universidades norte-americanas foram escolhidas para funcionar como nós da ARPANET: Universidade da Califórnia em Los Angeles, Universidade Stanford – através do Stanford Research Institute -, Unidade da Califórnia em Santa Barbara e Universidade de Utah" (GUIZZO, 2002, p. 19).

Para melhor esclarecer, a comutação de pacotes significa:

> [...] Em redes de computadores modernas, o originador fragmenta mensagens longas em porções de dados menores denominadas pacotes. Entre origem e destino, cada um desses pacotes percorre enlaces de comunicação e comutadores de pacotes (há dois tipos principais de comutadores de pacotes: roteadores e comutadores de camada de enlace). Pacotes são transmitidos por cada enlace de comunicação a uma taxa igual à de transmissão total do enlace. (KUROSE; ROSS, 2010, p. 22)

Um ano depois, outras universidades americanas e outras instituições do país que exerciam trabalhos relacionados à defesa obtiveram permissão para se conectar à ARPANET.

No final do mesmo ano, a rede tinha se desenvolvido tanto que seu NCP, que era o seu protocolo de comutação de pacotes original, passou a ser inadequado (BOGO, 2013).

Segundo Guizzo (2002) e Bogo (2013), no ano de 1983 houve a primeira transição do protocolo da ARPANET, passando de NCP para TCP/IP. Este novo protocolo interessou a Universidade da Califórnia em Berkeley, que o incorporou ao seu sistema operacional Unix BSD. O TCP/IP oferecia um crescimento ilimitado da rede, além de uma facilidade na execução de várias plataformas diferentes de *hardware* de computador.

Em 1986, o protocolo TCP/IP foi adotado pela NSFNET, criada pela NSF. Assim, esta nova rede acabou se tornando uma ampla rede acadêmica, englobando a ARPANET, a qual restou extinta em 1990. Ademais, a rede anunciou, no ano de 1991, a liberação de seu uso para fins comerciais (tendo em vista que anteriormente, era utilizada apenas para fins acadêmicos), gerando grandes investimentos pelo setor privado com relação a estrutura da rede. (GUIZZO, 2002, p. 20-21).

Nas palavras de Érico Marui Guizzo (2002), "esse emaranhado de redes acadêmicas, comerciais e militares, tendo como espinha dorsal a NSFNET e como protocolo patrão o TCP/IP, acabou evoluindo para o que hoje conhecemos como Internet".

2.1.2 O início da *internet* no Brasil

Assim como nos Estados Unidos, a *internet* no Brasil deu seus primeiros passos no meio acadêmico. Pesquisadores e professores que tinham o privilégio de estudar em universidades no exterior conheceram as redes de comunicação internacionais. Por meio disto, trouxeram ao Brasil seu conhecimento, destacando a rede BITNET (GUIZZO, 2002, p. 23).

Obviamente, não se pode deixar de dar grande destaque à rede NSFNET, que, além da grande aprovação nos Estados Unidos, também foi bem recebida pelos brasileiros. Michael Stanton (1993) fez uma breve diferenciação destas grandes redes, ressaltando que:

> A BITNET era uma rede de *mainframes*, que transportava mensagens de correio eletrônico usando tecnologia desenvolvida com outro propósito pela IBM. [...] A NSFNET, por outro lado, faria parte da Internet, usando a família de protocolos TCP/IP, desenvolvida dentro dos projetos da Defense Advanced Research Projects Agency (DARPA) , e que permitiria praticamente qualquer tipo de aplicação via rede, e especialmente o uso interativo de computadores remotos (TELNET), a transferência de arquivos (FTP) e, já nos anos 90, a consulta interativa de bases de informação (WWW), além do correio eletrônico, é claro.

Foi então realizado, em setembro de 1988, o primeiro acesso à BITNET no Brasil, tendo sido exercido pelo LNCC, localizado no Rio de Janeiro, estabelecendo uma conexão de 9.600 bps através da Universidade de Maryland (GUIZZO, 2002).

Após, surgiram mais duas conexões que ficaram conhecidas na história da *internet* no Brasil. Instalada em novembro de 1988, dois meses após o primeiro acesso, a FAPESP intermediou uma conexão de 4.800 bps com o FERMILAB de Chicago, permitindo o acesso não somente à BITNET, mas também à HEPNET. A última conexão conhecida pela inicialização da *internet* no país foi uma de mesma velocidade, efetivada entre a UFRJ e a UCLA, em maio de 1989, sendo esta independente à BITNET (STANTON, 1993).

Na figura a seguir, podemos visualizar como as conexões de redes privadas se encontravam no país no final do ano de 1991, destacando-se a FAPESP e o LNCC:

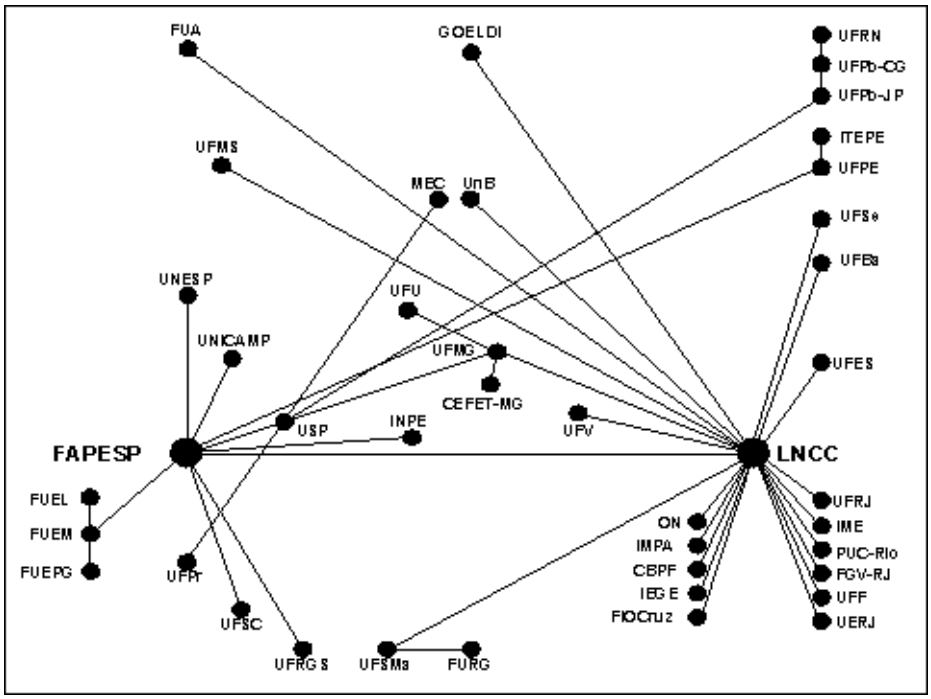

Imagem 1 - Conexões Usadas para a Rede Nacional em 1991 (Fonte: Stanton, 1993).

Outra ligação deveras importante, entre as demais pioneiras, é a realizada pela Alternex, que, em julho de 1989, foi ligada ao IBASE, que se trata de uma organização não governamental que se conectou às rede USENET, por meio de uma linha discada internacional (HISTÓRIA..., 2013).

O IBASE foi fundado em 1981, com o objetivo de disseminar informações à sociedade civil. Com a ligação ao Alternex, tornou-se o primeiro serviço brasileiro de acesso à *internet* fora da comunidade acadêmica (GUIZZO, 2002, p. 24).

Em junho de 1992 houve outro grande passo para a *internet*. O IBASE, na Conferência Mundial sobre Meio Ambiente e Desenvolvimento (UNCED-92), assinou um convênio com a Associação para o Progresso das Comunicações, com a finalidade de

conceder às ONGs brasileiras o acesso à *internet*. Também foi nesta conferência onde começou a ser operada a Rede Rio, o segundo ponto brasileiro de acesso à internet, que serviu de exemplo para outros estados brasileiros (PERSEGONA; ALVES, 2013).

No segundo semestre do referido ano, houve a montagem gradativa de uma nova rede, compreendendo a RNP, o *backbone* brasileiro, ligando dez capitais do país a Brasília, com uma infraestrutura disponibilizada pela EMBRATEL (PERSEGONA; ALVES, 2013).

Eis que, a partir de então, a *internet* começou a espalhar-se em outros estados nacionais, começando a ser utilizado também, em maior escala, para fins comerciais, além dos acadêmicos, em um longo processo, até chegar ao que possuímos atualmente.

2.2 ANÁLISE CONCEITUAL DA *INTERNET*, *WORLD WIDE WEB* E CORREIO ELETRÔNICO

2.2.1 *Internet*: a ferramenta

Conforme Houaiss e Villar (2009, p. 1098) a *internet* refere-se a "rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum, unindo usuários particulares, entidades de pesquisa, órgãos culturais, institutos militares, bibliotecas e empresas de toda envergadura".

Esta rede de computadores possui, atualmente, diversos sistemas finais, deixando a velha percepção de que são apenas os computadores de mesa ou estações de trabalho. No nosso dia-a-dia, os sistemas finais englobam também as televisões, *laptops*, consoles para jogos (como o Playstation, desenvolvido pela Sony, e o Xbox, criado pela Microsoft), telefones celulares, *webcams*, automóveis etc. Podemos perceber que, na verdade, o termo "rede de computadores" está ficando, de certa forma, desatualizado (KUROSE; ROSS, 2010, p. 2).

Os sistemas finais possuem o acesso à *internet* através de Provedores de Serviços de Internet (ICPs). Estes ICPs proporcionam aos sistemas finais uma série de tipos de dados à rede, abrangendo o acesso residencial, por exemplo, por modem discado de 56 kbps, de banda larga, acesso por LAN (redes locais) de alta velocidade, ou a *internet* sem fio (KUROSE; ROSS, 2010, p. 4).

Para melhor esclarecer, Patrícia Peck Pinheiro (2010, p. 102) descreve os referidos provedores da seguinte forma:

> O que é um Provedor de Acesso? Resumidamente, é uma empresa prestadora de serviços de conexão à Internet, agregando a ele outros serviços relacionados, tais

> como *e-mail*, *hosting* de páginas *web* ou *blogs*, entre outros, que detém ou utiliza determinada tecnologia, linhas de telefone e troncos de telecomunicação próprios ou de terceiros.

Ademais, é através do protocolo TCP/IP que há a interligação dos computadores ligados à *internet.* Utiliza-se, para isto, a chamada comutação de pacotes para que haja a transmissão de informações em pequenos pedaços. Estes pequenos pedaços são denominados "pacotes", esclarecendo assim o termo utilizado (GUIZZO, 2002, p. 33).

Na verdade, o TCP/IP trata-se de dois protocolos, o TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão) e o IP (*Internet Protocol* – Protocolo de Internet), sendo os mais importantes da *internet*. Este último é responsável pelo formato dos pacotes que serão enviados e recebidos por meio de roteadores e sistemas finais (KUROSE; ROSS, 2010, p. 4).

Um protocolo, nas palavras de Guizzo (2002), trata-se de um conjunto de regras, padrões e especificações que devem ser seguidos para que os computadores comuniquem-se perfeitamente.

Seguindo a mesma linha, Kurose e Ross (2010, p. 6) mencionam que "todas as atividades na Internet que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo".

Deste modo, conhecendo a *internet* e sua funcionalidade, faz-se necessário a compreensão de alguns atributos que serão de fundamental utilização no último capítulo do presente trabalho, o *World Wide Web* e o correio eletrônico.

2.2.2 *World Wide Web*

Também conhecida como *WWW*, *W3* ou *Web*, "a World Wide Web foi criada em 1991 no CERN (Laboratório Europeu de Física de Partículas), na Suíça, pelo físico Tim Berners-Lee. O termo *World Wide Web* pode ser entendido como "teia de alcance mundial", de acordo com Guizzo (2002, p. 72). Há que se abrir um pequeno parênteses referente à data, eis que alguns autores, como Maria Clara Aquino (2013, p. 5), afirmam que o ano de criação na verdade se deu em 1989, ou seja, um ano após a chegada da *internet* ao Brasil.

Existe uma diferença básica entre a *internet* e a *World Wide Web.* O primeiro disponibiliza a ligação entre computadores, objetivando o transporte de informações. Já o segundo refere-se a um sistema de documentos hipertexto que estão interligados (NUNES, 2012).

Vannevar Bush, físico e matemático australiano, publicou em seu artigo *As We May Think*, no ano de 1945, um esboço do *Memex*, um instrumento que pode ser comparado, atualmente, com um computador pessoal. Foi através desse esboço que surgiu o hipertexto, "[...] um conjunto de nós ligados por conexões. Os nós podem ser palavras, páginas, imagens, gráficos ou partes de gráficos, seqüências [sic] sonoras, documentos complexos que podem eles mesmos ser hipertextos" (AQUINO, 2013, p. 2-3).

Porém, somente em 1993 foi possível visualizar imagens na *World Wide Web*, por meio de um programa chamado *Mosaic*, desenvolvido por estudantes do NCSA, possibilitando assim a efetividade do hipertexto (GUIZZO, 2002, p. 73).

Por se tratar da versão multimídia da *internet*, as imagens e gráficos que eram transferidas na *Web*, quando havia sido recém-criada, representavam uma grande sobrecarga para a infraestrutura de comunicação de dados, fato este que foi superado com o surgimento de tecnologias mais eficientes e de baixo custo (POPULARIZAÇÃO..., 1997, p. 16).

A importância da *Web* se dá, atualmente, pelo acesso de informações controlado e personalizado, de acordo com os interesses do usuário, possibilitando uma facilidade na localização de serviços comerciais, como a venda de livros, roupas, alimentos, serviços de home-banking etc. (POPULARIZAÇÃO..., 1997, p. 17).

As páginas da *Web* ficam armazenadas em poderosos computadores que permanecem com uma conexão contínua com a *internet*. Por servirem informações, esses computadores são denominados "servidores". Um conjunto dessas páginas contido em um servido é chamado de *website* (GUIZZO, 2002, p. 75).

Um *websit*e (também denominado como *site* ou sítio eletrônico) é o local onde é fornecido informações acerca do que for de interesse de seu criador. A junção de todos os w*ebsites* já criados formam a *World Wide Web*.

Para ter acesso a um *website*, é necessária a utilização de um programa chamado *browser* (também conhecido como "navegador"). Este programa permite que seus usuários possam interagir com documentos HTML (INTERNET..., 2013).

O HTML é um arquivo de texto que contem pequenas *tags* de marcação que indicam ao navegador *web* como deve ser mostrada a página (DAPONT, 2013).

Quando o usuário de um navegador visualiza um *website*, ele observa uma série de imagens. O documento HTML, no caso, não aparece, mas pode ser localizado no código fonte da página.

2.2.3 Correio eletrônico

O correio eletrônico nasceu juntamente com os primórdios da *internet*. Seu objetivo era facilitar a transmissão de informações entre os pesquisadores que elaboravam a rede entre várias instituições americanas. Seu uso foi rapidamente disseminado quando a *internet* passou a ser usufruída no meio acadêmico. No Brasil, uma das primeiras instituições a utilizar o serviço foi o IBASE (POPULARIZAÇÃO..., 1997, p. 47).

Ana Amélia Menna Barreto (2003) caracteriza o correio eletrônico como "[...] um meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores, onde cada usuário possui um endereço eletrônico para se corresponder".

Esse sistema possui a mesma finalidade do correio tradicional, ou seja, enviar informações a um destinatário. Uma das diferenças é o tempo, pois, enquanto no correio tradicional levaria dias para entregar uma correspondência do Brasil para, por exemplo, um destinatário localizado no Japão, no eletrônico a mesma informação pode chegar em segundos, no mais tardar em minutos, a partir do momento em que a mensagem foi enviada (GUIZZO, 2002, p. 59).

Referente ao seu funcionamento:

> O funcionamento do correio eletrônico é muito simples. Quando você envia uma mensagem para um destinatário, seu computador prepara e formata essa imagem segundo os padrões aceitos pela rede e envia para o seu provedor de acesso. O computador do provedor de acesso analisa o endereço eletrônico do destinatário para verificar se é o endereço de um assinante desse provedor. Em caso positivo, a mensagem é colocada na caixa postal desse assinante, que irá recebê-la assim que acessar sua (dele) caixa postal. No caso contrário a sua mensagem é enviada para o próximo computador de rede, situado no "provedor" do seu provedor. Esse processo de reenvio é repetido, com a mensagem "pulando" de computador em computador até que um deles reconheça o endereço eletrônico do destinatário (POPULARIZAÇÃO..., 1997, p. 50).

Essas mensagens que são enviadas pelo correio eletrônico são denominadas *e-mail*. Assim como em todos os serviços disponíveis na internet, o *e-mail* utiliza-se do protocolo TCP/IP para enviar a mensagem criada (LEITÃO JÚNIOR, 2002).

Como dito por Barreto (2003), no conceito supracitado, cada usuário possui um endereço eletrônico. Leitão Júnior demonstra a estrutura de um endereço eletrônico da seguinte forma: nome do usuário, símbolo arroba ("@", que significa, em português, "em"), e o nome do provedor (local onde se localiza a caixa de entrada do correio eletrônico ou *webmail*).

Deste modo, o endereço eletrônico acaba se tornando a "identidade" do usuário, meio pelo qual será identificado por outras pessoas, pois, não há como existir dois ou mais endereços eletrônicos idênticos.

Segundo Castro (2005), o *webmail* "[...] é uma aplicação acessada diretamente na Internet, sem a necessidade de usar programa de correio eletrônico". Atualmente, há diversos *sites* que disponibilizam tal serviço, tais como Hotmail (www.hotmail.com), Gmail (www.gmail.bom), Yahoo! (br.yahoo.com), Bol (www.bol.com.br), entre outros.

É importante tomar tamanho conhecimento sobre correios eletrônicos, pois, é dessa forma que o *spam*, tema a ser abordado no presente trabalho, se prolifera, afetando diversos usuários do sistema.

2.3 A FACILIDADE PROPORCIONADA PELA PUBLICIDADE NA RELAÇÃO BANCÁRIA VIRTUAL

2.3.1 *Marketing* eletrônico

A primeira aparição da publicidade na *internet* se deu com a criação do *World Wide Web*, onde Dale Dougherty lançou a primeira publicação comercial, denominada *GNN*, que se tratava de uma espécie de revista eletrônica *on-line*. Através do programa *Mosaic*, foi possível o acesso de sites pioneiros na publicidade, como o *Mercury Center*, *Hotwired* e *Internet Shopping Network*, que tiveram, entre seus primeiros anunciantes, a Microsoft e o MCI (PINHO, 2000, p. 101).

Na visão de Pinho (2000, p. 102), com o surgimento de vários sites de diretórios e mecanismos de busca na *Web*, os usuários ganharam a facilidade de encontrar *sites* de organizações comerciais, e o conforto para fazer suas compras em lojas listadas nas famosas Páginas Amarelas. Este fato proporcionou grande atenção e interesse das empresas, que perceberam que a *internet* possuía um novo meio para novas oportunidades de crescimento, elevando assim o número de *sites* comerciais na rede.

Atualmente, o *marketing* eletrônico pode ser visualizado de duas formas: *websites* próprios, ou seja, a própria empresa cria um *site* onde é fornecido ao cliente informações sobre os produtos, suas características, história e localização da empresa, rede de assistência técnica, podendo proporcionar, caso seja de interesse da empresa, a opção de venda *on-line* ao seu cliente. A outra forma observada é o portal eletrônico, local onde o usuário/cliente adquire várias informações e serviços em um único lugar. Um bom exemplo para o caso é o UOL

(www.uol.com.br), que oferece serviços de *e-mail*, informações do que acontece no mundo em tempo real, além de diversas propagandas que estão contidas no *site*, sendo que é desta maneira que percebe sua renda (BARREIRA; LASALVIA, 2013, p. 6).

Para obter um sucesso favorável no meio virtual, é necessário que a empresa desenvolva suas estratégias publicitárias observando os seguintes pontos essenciais ao *marketing de* forma diferenciada: política do produto, política de pesquisa e desenvolvimento, política de pesquisa de mercado, pesquisa de origem de clientes, pesquisa de satisfação do cliente, política de processos, política de pessoas, política de precificação, política de negociação de preços, política de instalações, política de disponibilização, política de relações públicas, política de propaganda, política de vendas e política de parcerias (CARVALHO; GALLAS; PADINHA, 2007).

Mas por que se deve olhar estas políticas e pesquisas de forma diferenciada da tradicional? Porque o objetivo da publicidade na *internet* é diverso. O seu público alvo são usuários que possuem um grande "leque" de opções em poucos "cliques" na rede. Tudo está facilitado ao seu cliente, desde a chance de compras sem sair de casa, até a oportunidade de conhecer outras empresas do mesmo ramo, com condições melhores apresentadas do que outras. Tornou-se uma verdadeira guerra pela melhor publicidade na rede.

Mas, como é possível vislumbrar, há várias vantagens ao cliente com o *marketing* eletrônico, como: o baixo custo; a interação com cada cliente individualmente, adaptando produtos e serviços as suas necessidades; e a formação de bancos de dados com as informações disponibilizadas pelo cliente (BARREIRA; LASALVIA, 2013, p. 7).

O *marketing* eletrônico gerou aos usuários da *internet*, então, uma grande facilidade e conforto para a obtenção de produtos e serviços, entre eles, o *Internet Banking*, como será visto no assunto abordado a seguir.

2.3.2 *Internet Banking*

A relação entre o banco e a *internet* adveio, primordialmente, nas formas de *Home Banking* e *Office Banking.* O primeiro trata da relação entre o cliente que é pessoa física e a realização de operações bancárias pela *internet*. Já o segundo, trata-se do mesmo, entretanto a relação se faz com a pessoa jurídica (BANRISUL, 2013).

No ano de 1999, foi constatado que uma transação financeira realizada em uma agência bancária convencional custava dez vezes mais do que a mesma transação realizada remotamente, por meio do *Home* ou *Office Banking* (SÊMOLA, 1999).

Entretanto, a utilização desses serviços dava-se através da instalação de aplicativos no computador do cliente, bem como do licenciamento do banco fornecedor do serviço. Deste modo, o *Internet Banking* surgiu para facilitar a vida do cliente bancário, tendo em vista que o licenciamento é por meio de registro de senhas, e o acesso é diretamente pela *internet*, trazendo uma grande comodidade para o cliente, e economia para o banco (NEUBUSER et al., 2013).

Segundo Silva et al. (2006, p. 78), o "Internet Banking é o termo utilizado para caracterizar transações bancárias via internet, através de uma página segura do banco. Essas transações podem ser pagamentos, transferências, consultas a extratos etc."

A seguir pode-se analisar o crescimento do *Internet Banking*, e o desuso do *Home* e *Office Banking*, progressivamente:

MODALIDADE	1999	2000	2001	Variação –01/00
Clientes com Internet/home banking	4,3	6,8	2,4	-64,9%
Clientes com Internet/Office banking	0,6	1,5	1,3	-13,25%
Clientes com Internet banking	-	8,3	13,0	56,63%
Clientes com acesso a Centrais telefônicas de serviços	42,6	52,4	57,4	9,54%
Consultas às URA (Unidades de Resposta Audível)	744,01	164,01	328,4	14,12%

Tabela 1 – Comparativo entre *Home*, *Office* e *Internet Banking* em milhões (Fonte: Febraran apud Neubuser et al, 2003).

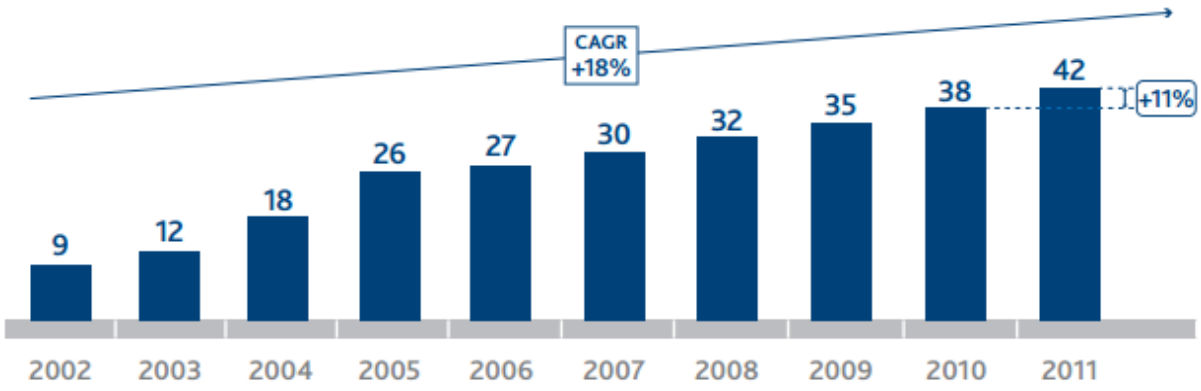

Gráfico 1 – Contas correntes com *Internet Banking* em milhões (Fonte: Febraban e Bacen, 2011).

Com o aumento crescente do uso da *internet* no Brasil, os fatos sobre o crescimento do *Internet Banking* no país tem tido cada vez mais confirmação e apreciação pelos clientes bancários brasileiros. A praticidade e comodidade oferecida pelo serviço têm atraído tantos usuários que o país está chegando ao patamar de grandes países, como EUA, Reino Unido e Alemanha.

Tal fato pode ser vislumbrado no presente gráfico, que aborda, em percentuais, as contas com *Internet Banking* sobre as contas ativa no Brasil:

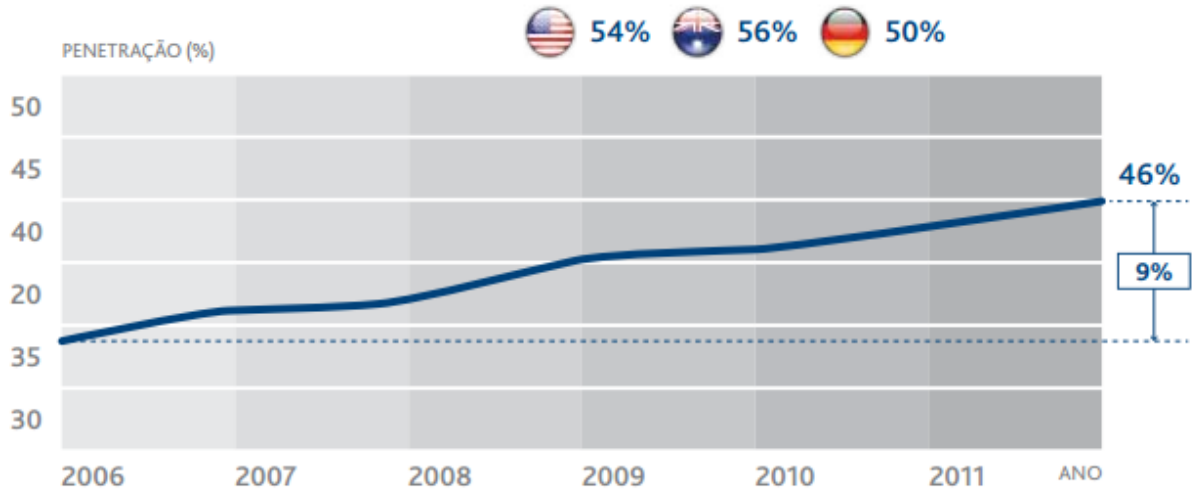

Gráfico 2 – Penetração de *Internet Banking* no Brasil (Fonte: FEBRABAN, IBGE, Nilsen e TIC, 2011)

As operações bancárias na *internet* proporcionam:

> a) diminuição de custos fixos de manutenção de uma agência bancária, especificamente nas despesas de pessoal;
> b) desburocratização de serviços, facilitando a vida do cliente, dispensando sua presença física no estabelecimento, evitando filas e perda de tempo realizando operações bancárias;
> c) o alcance geográfico, pelo fado da Internet atingir o mundo todo, podendo fornecer serviços em grande escala;
> d) diminuição de riscos de assaltos, porque há um menor movimento de pessoas, moeda e serviços nas agências bancárias (ESTRADA, 2005).

A evolução do uso do *Internet Banking* acarretou uma melhor qualidade nos serviços prestados pelas instituições financeiras, exigindo destas maiores projetos, além de fornecer ao consumidor um maior conhecimento sobre o funcionamento do serviço com comodidade (SILVA et al, 2006, p. 79).

Mas, assim como há pontos positivos, aduz Silva et al (2006, p. 79) que também há pontos negativos no uso desse serviço. A segurança na *internet* é um algo que ainda está em desenvolvimento. Por haver falhas na segurança, há programas para fraudar senhas, espalhar vírus, identificar fragilidades, entre outros, que acabam colocando em risco os aspectos positivos do *Internet Banking*.

2.4 ANÁLISE CONCEITUAL DA FRAUDE ELETRÔNICA

A fraude, em si, segundo entendem Houaiss e Villar (2009, p. 927), significa "qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever [...]".

Utilizando-se da ferramenta denominada *internet*, houve o surgimento da fraude eletrônica, também denominada como fraude informática ou informatizada.

Este delito significa o uso ilícito de sistema informático ou telemático a fim de obter injustamente proveito patrimonial de outrem (ROSA, 2005, p. 65).

Gil (1999, p. 15), conceitua esta espécie de fraude da seguinte forma:

> Fraude informatizada corresponde à ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (*software* e bancos de dados), de propriedade de pessoa física, ou jurídica, concretizada por entidade física, ou jurídica com o objetivo de alcançar benefício, ou satisfação psicológica, financeira, material.

A fraude eletrônica possui duas origens: a interna e a externa. A primeira refere-se à fraude praticada por funcionário ou terceiro que está dentro do local onde ocorrerá a mesma. Já a segunda se aduz quando o fraudador não possui vinculo com o local que será fraudado (PINHEIRO, 2010, p. 311).

Segundo Gil (1999, p. 15), a segunda origem da fraude eletrônica é dificilmente ocorrida de forma exclusiva. Tal fato se justifica pela força dos controles lógicos informatizados, que são disponibilizados pelos fornecedores de *software* e de *hardware* atualmente.

Deste modo, resta claro que o fraudador possui um ótimo conhecimento técnico em informática, conhecimento este que vai além do que o usuário convencional da *internet* possui, sabendo a forma e a estrutura dos meios utilizados por este usuário no vasto mundo informatizado.

Assim, Gil (1999, p. 18) complementa informando que a esta modalidade de fraude se classifica em: fraudes dos funcionários (fácil identificação, maior número de ocorrências, e menor impacto à continuidade de operações); fraudes por quadrilha (difícil identificação, ocorrendo mais raramente, e causadora de forte impacto na empresa, sendo que, uma vez instalada, possui longa duração, atingindo a lucratividade e capacidade de competitividade da organização); e fraudes das chefias (dificuldade na punição dos fraudadores, grandes prejuízos às empresas fraudadas, e apurações das fraudes descontinuadas pelo surgimento de irregularidades cometidas pela direção da organização prejudicada).

Segundo Nogueira (2008, p. 61-62), numa visão geral sobre os delitos informativos, os agentes causadores destes são:

a) *Hacker*: utiliza-se de seu grande conhecimento em informática para invadir *sites*, para seu entretenimento, e não a fim de criminalizar, disputando com outros de sua categoria para deixar páginas ou sistemas da *internet* vulneráveis e demonstrar sua capacidade.
b) *Cracker*: normalmente são vários jovens reunidos que formam quadrilhas com a finalidade de cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos, contra pessoas físicas ou jurídicas, órgãos públicos, entre outros.
c) *Phreaker*: especialista em burlar sistemas de telefonia fixa ou móvel.
d) *Spammers*: pessoas e empresas que enviam e-mails indesejados, de forma a lotar a caixa de entrada dos correios eletrônicos das vítimas, com propagandas de lojas, revistas para assinatura, produtos em geral etc. Em 2008, o Brasil foi considerado o 4º país a enviar mais *spams* no mundo.
e) Pichadores virtuais: tem por objetivo deixar sua marca em sites, sendo a maioria do poder público como do FBI, Pentágono, Supremo Tribunal Federal, INSS, entre outros, declarando a invasão ou como forma de manifestação, não causando, normalmente, danos.
f) *Cyber* terrorista: como o nome propriamente diz, faz apologia ao terrorismo e ataques em massa, sendo na maioria das vezes por motivo de protesto.

Dito isto, há de se ressaltar que, antes da Lei n.º 12.737 de 2012, que será abordada posteriormente, havia uma divergência, jurisprudencial e doutrinariamente, sobre a tipificação da pena sobre a fraude eletrônica inerente ao *internet banking*, tema que embasa o presente trabalho, entre os crimes de furto qualificado mediante fraude e estelionato. Assim, far-se-á a leitura do seguinte capítulo para melhor elucidar o seguinte conflito.

3 A QUALIFICAÇÃO CRIMINAL DAS CONDUTAS PRATICADAS NA FRAUDE ELETRÔNICA ANTECEDENTE À LEI 12.737/2012

3.1 FURTO

3.1.1 Conceituação e objetividade jurídica

Segundo Mirabete e Fabbrini (2008, p. 203), o "furto é a subtração de coisa alheia móvel para si ou para outrem (art. 155, *caput*). É, pois, o assenhoreamento da coisa com o fim de apoderar-se dela de modo definitivo. A pena prevista para o furto é a de reclusão de um a quatro anos, e multa". Deste modo, o furto pode ser vislumbrado no art. 155, *caput*, do CP.

Capez (2007, p. 382), aduz que tal delito possui como objeto jurídico não apenas a propriedade, mas sim o patrimônio e a posse do bem furtado. Complementa Bitencourt (2009, p. 4) que o objeto do furto será somente coisa móvel.

3.1.2 Sujeitos ativo e passivo

O sujeito ativo do furto pode ser qualquer pessoa, com exceção do proprietário do bem furtado e de seu possuidor, pois a coisa perderia o *status* de "coisa alheia", bem como não seria coisa de outrem, respectivamente (BITENCOURT, 2009, p. 5).

Já o sujeito passivo é qualquer pessoa, física ou jurídica, que possui a posse ou propriedade do bem. Se este for subtraído de pessoa que apenas tem detenção desnecessária, como o caixa, balconista ou outro empregado de um estabelecimento, por exemplo, a vítima será somente o proprietário (MIRABETE; FABBRINI, 2008, p. 204).

3.1.3 Tipos objetivo e subjetivo

O centro do tipo objetivo é "subtrair", ou seja, tirar, retirar, surrupiar. Subtrair não é só retirar a coisa do local onde se encontrava, pois, é indispensável deixá-la sujeita ao poder de disposição do agente para si ou para outrem. Usar apenas a coisa não induz à punição criminal. Além do mais, coisa sem dono ou abandonada não pode ser objeto do furto. E, por último, com salientado anteriormente, a coisa móvel deve ser economicamente apreciável (BITENCOURT, 2009, p. 5-6).

Coisa é toda a substância material, corpórea, que seja passível de subtração e que tenha considerável valor econômico. Uma ideia, por exemplo, só pode ser furtada se for corporificada em um documento. Além disso, as coisas de uso comum, como o ar ou a luz, também não podem ser reconhecidas como coisa furtada, em princípio, a menos que possua a possibilidade de destacamento e aproveitamento individual (CAPEZ, 2007, p. 383).

Quanto ao móvel, Capez (2007, p. 384) leciona que:

> É tudo aquilo que pode ser transportado de um locar para outro, sem separação destrutiva do solo. Os animais e os semoventes está sujeitos à apropriação por terceiros, por exemplo, furto de gado (denominado abigeato). Os bens imóveis, por sua vez, não podem ser objeto do delito de furto.

O autor complementa informando que a lei civil considera imóveis como determinados bem, por exemplo, um navio, porém aqui, para fins penais, são considerados como bens passíveis de furto. Ademais, há bens que são apreciados por lei como móveis, tais como direitos reais sobre objetos móveis e ações correspondentes, entre outros, que não poderão ser suscetíveis ao furto, tendo em vista que se tratam de bens imateriais, incorpóreos, sendo assim insuscetíveis de apropriação. Entretanto, se tais direitos restarem como documentos, será possível instituir objeto de furto. (CAPEZ, 2007, p. 384).

Já quanto ao tipo subjetivo, ensina Mirabete e Fabbrini (2008, p. 206):

> O dolo é a vontade consciente de subtrair, acrescido do elemento subjetivo do injusto (dolo específico), que é a finalidade do agente expressa no tipo: "para si ou para outrem". É o denominado *animus furandi* ou *animus rem sibi habendi*. Independe, porém, do intuito de lucro por parte do agente (RT 716/445), que pode atuar por vingança, despeito, superstição, capricho etc. É atípico, por outro lado, o fato de fazer desaparecer a coisa (soltar um pássaro alheio da gaiola, tirar uma jóia [sic] para jogá-la ao mar etc.). Diz-se, também, que o consentimento da vítima na subtração elide o crime, já que o patrimônio é um bem disponível, mas, se ele ocorre após a consumação, é evidente a existência de ilícito penal.

Ademais, é necessário que o agente possua o conhecimento de que a coisa furtada é coisa alheia, pois se, sem saber, furtar coisa própria, não configurará o crime de furto, e também que possua a finalidade de apoderar-se da coisa (BITENCOURT, 2009, p. 13).

3.1.4 Consumação

Há três orientações distintas quanto ao momento da consumação do furto, que são: a) deslocamento da coisa, mesmo que a vítima ainda possa visualizar a execução do crime; b) afastamento da esfera de vigilância da vítima; c) posse tranquila (BITENCOURT, 2009, p. 14).

Capez (2007, p. 387-388) informa que há divergência quanto às duas últimas orientações. Alguns autores, como Damásio E. de Jesus, entendem que não é exigida a posse mansa e pacífica da coisa para que o crime se consume. Outros, entretanto, são adeptos à corrente, necessitando assim, para o aperfeiçoamento da conduta, a retirada do bem da esfera de visão da vítima, bem como a posse tranqüila da coisa, mesmo que por curto período.

Então, adotando as três orientações, o furto consuma-se quando há a retirada da coisa da disponibilidade do sujeito passivo, assegurando-se a posse pacífica da *res* (do latim, coisa), mesmo que de forma passageira. Ocorre, então, a inversão da posse da coisa, passando da vítima para o agente (BITENCOURT, 2009, p. 14).

As hipóteses de consumação do furto são: a) perda do bem subtraído (não há mais a possibilidade da vítima exercer o seu direito sobre a coisa); b) prisão em flagrante de um dos agentes e fuga dos demais com a *res* (houve a consumação do delito, neste caso, para todos os co-participantes); c) subtração de parte dos bens (se o agente furtar os bens em sua totalidade, mas apenas apoderar-se, posteriormente, de parte destes e guardá-los em esconderijo próximo ao local do crime, será preso em flagrante ao tentar apossar-se do restante dos bens, consumando, desta forma, o delito); d) prisão em flagrante (não há incompatibilidade com a consumação do crime, ou seja, o agente é localizado depois de apoderar-se dos bens com instrumentos utilizados, caracterizando-o, assim, como autor da infração) (CAPEZ, 2007, p. 388).

3.1.5 Tentativa

Quando a pratica do crime foi interrompida por causas estranhas ao agente, configurar-se-á a tentativa. Ou seja, se antes de o infrator deslocar a coisa para fora do alcance visual da vítima, bem como de sua disponibilidade, para a posse tranquila, for interrompido, logicamente não haverá a consumação do delito (BITENCOURT, 2009, p. 15).

Somente haverá tentativa quando houver o início da execução do crime, ou seja, com o primeiro ato idôneo e inequívoco a fim de consumar o ato. Caso contrário, o crime ainda se encontrará na fase de preparação. Ademais, é necessário ter certeza de que o agente possui a intenção de consumar o furto, como quando este é surpreendido pelos donos de uma residência apoderando-se de seus bens. No caso de crime impossível também se caracteriza a tentativa, pois há a ineficácia absoluta do meio empregado ou impropriedade absoluta do objeto material, por exemplo, em uma loja fiscalização e sistema antifurto, o criminoso é abordado pelos seguranças do estabelecimento cometendo o crime. Ainda há, no ordenamento

jurídico, a hipótese de desistência voluntária, ou seja, quando por vontade própria interrompe a execução do delito (CAPEZ, 2007, p. 389-390).

3.1.6 Furto noturno

Segundo consta no art. 155, § 1º do CP, haverá aumento de um terço da pena se o furto for praticado durante o repouso noturno (BRASIL, CP, 2011).

A razão da majorante é que, durante o repouso noturno, torna-se precária a vigilância da vítima com relação ao bem objeto do furto. Este repouso não se confunde com a noite, pois, consiste no momento em que há a ausência da luz solar, tornando-se, deste modo, variável, pois depende da observância nos costumes locais relativos ao horário de recolhimento da população e de seu despertar (MIRABETE; FABBRINI, 2008, p. 209-210).

Ademais, Mirabete e Fabbrini (2008, p. 210) destacam que não há a necessidade da casa estar habitada e que haja moradores repousando para caracterizar tal conduta. Entretanto, que tal opinião é divergente, tendo em vista que há ponderável corrente que estipula a necessidade destes requisitos para a caracterização. Bitencourt (2009, p. 18), por exemplo, adota a corrente ponderada, tendo em vista a finalidade protetiva da norma e a necessidade de sua interpretação restritiva.

Além disso, conforme corrente majoritária, também poderá ocorrer o furto noturno em estabelecimento comercial, tendo em vista que o objetivo da existência do aumento da pena é dar uma maior proteção aos bens durante o horário noturno, não se importando com um local somente. Aliás, no período noturno, o estabelecimento comercial possui uma diminuição na vigilância, maior desatenção das pessoas, e menor tráfego destas nas ruas, tornando assim os bens existentes em seu interior mais vulneráveis à prática do furto (MENEZES, 2013).

3.1.7 Furto privilegiado

O art. 155, § 2º do CP traz à tona um caso de furto privilegiado, esclarecendo que quando o autor do delito é primário (ou seja, não é reincidente) e a coisa furtada possui pequeno valor, a pena de reclusão poderá ser, pelo juiz, substituída pela detenção, diminuída de um a dois terços ou aplicada apenas a pena de multa (BRASIL, CP, 2011).

Jurisprudencialmente, é considerado mínimo o furto de coisa que não alcança o valor de um salário mínimo vigente à época do fato. Ademais, existe distinção entre pequeno

valor e pequeno prejuízo relativo ao bem. A jurisprudência aduz duas posições, sendo a primeira apoiada pelo STF e STJ, reconhecendo assim somente a existência do furto privilegiado quando a *res* for de pequeno valor, conforme estabelece a doutrina. Já a outra corrente jurisprudencial equipara o pequeno valor e o pequeno prejuízo (MIRABETE; FABBRINI, 2008, p. 211).

Embora o artigo dê o entendimento de que o consentimento do privilégio é facultativo ao juiz, o entendimento majoritário é de que é um direito subjetivo do réu. Sendo assim, uma vez presentes as condições supracitadas, o juiz estará obrigado a conceder o benefício (CAPEZ, 2007, p. 400).

3.1.8 Furto qualificado

O furto pode apresentar particularidades que ocasionam maior comoção social, com uma violação mais gravosa ao patrimônio alheio, necessitando assim de uma maior punição, tanto no caso de desvalor da ação ou de desvalor do resultado. Ademais, elas podem possui diferentes níveis de intensidade, sendo qualificadas, de acordo com a gravidade, como qualificadoras, majorantes ou agravantes (BITENCOURT, 2009, p. 22).

Os parágrafos 4º e 5º do art. 155 do CP indicam as hipóteses de furto qualificado previstos em nosso ordenamento jurídico, às quais será aplicada uma sansão mais rigorosa.

3.1.8.1 Com destruição ou rompimento de obstáculo à subtração da coisa

Conforme explica Capez (2007, p. 203), “trata-se de violência empregada contra obstáculo que dificulte a subtração da coisa. Destruir significa desfazer. Romper significa abrir. O emprego de violência contra a pessoa configura o creme de roubo”.

O obstáculo é tudo aquilo que empregado a fim de proteger a coisa contra um eventual delito. Aquilo que faz parte da coisa, que a integra, não pode ser considerado um obstáculo, como, por exemplo, o vidro de um carro quando o objetivo é o furto do automóvel. A violência deve ser proferida ao obstáculo exterior à coisa objeto do crime. Contudo, entende-se que há dois tipos de obstáculo: externo (quando a violência é direcionada a um obstáculo que impede que o agente tenha acesso à parte interna de um ambiente fechado) ou interna (quando a violência é direcionada a um obstáculo que se encontra no interior do local onde ocorrerá a subtração). Por fim, ressalta-se, novamente, que o obstáculo tem a finalidade

de proteção da coisa que será furtada, devendo o agente destruí-lo ou rompê-lo para caracterizar a qualificadora (BITENCOURT, 2009, p. 23-24).

Ademais, a simples retirada do obstáculo, sem acarretar destruição ou rompimento, para facilitar a subtração não caracteriza a qualificadora. Outro fator a ser considerado é que só será dada como qualificadora se o rompimento for anterior à consumação do furto (MIRABETE; FABBRINI, 2008, p. 213).

3.1.8.2 Abuso de confiança, ou mediante fraude, escalada ou destreza

Para Mirabete e Fabbrini (2008, p. 213), o abuso de confiança ocorre quando o agente aproveita-se da menor proteção dada pela vítima para subtrair a coisa. Complementa Capez (2007, p. 405), que a confiança é fruto das relações estabelecidas pelas partes (ativa e passiva), seja por relação empregatícia, seja por relação de amizade ou parentesco. É requisito necessário, para caracterizar esse tipo de qualificadora, que seja utilizada a confiança para consumar o furto.

Bitencourt (2009, p. 25) caracteriza confiança como "um sentimento interior de credibilidade, representando um vínculo subjetivo de respeito e consideração entre o agente e a vítima, pressupondo *especial relação pessoal* entre ambos" (grifo do autor).

Ademais, o autor alerta que apropriação indébita diverge de abuso de confiança, eis que no primeiro o agente aproveita-se de um momento em que a posse da coisa está desvigiada, conseqüência da confiança dada pela vítima, e já no segundo o agente exerce um contato com a coisa, e não com a sua posse (BITENCOURT, 2009, p. 26).

A fraude é o meio enganoso pelo qual a parte ativa utiliza-se para subtrair a *res*. Temos, como um dos vários exemplos, a pessoa que se disfarça de empregado de alguma empresa para entrar na residência da vítima e subtrair alguma coisa (CAPEZ, 2007, p. 405).

Diferencia-se, no entanto, furto mediante fraude de estelionato. Naquele, o enredo da fraude possibilita a subtração da *res*, sem a vontade e consentimento da vítima. Neste, a vítima é induzida em erro, que leva à consumação do delito, com a concordância da vítima, entregando a coisa livremente (MIRABETE; FABBRINI, 2008, p. 214).

Escalada, segundo Mirabete e Fabbrini (2008, p. 214), "é a utilização de via anormal para penetrar na casa ou local em que vai operar-se a subtração [...]". Ainda, Bitencourt (2009, p. 28) aduz que o acesso ao local pretendido para a execução do delito deve ser difícil, necessitando da utilização de esforço incomum, habilidade ou destreza para cumprir seu objetivo.

Conforme Capez (2007, p. 406), também podem ser utilizados instrumentos, como corda ou escada, para adentrar o local. O autor ainda dá um exemplo interessante: e se for um anão o agente do crime? Considerar-se-á o obstáculo sob o prisma objetivo, comparando-o com um homem comum, tendo em vista que a natureza da qualificadora é objetiva.

Sobre a destreza, ensina Bitencourt (2009, p. 29):

> Significa *especial habilidade* capaz de impedir que a vítima perceba a subtração realizada em sua presença. [...] A destreza pressupõe uma atividade dissimulada, que exige habilidade incomum, aumentando o risco de dano ao patrimônio e dificultando sua proteção (grifo do autor).

O exemplo mais comum desta modalidade é a denominada punga, ou seja, quando o agente subtrai objetos que estão junto à vítima, como uma carteira retirada do bolso da vítima sem que esta perceba (CAPEZ, 2007, p. 406).

Se a vítima notar o agente executando o furto, não configurará a qualificado, pois será considerado, neste caso, como tentativa de furto simples. Entretanto, se a prática for observada por terceiro, será então caracterizada então como tentativa de furto qualificado (MIRABETE; FABBRINI, 2008, p. 215).

3.1.8.3 Emprego de chave falsa

Caracteriza-se como chave falsa todo instrumento utilizado pelo agente para fazer funcionar o mecanismo de fechadura ou similar (MIRABETE; FABBRINI, 2008, p. 215).

A fim de complementar tal lição, Bitencourt (2009, p. 30) apresenta uma diferenciação no tratamento de chave falsa e verdadeira:

> *Chave falsa* é qualquer instrumento de que sirva o agente para abrir fechaduras, tendo ou não formato de chave. Exemplos: grampo, alfinete, prego, fenda, gazua etc. A *chave verdadeira*, à evidência, não qualifica o crime, pois lhe falta a elementar normativa "falsa". O emprego de chave falsa traduz maior perigosidade do agente, que, dessa forma, demonstra a instabilidade da normal proteção patrimonial, que uma fechadura, por si só, não pode elidir o risco de sua violação (grifo do autor).

3.1.8.4 Mediante concurso de duas ou mais pessoas

Segundo Capez (2007, p. 407-408), existem duas correntes acerca da necessidade da execução do delito por todos os agentes: 1ª) corrente adotada por Nélson Hungria, Celso Delmanto, e com posicionamento do STJ, aduz que se faz necessária a presença e cooperação dos concorrentes no local do crime, deixando a vítima com maior dificuldade para se

defender; 2º) está corrente diz que mesmo os agentes não executando o furto, ou não estando no local do delito, a prática será caracterizada como qualificada.

Não importa se um dos agentes é inimputável (menor, doente mental etc.), ou se não foi possível identificar um, pois, mesmo assim, será caracterizada como furto qualificado (MIRABETE; FABBRINI, 2008, p. 215).

Há que se ressaltar a relação entre quadrilha e esta qualificadora. Quando houver a associação de pelo menos quatro pessoas que tem, como finalidade, a prática de qualquer crime, caracterizar-se-á a quadrilha. Deste modo, os agentes, ao praticar um furto, já eram anteriormente caracterizados como quadrilha, respondendo assim pelo crime de quadrilha cumulado com furto. Mas este furto possui a qualificadora "mediante concurso de duas ou mais pessoas"? O STF entende que sim, que não ocorre, deste modo, o *bis in idem* (dupla sanção pela prática de um fato). Entretanto, há quem entenda não ser cabível a aplicação do *bis in idem,* pois, o concurso de pessoas já foi julgado no crime de quadrilha (CAPEZ, 2007, 409-410).

Ressalta-se, por fim, que não se faz necessário, no presente trabalho, adentrar no furto de coisa simples, tendo em vista que este trata da subtração de coisa comum gerada pelo condomínio, herança ou sociedade (CAPEZ, 2007, p. 413).

3.1.9 Enquadramento do furto na fraude eletrônica inerente ao *Internet Banking*

Quando o ordenamento penal brasileiro não possuía previsão específica sobre os crimes cometidos no ambiente informático, alguns entendiam (jurisprudencial e doutrinariamente) que as condutas fraudulentas exercidas no *Internet Banking* caracterizavam o furto qualificado.

Damasceno (2007) é um dos autores que apoiam esta corrente, aduzindo que a tipificação da conduta no art. 155, § 4º, inciso II, do Código Penal (furto mediante fraude) é cabível, pois, não há o consentimento da vítima quando o cliente cede dinheiro de sua conta bancária, mesmo havendo vício.

Simon (2013) justifica sua defesa nesta corrente da seguinte forma:

> Compreender as instituições financeiras como sujeito passivo de estelionato se mostra algo equivocado. Não se pode falar que a instituição foi induzida em erro ao aceitar a transação. O programa responde a uma chave. Inserida a chave (senha), ele reage com o acesso. Não se vislumbra artifício, ardil ou meio fraudulento que conduzam ao erro nesse procedimento. Se fosse assim, cada vez que alguém utiliza o *Internet Banking*, estaria se valendo de um meio fraudulento, que seria a senha, para tanto. A presunção de que o titular da conta é quem detém os dados relativos à senha não é absoluta.

Ademais, o autor complementa informando que a vítima não é induzida a fornecer seus dados pessoais ao sujeito ativo. A subtração destes é feita de forma imperceptível ao sujeito passivo, descaracterizando assim o estelionato (SIMON, 2013).

O STJ também utiliza esta corrente, como pode ser vislumbrado em julgamento:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. **FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO.** CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.
> [...]
> 2. **Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato** [...] (BRASIL, STJ, 2007, grifo nosso).

Por fim, Damasceno (2007) informa que se caracterizando as transações bancárias indevidas praticadas na *internet* como furto qualificado, o local de consumação será "[...] onde está situada a conta bancária da vítima e devem ser investigadas pela polícia judiciária e julgadas pelo Poder Judiciário deste local".

3.2 ESTELIONATO

3.2.1 Conceituação e objetividade jurídica

O estelionato está disposto no art. 171 do CP e significa "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", possuindo como pena um a cinco anos de reclusão, e multa (BRASIL, CP, 2011).

Quanto à objetividade jurídica, visa-se a proteção da inviolabilidade do patrimônio, bem como, subjetivamente, a boa-fé, segurança, veracidade e fidelidade nas relações de caráter patrimonial (MIRABETE; FABBRINI, 2008, p. 289).

3.2.2 Sujeitos ativo e passivo

Nada impede a autoria do crime, podendo ser agente qualquer pessoa, bem como a co-autoria ou participação no delito. Deste modo, mesmo que uma pessoa induza ou mantenha

a vítima à erro enquanto outra pessoa toma a posse da coisa, caracterizar-se-á o crime de estelionato, tornando-os co-autores (CAPEZ, 2007, p. 524).

Bitencourt (2009, p. 228) explica que não há necessidade de que o "outrem" citado no artigo supracitado seja co-autor ou partícipe do crime. Se este simplesmente ignorar a origem criminosa da vantagem atribuída, não será passível de punição. Entretanto, Capez (2007, p. 524) complementa informando que caso o beneficiário (ou seja, o "outrem") tenha induzido ou instigado o agente ao cometimento do crime, será considerado partícipe do delito, respondendo por este.

A vítima do delito pode ser conceituada da seguinte forma:

> Sujeito passivo do estelionato é a pessoa que sofre a lesão patrimonial; normalmente, é a mesma que é enganada. Pode-se, porém, enganar alguém vindo o prejuízo atingir terceiro; não é necessário que a vítima do dano patrimonial seja a mesma do erro, tanto que a lei se refere genericamente a prejuízo *alheio* [...] (MIRABETE; FABBRINI, 2008, p. 289).

Porém, para que a vítima do crime seja enganada, é requisito indispensável a capacidade de discernimento, pois um incapaz não tem capacidade suficiente para entender e querer algo. A ausência deste requisito caracteriza o crime vislumbrado no art. 173 do CP (abuso de incapazes). Ademais, se a vítima não tiver capacidade natural para ser iludida, como, por exemplo, se ela se encontrar em estado de coma, o delito caracterizará o crime de furto (BITENCOURT, 2009, p. 229).

3.2.3 Tipos objetivo e subjetivo

"Artifício" refere-se à simulação ou dissimulação idônea apropriada para a situação a fim de iludir alguém ao erro, aparentando uma falsa realidade dos fatos. "Ardil" é a astúcia, a conversa enganosa. Extrai-se de "qualquer outro meio fraudulento" toda possibilidade de fraude que resulte no equívoco da vítima (BITENCOURT, 2009, p. 232).

Mirabete e Fabbrini (2008, p. 291) lecionam que "induzir" quer dizer que a vítima chega a uma falsa aparência da realidade por meio da iniciativa do agente ao causar o erro. "Manter" alguém em erro significa que o erro já existe, o agente apenas o prolonga. Bitencourt (2009, p. 233) complementa informando que "*erro* é a falsa representação ou avaliação equivocada da realidade. A vítima supõe, por erro, tratar-se de uma realidade, quando na verdade está adiante de outra; faz, em razão do erro, um juízo equivocado da relação proposta pelo agente".

Quanto ao objeto do crime, pode extrair-se que:

> Objeto do crime é a vantagem ilícita, ou seja, qualquer utilidade obtida em favor do sujeito ativo ou de terceiro: propriedade, gozo, execução de um ato, crédito etc. [...] Embora já se tenha afirmado não ser necessário o caráter econômico da vantagem, em se tratando de crime patrimonial é ele necessário. Não havendo vantagem econômica a ser obtida pela fraude, não se configura o crime de estelionato. [...] Deve a vantagem ser ilícita, uma vez que, se devida, poderá ocorrer apenas o delito de exercício arbitrado das próprias razões (art. 345). Indispensável, ainda, para a concretização do tipo, o prejuízo efetivo da vítima, ou seja, um dano, uma perda de utilidade econômica (MIRABETE; FABBRINI, 2008, p. 291).

O dolo é o elemento subjetivo do estelionato, significando a vontade que o agente tem, espontaneamente, de ludibriar alguém, mediante meio fraudulento, a fim de obter vantagem ilícita patrimonial, restando no prejuízo de outrem. Quando referir-se ao "induzir ao erro", o dolo deve vir antes da aplicação do meio fraudulento, e da vantagem ilícita e prejuízo de outrem como resultados. Entretanto, quando referir-se ao "manter em erro", o dolo acompanhará o erro, ou seja, constatando este, o dolo se manterá nele (BITENCOURT, 2009, p. 238).

3.2.4 Consumação

O estelionato consuma-se, nas palavras de Capez (2009, p. 525), "com a obtenção da vantagem ilícita indevida, em prejuízo alheio, ou seja, quando o agente aufere o proveito econômico, causando dano à vítima". Bitencourt (2009, p. 239) ressalta que é requisito necessário para a consumação, além da vantagem ilícita, o prejuízo patrimonial de outrem.

Mirabete e Fabbrini (2008, p. 293) confirmam e informam, ainda, que no caso de cheque falsificado, deve-se seguir a Súmula 28 do STJ, que diz que o juízo competente para julgar o estelionato, neste caso, será o do local da vantagem ilícita.

3.2.5 Tentativa

Segundo Capez (2007, p. 526), haverá a tentativa se o agente não conseguir lograr êxito na vantagem ilícita. Bitencourt (2009, p. 239) acrescenta que "quando o agente não consegue enganar a vítima, o simples emprego de artifício ou ardil caracteriza apenas a prática de *atos preparatórios*, não se podendo cogitar tentativa de estelionato".

Ademais, se o meio aplicado no estelionato for ineficaz, não caracterizará a tentativa, como no caso de adulteração grosseira de documento, que, deste modo, fica facilmente identificável (CAPEZ, 2007, p. 526).

3.2.6 Estelionato privilegiado

Quando o criminoso for primário e o prejuízo for de pequeno valor, vislumbrar-se-á a redução ou substituição da pena, como pode ser observado no art. 171, §1º, do CP (BRASIL, CP, 2011).

Se o delito for instantâneo (lesão patrimonial), o prejuízo deverá ser averiguado no momento da consumação, a fim de verificar se cabe ou não a aplicação da minorante, como corrobora o STF. Entretanto, tratando-se de composição, transação, devolução da coisa ou reparação do dano, os nossos Tribunais tem entendido que a minorante se dará quando a reparação ocorrer antes do julgamento (MIRABETE; FABBRINI, 2008, p. 295).

Complementa Bitencourt (2009, p. 240):

> As *minorantes* constituem *direitos públicos subjetivos do réu*, cuja admissão é obrigatória, estando presentes os dois requisitos legais (*primariedade* e *pequeno prejuízo*). Para reconhecimento da figura privilegiada, tem predominado o entendimento (mais liberal) de que o limite de um salário mínimo não é intransponível (grifo do autor).

Ademais, Mirabete e Fabbrini (2008, p. 295) esclarecem que a primariedade e o pequeno prejuízo são condições básicas, devendo observar, ainda, outros pontos, como a importância do fato e a periculosidade reduzida do agente.

3.2.7 Disposição de coisa alheia como própria

Conforme se extrai do art. 171, §2º, I, do CP, nas mesmas penas incorre quem vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria.

"Vender" diz respeito à transferência do domínio da coisa através de pagamento. Tendo isso em vista, a venda aplica-se aqui quando o agente vender para alguém coisa que não é sua, mas que diz ser de sua propriedade, induzindo assim o comprador ao erro. Doutrinariamente, com relação ao bem imóvel, basta a lavratura da escritura e o recebimento do valor para a configuração da venda. Quanto à alienação fiduciária, configurará o crime quando o comprador ignorar o fato. "Permutar" significa trocar, ou seja, as partes estabelecem, entre si, uma obrigação de trocar uma coisa por outra, entretanto, uma das pessoas troca coisa que não é sua. "Dar em pagamento" quer dizer que o devedor dá algo que não é seu em substituição da prestação que lhe é devida. "Dar em locação" é quando o sujeito passivo cede coisa alheia à outra parte, por tempo determinado ou não, objetivando retribuição, com exceção do caso de locação pelo locador (sublocação). "Dar em garantia"

refere-se ao penhor, garantia e hipoteca. Desta forma, o crime ocorre quando o devedor dá, em garantia, bem alheio como se fosse seu (CAPEZ, 2007, p. 531).

Ou seja, é requisito que a o agente possua bem alheio (que pode ser tanto móvel, quanto imóvel), se passando por proprietário (domínio da coisa), e que a vítima acredite que é bem próprio daquele, agindo assim o sujeito ativo com má-fé, e o passivo, com boa-fé (BITENCOURT, 2009, p. 241).

3.2.8 Alienação ou oneração fraudulenta de coisa própria

Enquadrar-se-á, segundo o art. 171, §2º, II, do CP, como agente deste aquele que, "vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias" (BRASIL, CP, 2011).

A diferença deste para o anterior (3.3.7) é o objeto material, pois, enquanto naquele recai sobre coisa alheia móvel ou imóvel, aqui recairá sobre coisa própria do agente. Desta forma, "coisa própria inalienável" é a *res* que não pode ser vendida por convenção ou disposição legal. A "coisa própria gravada em ônus" é, além dos direitos reais de garantia (hipoteca, anticrese e penhor), outros direitos reais, como o usufruto, a habitação, a servidão e o uso. "Coisa própria litigiosa" refere-se ao bem objeto da discussão judicial. Neste caso, o crime de estelionato não configurará caso o adquirente sabia que o bem era litigioso. "Imóvel que prometeu vender a terceiro, mediante pagamento em prestações" é quando o sujeito ativo exerce alguma das ações indicadas no artigo supracitado mediante pagamento em prestações, por meio de promessa à terceiro (CAPEZ, 2007, p. 533).

O sujeito passivo é aquele que recebe a coisa desconhecendo a existência do ônus, sendo lesado em seu direito e fraudado em sua expectativa, sofrendo, assim, prejuízo patrimonial (BITENCOURT, 2009, p. 242).

Ademais, quanto à penhora, Mirabete e Fabbrini (2008, p. 299) lecionam que:

> [...] Embora já se tenha decidido que constitui o fato crime de alienação fraudulenta de coisa própria [...], a penhora é instituto processual e não o ônus a que se refere o dispositivo, ou seja, o direito real sobre a coisa alheia. Por essa razão, tem-se entendido ora pela atipicidade do fato e responsabilidade meramente civil do agente como depositário infiel [...], ora pelo delito de fraude à execução [...], e ora pelo delito de estelionato na forma básica.

3.2.9 Defraudação de penhor

A defraudação de penhor ocorre quando o agente, por alienação não permitida pelo credor ou outro modo, defrauda a garantia pignoratícia, quando possui a posse do bem empenhado, como se faz percebido no art. 171, §2º, III, do CP (BRASIL, CP, 2001).

Para Mirabete e Fabbrini (2008, p. 301), "a conduta do crime é alienar, transferir a propriedade (vender, permutar, doar etc.) ou defraudar o objeto material *de outro modo* (destruir, desviar, ocultar, abandonar, inutilizar etc.)" (grifo do autor). Ademais, acrescenta que independe da fungibilidade da coisa.

Para a defraudação do penhor aprimorar-se, Bitencourt (2009, p. 243) salienta que se faz cabível o exame pericial, mas que esta não é obrigatória.

Segundo Capez (2007, p. 534), a defraudação pode ser parcial, ou seja, quem comete a defraudação do penhor é o devedor que vende parte do gado, por exemplo. Entretanto, havendo a anuência do credor, poderá ser feita a defraudação sem o cometimento de qualquer crime.

3.2.10 Fraude na entrega de coisa

Conforme dispõe o art. 171, §2º, IV, do CP, caracterizará a fraude na entrega de coisa quando o sujeito ativo "defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém" (BRASIL, CP, 2011).

"Substância" significa essência, enquanto a "qualidade" refere-se à espécie, e a "quantidade" é o número, peso ou dimensão da coisa. Ademais, para a ocorrência do crime, se faz necessário a fraude, de modo que beneficie o agente e prejudique a vítima, e não simplesmente a falta de algum dos itens citados (BITENCOURT, 2009, p. 244).

É necessário, ademais, que haja uma obrigação entre as partes sobre a entrega do bem, decorrendo esta de lei, contrato ou ordem judicial. Quando for a título gratuito, a entrega da coisa defraudada não caracterizará tal conduta, pois, não haverá dano patrimonial (CAPEZ, 2007, p. 535).

3.2.11 Fraude para recebimento de indenização ou valor de seguro

Comete o crime disposto no art. 171, §2º, V, do CP quem "destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as

conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro" (BRASIL, CP, 2011).

A mera autolesão e a danificação ou destruição de coisa própria não constituem ato ilícito, exceto quando prejudicar terceiro, caracterizando assim o delito em apreço. A finalidade deste crime é a obtenção indevida do prêmio do seguro, ou seja, quando o agente é segurado de uma seguradora, e comete algum dos atos citados a fim daquela obtenção indevida, prejudicando, desta forma, a fornecedora do seguro. Assim, observa-se a necessidade de contrato de seguro válido e vigente no momento da ação criminal (CAPEZ, 2007, p. 536).

Para melhor interpretar o referido crime, Bitencourt (2009, p. 244) aduz que:

> *Destruir* significa aniquilar, fazer desaparecer ou extinguir, total ou parcialmente; *ocultar* significa esconder ou encobrir coisa própria; *lesar* significa ofender fisicamente, causar dano, danificar o próprio corpo ou a saúde, ou *agravar* as consequências de lesão ou doença (grifo do autor).

Ou seja, a destruição refere-se ao dano causado ao bem. Ocultar significa fazer com o bem objeto do crime fique imperceptível, escondido, que a outra parte não consiga vê-lo. Deste modo, percebe-se que o objeto material é o bem patrimonial do seguro (MIRABETE; FABBRINI, 2008, p. 305).

Ademais, os autores ainda complementam informando que, caso o agente não for o beneficiário do seguro, ou seja, se o proveito for de terceiro, poderá ocorrer o crime de estelionato comum, não cabendo o delito aqui estudado (MIRABETE; FABBRINI, 2008, p. 305).

3.2.12 Fraude no pagamento por meio de cheque

O art. 171, §2º, VI, do CP leciona que quem "emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento" (BRASIL, CP, 2011).

O cheque, para Capez (2007, p. 538), "constitui uma ordem de pagamento à vista. Uma vez emitido o título em favor do beneficiário (tomador), a instituição bancária (sacado) tem o dever de realizar o pagamento do valor nele inscrito, caso o emitente disponha de suficiente provisão de fundos".

Para caracterizar a emissão do cheque, não basta preenchê-lo ou assiná-lo, mas deve-se colocá-lo em circulação, neste caso, sem suficiente provisão de fundos. Quanto à frustração, este se refere ao impedimento do pagamento do cheque, seja pelo bloqueio, seja pela retirada do salvo existente, ou pela contra-ordem. Para configurar o delito, se faz

necessário que a frustração seja indevida, isto é, deverão existir fundos no momento da emissão do título (BITENCOURT, 2009, p. 245).

O sujeito ativo do delito, logicamente, é o emitente do título. Quando o tomador do cheque (sujeito passivo) souber que o mesmo não possui fundos, e passar para terceiro, caracterizará, apenas, a prática do estelionato comum, e não este em apreço. Entretanto, se o avalista do tomador participar, de má-fé, da elaboração da cambial, contribuindo, deste modo, para o livramento do cheque, estará praticando o presente delito, sendo caracterizado como co-autor. Ademais, também será co-autor aquele que, ciente da inexistência de fundos no título, convencer o tomador a receber em pagamento o cheque emitido por outra pessoa (MIRABETE; FABBRINI, 2008, p. 307).

É necessário, portanto, que reste comprovada a má-fé do agente desde o início da execução, ou seja, que este tenha o conhecimento de que há ausência ou insuficiência de fundos, com a finalidade de não realizar o real pagamento (CAPEZ, 2007, p. 539).

Enquanto que o título utilizado neste delito é aquele que se trata de uma ordem de pagamento à vista, existem, ainda, outros dois tipos de cheques: pós-datado e especial. O primeiro desnatura a ordem de pagamento à vista, representando uma promessa de pagamento. A eventual inexistência de fundos suficiente neste título, no momento de sua apresentação, não caracteriza o delito ora estudado. Já quanto ao segundo, mesmo se o limite for ultrapassado, os bancos têm honrado o pagamento de cheques de clientes especiais. A recusa é eventual, não sendo, deste modo, decisiva para configurar a conduta do emitente, tendo em vista que, à evidência, a má-fé não existe neste caso (BITENCOURT, 2009, p. 247).

Quanto à consumação, essa se dará, nos moldes da Súmula 521 do STF, no momento e local em que o banco sacado recusar o pagamento, tendo em vista o prejuízo sofrido neste momento. Havendo o arrependimento do agente, e efetuando, deste modo, o depósito do numerário necessário antes da apresentação do título no banco sacado, não configurará, logicamente, o delito em tese. Ademais, se o arrependimento for posterior à consumação do crime e anterior à denúncia, aplicar-se-á a Súmula 554 do STF, extinguindo assim a punibilidade do sujeito ativo (CAPEZ, 2007, p. 543).

3.2.13 Enquadramento do crime de estelionato na fraude eletrônica inerente ao *Internet Banking*

Enquanto alguns doutrinadores e algumas jurisprudências apoiavam o furto qualificado como o crime que caracterizava a conduta ilícita da fraude eletrônica na *internet*,

antes da previsão específica sobre os delitos informáticos, outros, entretanto, apoiavam a idéia de que, na verdade, tratava-se de estelionato.

Para Lôbo (2007), quando o agente obtém a senha do usuário do banco, ora vítima, para adentrar-se ao sistema bancário identificando-se como este, a instituição financeira é iludida, permitindo a transferência sob sua guarda. Ademais, o sujeito passivo, em seu entendimento, não despojaria de seus bens conscientemente, caracterizando, deste modo, o estelionato. Acrescenta, ainda, que o sujeito passivo não é somente o usuário, aquele que teve seus dados descobertos pelo agente, mas também a instituição financeira pela ilusão sofrida.

Segundo Costa (1995, p. 4), "o que caracteriza o estelionato na informática é o meio fraudulento, o artifício, o ardil que é usado pelo agente ativo para atingir o patrimônio de outrem".

Deste modo, para caracterizar o supracitado, extrai-se decisão do TRF da 3ª Região:

> PENAL. RECURSO EM SENTIDO ESTRITO. **ESTELIONATO. SAQUES INDEVIDOS DE CONTA CORRENTE VIA INTERNET BANKING. PREJUÍZO PATRIMONIAL À CAIXA ECONÔMICA FEDERAL**. ART. 171, § 3º, DO CP. COMPETÊNCIA DA JUSTIÇA FEDERAL. ART. 109, IV, DA CF. PROVIMENTO.
> 1. **Os fatos apurados consistem na retirada indevida de valores de correntista da Caixa Econômica Federal, por meio de movimentação financeira fraudulenta através do sistema de internet banking.**
> [...]
> 3. Cabe recordar que, **na hipótese de estelionato**, é pacífica a doutrina ao enunciar que **figuram no pólo passivo do delito tanto aquele que foi ludibriado quanto aquele que sofreu o prejuízo econômico, podendo ser pessoas distintas**.
> 4. **No caso sob análise, desde o desfecho da execução do crime, o artifício fraudulento ludibriou os mecanismos de vigilância e guarda de responsabilidade da CEF, provocando-lhe posterior lesão patrimonial, além de dano subjacente à credibilidade da instituição bancária.** [...] (BRASIL, TRF3, 2011, grifo nosso).

Ademais, Damasceno (2007, p. 1) diz que, "se entendermos que o tipo penal é o estelionato (art. 171, CP), a infração consumar-se-ia com a obtenção da vantagem indevida pelo agente [...]". E acrescenta "o local do crime seria o local onde os criminosos receberam a vantagem indevida, que poderia se dividir em local imediato e local mediato".

Assim, entendendo melhor o entendimento doutrinário e jurisprudencial anterior à Lei 12.737/2012, a aplicação da fraude inerente ao *Internet Banking*, o furto qualificado mediante fraude e o estelionato, se faz necessário o conhecimento atual jurídico com relação ao assunto, seguindo, deste modo, ao próximo capítulo.

4 A RELAÇÃO DOS MECANISMOS UTILIZADOS NA FRAUDE ELETRÔNICA INERENTES AO *INTERNET BANKING* AOS DIAS ATUAIS

Cláudio Antônio de Paiva Simon (2013) leciona que as técnicas utilizadas para fraudar no ambiente do *Internet Banking* são o *scam*, o *phishing* e o *pharming*.

4.1 *SCAM*

O *scam*, proveniente da Nigéria, recebe a denominação "419", advinda do Código Penal Nigeriano que restringe sua prática. Seu exercício se resume ao ato de extorquir soma de dinheiro do usuário, enganando este ao dizer que lhe será concedido certa percentagem do dinheiro pelo golpista (FRAUDES..., 2013).

Adaptando ao sistema brasileiro, Simon (2013) conceitua esta prática fraudulenta como sendo "[...] a mensagem enviada em massa, à moda do *spam*, com um diferencial: ela contém arquivo anexado ou *link* de condução a *download* de arquivo. Esse arquivo, por seu turno, proporciona a instalação de um *trojan horse* na máquina do usuário".

Então, deste modo, o *spam* significa o envio "em massa", ou seja, para um grande número de pessoas, de *e-mails* não solicitados (SPAM, 2013).

Utiliza-se o *spam* para proporcionar uma forma de publicidade ao *spammer* (pessoa que prática do spam) de forma prática e barata e que atinja numa escala universal. Deste modo, esta prática tem crescido muito nos últimos tempos, causando demasiada preocupação nos usuários da rede de comunicação (*internet*) por causa da natureza e objetivo das mensagens (SPAM, 2013).

Os prejuízos causados pelo *spam* ao usuário podem ser elencados como: perda de mensagens importantes (como há na caixa de entrada uma grande quantidade de *spam*, acabam passando despercebidos, muitas vezes, *e-mails* importantes, deixando o usuário de lê-las, ou então vislumbrá-las em atraso); recebimento de conteúdo impróprio ou ofensivo; gasto desnecessário de tempo; não recebimento de *e-mails* importantes; classificação feita de forma errônea das mensagens recebidas (no caso de utilização de sistema de filtragem de *e-mails*); impacto na banda da *internet* em decorrência do tráfego gerado; má utilização dos servidores; inclusão em listas de bloqueio, prejudicando, desta forma, o envio de *e-mails* importantes pelo usuário bloqueado; e por fim, o investimento extra em recursos para que o objetivo do *spam* não seja concretizado (SPAM, 2013).

Através dos sites Spamcop.net e Abusix.org, onde são feitas reclamações de *spams* que ocorrem no mundo pelos usuários, o Centro de Estudos, Resposta e Tratamento de

Incidentes de Segurança no Brasil (CERT.br) fez uma análise das reclamações feitas no Brasil, criando um gráfico de estatísticas de notificações da prática que foram reportadas desde o ano de 2003 até dezembro de 2012:

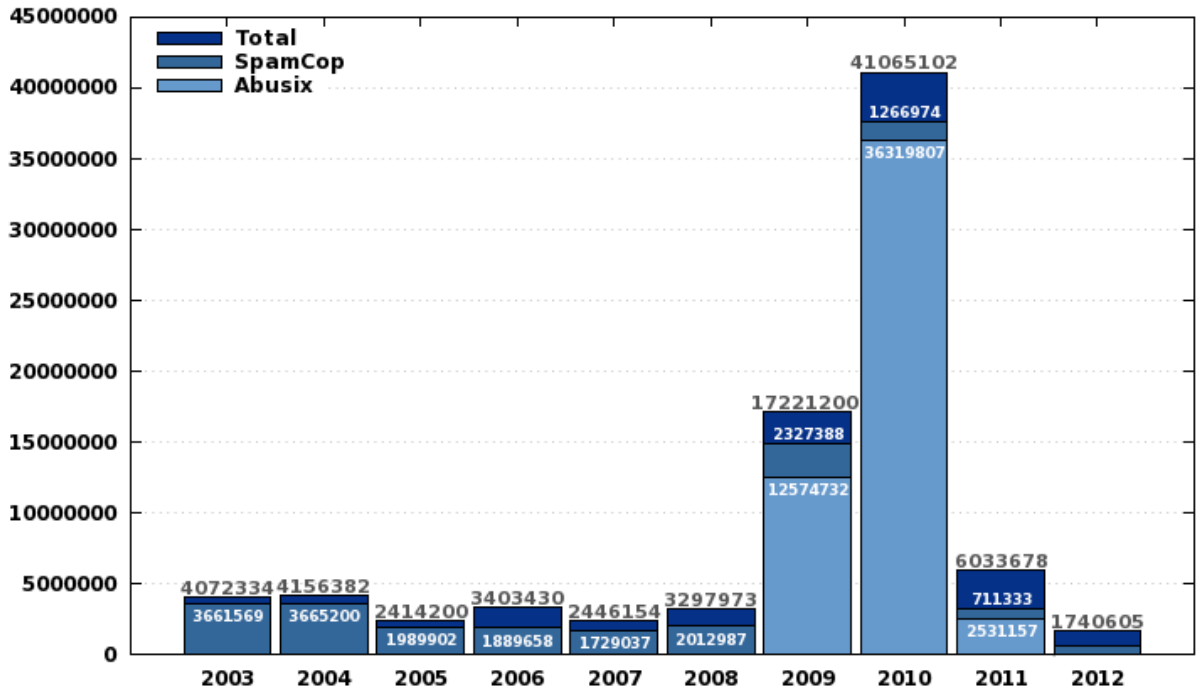

Gráfico 3 – Spams Reportados ao CERT.br por Ano (Fonte: CERT.br, 2013).

Como é possível vislumbrar no gráfico acima exposto, apesar da prática ainda ser contínua no Brasil, a divulgação dos métodos de segurança a serem adotados pelos usuários de forma generalizada tem resultado na atual diminuição da incidência demasiada do *spam*, diversamente do que era visto no ano de 2010, onde houve o maior número de registros, ano este em que a preocupação passou a tomar graus mais elevados, como era possível visualizar nos meios de comunicação da época.

Conforme mencionado no início deste título, o *scam* possui um arquivo anexado ou *link* de condução a *download* de *trojan horse* (cavalo de tróia).

O cavalo de tróia possui esse nome em decorrência do conflito mais importante da mitologia grega, quando o guerreiro grego Odisseu ordenou aos seus subordinados que construíssem um cavalo de madeira grande o suficiente para comportar seus soldados no interior do objeto, com a finalidade de adentrar na cidade de Tróia. Aproveitando o fato de o cavalo ser considerado um animal sagrado para os troianos, Odisseu formulou uma situação não qual o seu objetivo foi cumprido, iludindo, desta forma, os troianos, que não sabiam que

existiam gregos dentro do animal. Desta forma, enquanto os gregos dormiam em seus aposentos, os troianos aproveitaram a situação e devastaram a cidade (FULLER, 2008).

No ambiente informático, conceitua-se o cavalo de tróia como:

> Na informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário (UOL, 2013).

Algumas destas funções maliciosas são: a instalação de *keyloggers* ou *screenloggers* no computador do usuário; o furto de dados; e a alteração ou destruição de arquivos (UOL, 2013).

Para melhor informar, segundo Machado (2012) os "*keyloggers* são aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado". Desta forma, a pessoa que está acessando o computador do usuário ilicitamente poderá visualizar qualquer ato realizado, como quando o proprietário da máquina digita sua senha em algum *site* bancário. Já o *screenlogger* é "capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado" (CÓDIGOS..., 2013).

Existem vários exemplos visíveis na *internet*. Visando disponibilizar à população maiores informações, foi criada no *site* do RNP uma seção onde podem ser encontradas diversas imagens de fraudes efetuadas na *internet*, enviadas por usuários e recebidas pelo CAIS, sendo, em grande maioria, relacionadas com o *Internet Banking*:

Imagem 2 – Boleto de Cobrança Referente ao Dia 20/04/2013 (Fonte: RNP, 2013).

4.2 *PHISHING*

De modo geral, o *phishing* é quando a identidade *online* do usuário (dados de cartões de crédito, senhas, dados de conta etc.) é subtraída, por meio de *e-mail* ou *site* fraudulento projetado para desenvolver a prática (MICROSOFT, 2013).

Também chamado de *phishing-scam* ou *phishing/scam*, em decorrência da grande associação feita entre esses mecanismos, as mensagens que este golpe utiliza para iludir o usuário, normalmente, se passam por enviadas de uma instituição conhecida, como se fosse uma comunicação oficial desta, tentam atrair de alguma forma a curiosidade da vítima, algumas vezes a assustando, como quando informam que se não for cumprido o requerido na mensagem, acarretará sérias consequências, e, por fim, tentam induzir o usuário a fornecer seus dados (GOLPES..., 2013).

Com relação a 2011, tal mecanismo aumentou 59% em 2012 no mundo, atingindo, desta forma, cerca de 1.5 bilhões de dólares, ou seja, 22% a mais do que no ano anterior. O Brasil encontra-se em 4º lugar na lista de países com maior frequência de *phishing*, perdendo apenas para os EUA, Reino Unido e Alemanha (EMC, 2013).

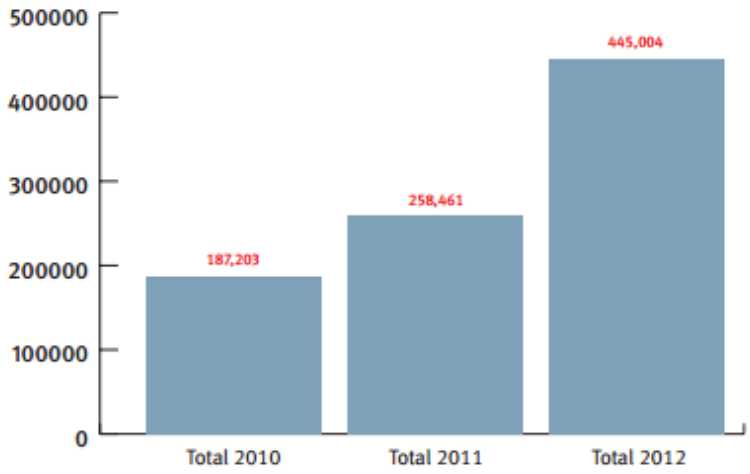

Gráfico 4 – Ataques de *Phishing* por Ano (Fonte: EMC, 2013).

Então, como visto, o *phishing* ataca por meio de mensagens encaminhadas ao usuário. É possível vislumbrá-lo quando o usuário recebe um *e-mail* de uma instituição financeira, onde existe um *link* que dará acesso ao suposto *site* bancário, quando, na verdade, trata-se de uma página falsa, onde os dados fornecidos serão encaminhados ao fraudador. O mesmo também é visto em casos de comércio eletrônico, redes sociais e companhias aéreas (GOLPES..., 2013).

No *site* da RNP, relatado no título "*Scam*" do presente trabalho, também é possível ver a prática do *phishing*, tendo em vista sua grande incidência no Brasil, como informado anteriormente. Como já explicado, primeiramente é encaminhada à vitima uma mensagem:

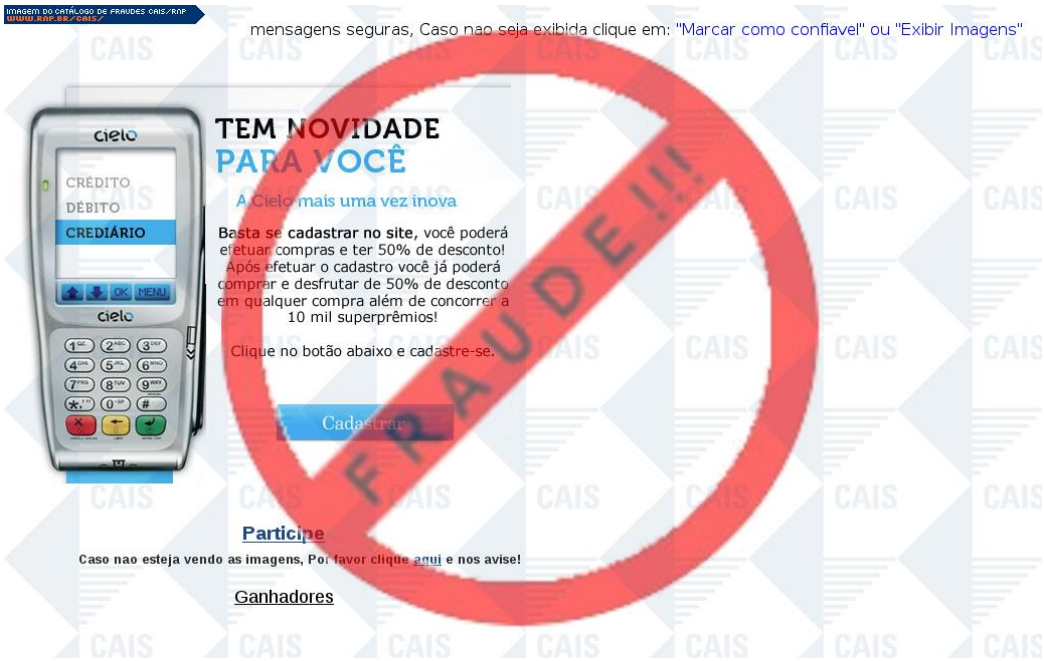

Imagem 3 – Mensagem de *Phishing* (Cielo Compra Premiada 50% de Desconto). (Fonte: RNP, 2013).

E, posteriormente, é o usuário é encaminhado para uma página falsa, onde disponibilizará seus dados que, na verdade, serão recebidos pelo fraudador:

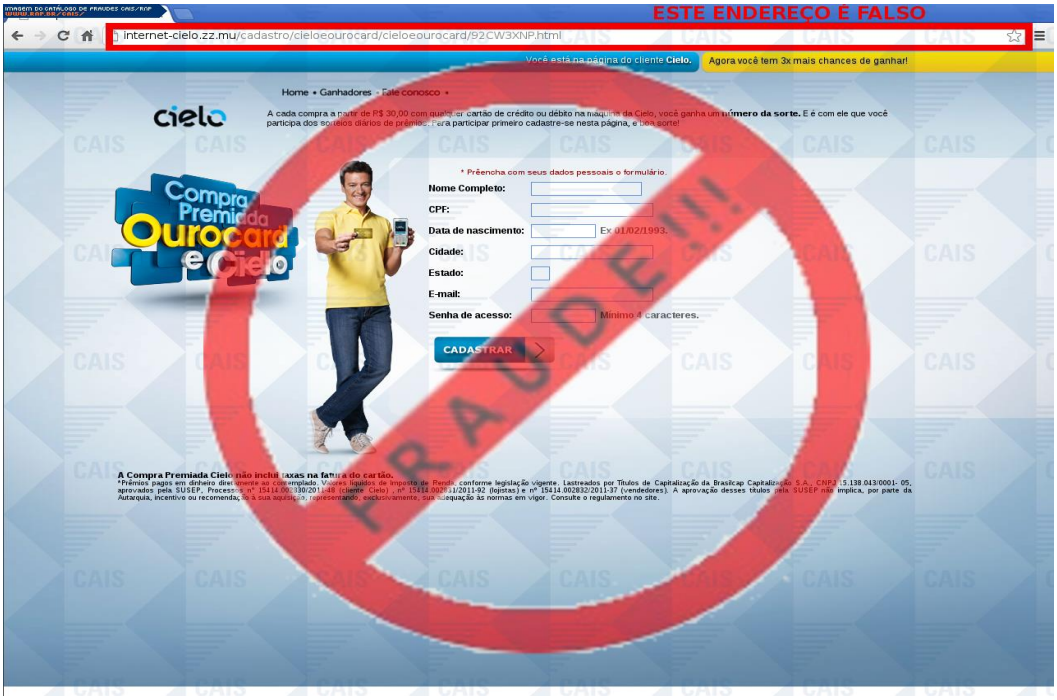

Imagem 4 – Página Falsa (Cielo Compra Premiada 50% de Desconto). (Fonte: RNP, 2013).

4.3 PHARMING

O *pharming* é uma variante do *phishing*, tendo em vista que também leva o usuário a uma página falsa. A diferença, neste caso, é que não há a necessidade da utilização de uma mensagem como "isca" para levar a vítima até o suposto *site* (NORTON, 2013).

Ademais, é mais imperceptível ao usuário vislumbrar que se trata, no caso, de uma página falsa, pois, tal redireção ao *site* se dá por meio de alterações no serviço DNS, como pelo comprometimento do servidor do serviço, ação de códigos maliciosos (*malwares*) com a finalidade desta alteração, ou ainda pela ação direta do fraudador nas configurações do serviço (GOLPES..., 2013).

Primeiramente, se faz necessário explicar o que é um serviço DNS. Segundo Maziero (2013) "[...] é o principal responsável pela resolução de nomes na Internet. Esse serviço é construído por um conjunto de servidores operando de forma descentralizada. Cada servidor DNS é responsável por um domínio ou sub-domínio de nomes na Internet. [...]".

Explicando melhor, todo *site* ou serviço disponibilizado na *internet* precisa ter um endereço IP para que seja localizado o servidor que lhe hospeda, a fim de que, deste modo, seja possível o acesso do mesmo. Seria impossível decorar todos os endereços IP dos *sites* que os usuários da *internet* acessam diariamente. Por isso, para que seja mais facilitado o acesso, existem os chamados "domínios", ou seja, o endereço do *site*, como por exemplo "www.facebook.com" ou "www.google.com" (ALECRIM, 2011).

Já um código malicioso (*malware*) é um programa criado com a finalidade de execução de ações danosas e atividades maliciosas em um computador, agindo:

> - pela exploração de vulnerabilidades existentes nos programas instalados;
> - pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
> - pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
> - pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
> - pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos) (CÓGIGOS, 2013).

Um exemplo de *malware*, para melhor representá-lo, e diferente do utilizado no *pharming*, é a alteração de boletos bancários gerados na *web*. Este *malware*, que se encontra no computador do usuário, detecta quando este último visualiza um boleto bancário no navegador (*browser*), e altera, em tempo real, os números da linha digitável a fim de desviar a quantia paga através do documento (NOVO..., 2013).

Outro exemplo de *malware* é o cavalo de tróia, como foi visto quando foi tratado do assunto *scam* no presente trabalho, por se tratar de um programa malicioso que é recebido pela vítima na forma de um presente.

Então, deste modo, o *pharming* é visto quando o usuário, ora vítima, é levado ao *site* falso por uma alteração no domínio da página, como no exemplo que será demonstrado a seguir, e quando há o acesso, vislumbra diversas semelhanças com o verdadeiro, pensando, assim, que realmente está entregando seus dados ao operador da página legítima quando, na verdade, está fazendo esta entrega ao criminoso.

Para melhor visualizar essa prática, imagine que um *site* possui o domínio "www.bancoverde.com". O criminoso, então, informa ao usuário o domínio "www.bancoverda.com". Vislumbre que, de um domínio para o outro, há apenas uma pequena alteração, retirando a letra "e" e acrescentando a letra "a". Desta forma, a vítima, sem perceber o erro, é direcionada ao *site* falso, pensando estar no verdadeiro e, informando lá seus dados pessoais e bancários, concretizando, desta forma, a prática do *pharming*.

4.4 LEI N.º 12.737/2012 – TIPIFICAÇÃO CRIMINAL DE DELITOS INFORMÁTICOS

Conhecida popularmente como "Lei Carolina Dieckmann", pela situação vivida pela atriz brasileira no ano de 2012, quando teve fotos íntimas suas divulgadas pela *internet* por ter seu computador invado, e tal conduta ainda não era prevista como infração penal, a Lei n.º 12.737/2012, que trata sobre a tipificação criminal de delitos informáticos, entrou em vigor em 02 de abril de 2013.

Referida lei promoveu algumas importantes alterações no CP, como o acréscimo dos arts. 154-A e 154-B, inserindo, deste modo, o novo tipo penal denominado como "invasão de dispositivo informático", a inclusão do § 1º ao art. 266, no qual a "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" foi considera uma conduta criminosa, e, por fim, a inclusão do parágrafo único ao art. 298 estabelecendo que a "falsificação de cartão" também configura o crime de "falsificação de documento particular" (CAVALCANTE, 2012).

4.4.1 Invasão de dispositivo informático

4.4.1.1 Bem jurídico

O bem jurídico, neste caso, trata-se da privacidade, tratando, deste modo, de suas espécies, quais sejam a vida privada e a intimidade da pessoa (CAVALCANTE, 2012).

Objetiva, deste modo, a liberdade individual e a privacidade dos dados e informações, pessoais ou profissionais, do usuário, que estão inseridas em dispositivo informático (PRADO, 2013, p. 407).

4.4.1.2 Sujeitos ativo e passivo

O criminoso pode ser qualquer pessoa, desde que, logicamente, não possua autorização para acessar os dados e informações inerentes ao dispositivo (CAVALCANTE, 2012).

Como vislumbrado no primeiro capítulo do presente trabalho, e salientado por Prado (p. 407, 2013), "segundo a terminologia utilizada na informática, aquele que invade tais dispositivos com finalidade ilegal, de obtenção de vantagem indevida ou de prejuízo alheio, é denominado *cracker*".

O *cracker* não tem a necessidade de invadir esses dispositivos para obter lucros. Muitas vezes, a obtenção dos dados e informação são um mero modo de ultrapassar um desafio, demonstrando sua capacidade, demonstrando que o dispositivo possui pontos fracos passíveis de invasão. Não se deve, deste modo, confundir o *cracker* com o famoso *hacker*. Este último, por sua vez, é um profundo conhecedor da programação, visa ampliar seus conhecimentos, dedicando-se à compreensão do funcionamento dos sistemas operacionais (PRADO, 2013, p. 407).

Conforme Prado (2013, p. 408) e Cavalcante (2012), o sujeito passivo é o titular do dispositivo informático, podendo ser tanto pessoa física, como pessoa jurídica. Entretanto, não se deve interpretar o "titular" como somente o proprietário do dispositivo, pois pode ser também o detentor do mesmo, como, por exemplo, quando uma empresa fornece ao seu funcionário o dispositivo para trabalho.

4.4.1.3 Tipos objetivo e subjetivo

Extrai-se do art. 154-A, *caput*, do CP que esta conduta criminal consiste na invasão de dispositivo informático alheio, estando, ou não, conectado à *internet*, por meio da violação indevida de mecanismo de segurança, com a finalidade de obter, adulterar ou destruir os dados ou informações ali contidos sem a autorização expressa ou tácita de seu titular, ou no caso de instalação de vulnerabilidades para obter vantagem ilícita.

Prado (2013, p. 408) informa que "invadir" refere-se ao "devassar, adentrar, vasculhar, tomando conhecimento parcial ou integral daquele conteúdo". Cavalcante (2012) complementa dizendo que o local invadido, no caso, é o sistema ou memória do dispositivo informático.

O "dispositivo informático alheio" significa o equipamento físico, denominado na informática como *hardware*, utilizado para executar programas, chamados de *softwares*, ou para se conectar a outros equipamentos com finalidade funcional. Este *hardware*, no presente caso, deve pertencer à terceiro (CAVALCANTE, 2012).

A "violação indevida de mecanismo de segurança" de que trata o artigo supracitado diz respeito ao modo pelo qual ocorre a invasão. O mecanismo aqui tratado pode ser tanto físico (como uma trava para teclado com chave) ou lógico (uso de nome de usuário e senhas, por exemplo). Ressalta-se, entretanto, que nem todo dispositivo informático possui mecanismo de segurança (antivírus, senha para acesso, anti-*malware* etc.). Neste caso, vincular-se-á ao presente delito, tendo em vista que também há vulnerabilidades, na verdade, ainda maiores, tendo em vista a falta de proteção, no dispositivo (PRADO, 2013, p. 408-409).

Complementando o tipo objetivo:

> *Com o fim de obter* (alcançar, adquirir), *adulterar* (alterar, modificar) *ou destruir* (inutilizar, extinguir) *dados ou informações*, tem-se o elemento subjetivo do injusto. *Dados* são letras, caracteres e símbolos organizados em uma determinada forma, permitindo seu armazenamento e processamento por um computador; *informações* são os resultados do processamento e que tem significado para as pessoas que o utilizam. Em situações correntes, informações e dados são utilizados como sinônimos (PRADO, 2013, p. 409, grifos do autor).

Por fim, "ou com o fim de instalar vulnerabilidades para obter vantagem ilícita", é, por exemplo, quando o criminoso entra em dispositivo informático alheio e instala um programa espião que lhe revela as senhas digitadas pelo sujeito passivo ao acessar algum *site* (CAVALCANTE, 2012).

O tipo subjetivo é o dolo, possuindo, na primeira parte do *caput* do referido artigo o elemento subjetivo especial qual seja a obtenção, adulteração ou destruição de dados ou

informações e, já na segunda parte, a instalação de vulnerabilidades para a obtenção de vantagem ilícita (PRADO, 2013, p. 410).

4.4.1.4 Consumação e tentativa

A consumação ocorre pela mera invasão ou instalação, não necessitando que haja a obtenção, adulteração ou destruição dos dados ou informações contidas no dispositivo informático, ou a obtenção de vantagem ilícita, tendo em vista que o crime é formal (CABETTE, 2013, p. 1).

Em regra, a comprovação da invasão se dá pela prova pericial. Contudo, também é possível a comprovação por outros meios, como, por exemplo, a prova testemunhal (CAVALCANTE, 2012).

A tentativa é possível, tendo em vista que a pessoa pode, no caso, tentar "[...] invadir um sistema ou instalar vulnerabilidades e não o consiga por motivos alheios à sua vontade, seja porque é fisicamente impedida, seja porque não consegue, embora tente violar os mecanismos de proteção" (CABETTE, 2013, p. 1).

4.4.1.5 A invasão de dispositivo informático (art. 154-A do CP) versus o furto mediante fraude (art. 155, § 4º, II do CP) na visão de Márcio André Lopes Cavalcante

Segundo Cavalcante (2012), quando há a subtração de valores da conta bancária da vítima através da instalação de um *malware*, a conduta permanece sendo tipificada como um furto mediante fraude, tendo em vista que este trata da subtração de coisa alheia, enquanto que a invasão de dispositivo informático trata apenas da invasão de um dispositivo informático, violando seu mecanismo de segurança, e instalando uma vulnerabilidade que acarreta em vantagem ilícita.

Cavalcante (2012) ainda menciona alguns exemplos interessantes, que tornam mais clara a situação:

> • O agente tenta invadir o computador da vítima com o objetivo de instalar o malware e obter a senha para realizar o furto, mas não consegue: responderá por tentativa de invasão (art. 154-A) e não por tentativa de furto qualificado (art. 155, § 4º, II);
> • O agente invade o computador da vítima com o objetivo de instalar o malware e obter a senha para realizar o furto, porém não inicia os atos executórios da subtração: responderá por invasão consumada (art. 154-A) e não por tentativa de furto qualificado (art. 155, § 4º, II);
> • O agente invade o computador da vítima com o objetivo de instalar o malware e obter a senha para realizar o furto, inicia o procedimento para subtração dos valores,

> mas não consegue por circunstâncias alheias à sua vontade: responderá por tentativa de furto qualificado (art. 155, § 4º, II);
> • O agente invade o computador da vítima com o objetivo de instalar o malware e obter a senha para realizar o furto, conseguindo efetuar a subtração dos valores: responderá por furto qualificado consumado (art. 155, § 4º, II).

Desta forma, segundo o ponto de vista do autor, vislumbra-se que quando houver a subtração de coisa alheia, como o dinheiro, a prática será caracterizada como furto mediante fraude, com base no art. 155, § 4º, II, do CP, enquanto que, quando houver, por exemplo, apenas a obtenção de dados, sem que haja a subtração de coisa alheia, a conduta será tipificada como invasão de dispositivo informático, observando o exposto no art. 154-A do CP, extraído da Lei n.º 12.737/2012.

4.4.1.6 A conduta equiparada e o aumento de pena por prejuízo econômico

Conforme consta no §1º do art. 154-A do CP, "na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput" (BRASIL, Lei n.º 12.737/2012, 2013).

Deste modo, possui como finalidade na conduta equiparada, a permissão da conduta definida no *caput* do artigo supracitado pela fabricação, oferta, repartição, comercialização ou divulgação do dispositivo ou programa de computador que será utilizado no referido delito (PRADO, 2013, p. 410-411).

Segundo o §2º do referido artigo do CP, "aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico" (BRASIL, Lei n.º 12.737/2012, 2013).

De forma clara, este parágrafo torna-se restrito ao prejuízo econômico, ou seja, o dano moral não se aplica ao caso. Ademais, aplicar-se-á somente na figura simples e na equiparada (art. 154-A, *caput* e §1º, CP), não compreendendo, desta forma, o §3º do dispositivo penal.

4.4.1.7 Forma qualificada

Vislumbra-se no art. 154-A, §3º, do CP que, se através da invasão do dispositivo informático, o criminoso adquirir conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas (definidas, desta forma, por lei), ou obter o controle remoto não autorizado daquele, a pena será aumentada para 6 (seis) meses a 2 (dois)

anos, na forma de reclusão, e aplicação de multa, se a conduta não constituir crime mais grave (BRASIL, Lei n.º 12.737/2012, 2013).

As "comunicações eletrônicas privadas" são as trocas de *e-mails*, SMS (serviço de mensagens curtas, disponível em telefones celulares), conversas realizadas em redes sociais, salas de bate-papo da *internet*, programas de trocas de mensagens (como Skype ou Windows Live Messenger, mais conhecido como MSN), troca de fotos, imagens ou vídeos privados feitos nestas comunicações (CABETTE, 2013, p. 2).

Com relação aos "segredos comerciais e industriais":

> É irrelevante que os segredos sobreditos possam ser abertos devido a previsões contratuais de validade temporal do sigilo ou mesmo outras condições específicas. Se essas condições temporais ou de outra natureza não estiverem satisfeitas, o invasor responde pelo crime qualificado (CABETTE, 2013, p.2).

O "controle remoto", informado no artigo supracitado, diz respeito, segundo Cabette (p. 2, 2013) à operação de acesso remoto que pode ser implantada por empresas, legalmente, como o programa Team Viewer, que permite que alguns dos funcionários da empresa tenham acesso, visual e operacionalmente, às máquinas dos demais, para verificar se estão trabalhando corretamente. Todavia, se este acesso for realizado de forma clandestina, ou seja, ilegalmente, configurar-se-á o crime aqui discutido.

Prado (2013, p. 411) complementa dizendo que este controle remoto pode apresentar diversas possibilidades de instalação, ou não, de vulnerabilidades no dispositivo informático, destacando a realização de tarefas para o atacante (criminoso) através da utilização do dispositivo, a obtenção de dados e o monitoramento do usuário (vítima) do dispositivo, e a destruição de arquivos, ou até mesmo do próprio dispositivo. Ademais, este controle não se dá apenas pela instalação dessas vulnerabilidades, como dito. Também pode ser feito pelas ferramentas legítimas do controle remoto, obtidas pelo atacante através de falhas no sistema de segurança na ferramenta ou no dispositivo informático.

Ademais, há duas formas de controle: a direta e a indireta.

> Na primeira, o atacante consegue invadir o dispositivo informático e instala uma vulnerabilidade. Esta última permite ao atacante controlar o dispositivo afetado. [...] Basicamente, o invasor pode detém o controle completo do equipamento, executando programas sem que o proprietário do dispositivo perceba. Na segunda, com controle indireto, a vulnerabilidade é instalada no dispositivo informático por algum método. [...] É utilizada com frequência quando se deseja dificultar a localização e identidade do atacante, além de possibilitar que milhares de equipamentos possam ser comandados simultaneamente (PRADO, 2013, p. 411-412).

4.4.1.8 Outros aumentos de pena

Resta vislumbrar, por fim, o § 4º e § 5º, e seus incisos (I a IV), do art. 145-A, do CP. O primeiro informa que se houver divulgação, comercialização ou a transmissão, a qualquer título, dos dados ou informações obtidos do dispositivo informático, a pena será aumentada de um a dois terços. Já no segundo, se o crime for praticado contra o Presidente da República, os governadores, os prefeitos, o Presidente do Supremo Tribunal Federal, o Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou, ainda, do dirigente máximo de administração direta e indireta federal, estadual, municipal ou do distrito Federal, a pena será aumentada de um terço à metade (BRASIL, Lei n.º 12.737/2012, 2013).

4.4.1.9 Pena e ação penal

A pena prevista para o crime simples (art. 154-A, *caput*, CP), bem como para a forma equiparada (art. 154-A, § 1º, CP), é de 3 (três) meses a 1 (um) ano de detenção, e multa (BRASIL, Lei n.º 12.737/2012, 2013).

Sobre o art. 154-B do CP, Prado (2013, p. 413) leciona:

> O artigo 154-B determina que a ação penal nos delitos definidos pelo artigo 154-A é pública condicionada, salvo se o crime é cometido contra administração pública direta ou indireta de qualquer um dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, hipótese em que a ação é pública incondicionada.

Ademais, o processo e julgamento desse delito é função dos Juizados Especiais Criminais, segundo é vislumbrado no art. 61, da Lei n.º 9.099/95. É admitida, desta forma, a suspensão condicional do feito, conforme art. 89 da mesma lei.

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

O art. 266 do CP diz respeito à interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefone, além do impedimento ou dificuldade no seu restabelecimento. Desta forma, a fim de complementar, foi introduzido pela Lei n.º 12.737/2012 do § 1º a este artigo, informando que sobre a mesma pena incorrerá quem interromper o serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar o restabelecimento. Desta

forma, o parágrafo único do art. 266 do CP passou a ser o § 2º, com o texto mantido (BRASIL, CP, 2011; Lei n.º 12.737/2012, 2013).

Segundo Cavalcante (2012), se o agente perturbar, sem interromper o serviço telemático ou de informação de utilidade pública, não será caracterizado como delito, pois houve falha do legislador ao não tipificar tal conduta na Lei n.º 12.737/2012.

4.4.3 Falsificação de cartão

O art. 298 do CP dispõe que "falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro" trata do crime de falsificação de documento particular. Dito isto, a Lei 12.737/2012, acrescentando o parágrafo único ao artigo citado, equiparou o documento particular ao cartão de crédito ou débito (BRASIL, CP, 2011; Lei n.º 12.737/2012, 2013).

Quanto à clonagem do cartão, Cavalcante (2012) faz algumas observações:

> Assim, se o agente faz a clonagem do cartão e, com ele, realiza saques na conta bancária do titular, pratica apenas furto mediante fraude, ficando, em princípio, absorvida a falsidade.
> De igual sorte, se o sujeito faz a clonagem do cartão e, com ele, realiza compras em estabelecimentos comerciais incorre em estelionato, sendo absorvida a falsidade, se não houver mais potencialidade lesiva (Súmula 17 do STJ).

4.5 A LEI N.º 12.735/2012 E SUAS ALTERAÇÕES

Sancionada na mesma data da "Lei Carolina Dieckmann", ou seja, em 30 de dezembro de 2012, a Lei n.º 12.735/2012, vulgarmente conhecida como "Lei Azeredo", em homenagem ao deputado Eduardo Azeredo, autor do projeto que lhe originou, causou alterações no Código Penal, Código Penal Militar, e Lei n.º 7.716/1989, que trata dos crimes resultantes de preconceito de raça e de cor.

Referida lei, observando seus artigos 1º e 4º, trouxe a tipificação das condutas realizadas através do uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares, além da obrigação aos órgãos da polícia judiciária à estruturação, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores (*internet*), dispositivo de comunicação ou sistema informatizado (BRASIL, Lei n.º 12.735/2012, 2013).

4.6 O MARCO CIVIL DA *INTERNET* – PROJETO DE LEI N.º 2.126/2011

No ano de 2009, a Secretaria de Assuntos Legislativos do Ministério da Justiça em conjunto com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas, no Rio de Janeiro, deu início a elaboração do projeto de lei posteriormente denominado como "Marco Civil da *Internet*", que tem por finalidade estabelecer direitos e deveres na utilização da *internet* no Brasil (MARCO..., 2013).

Na minuta de anteprojeto de lei para debate colaborativo, restam estabelecidos os direitos e garantias dos usuários, a provisão de conexão e de serviços de *internet*, esclarecendo acerca do tráfego de dados, dos registros de dados, da guarda de registros de conexão, da guarda de registros de acesso a serviços de *internet*, da proteção ao sigilo das comunicações pela *internet*, da remoção do conteúdo, além das propostas de novas redações e de supressão, bem como da atuação do Poder Público (MINUTA..., 2013).

Referido projeto tem ganhado forte apoio no país, obtendo pareceres favoráveis como, por exemplo, da Mozilla Foundation (criadora do *browser* "Firefox"), da RNP, e do CGI.br (Comitê Gestor da *Internet* no Brasil), como é possível vislumbrar em um dos *sites* que fazem a divulgação do projeto de lei (MARCO..., 2013).

Outro apoio, de grande nome, obtido recentemente, foi o de Tim Barners-Lee, o criador da *Web*:

> "Precisamos de algo que reforce a neutralidade da rede em benefício dos usuários", disse Lee ao argumentar que uma lei regulatória não basta e que deve haver consenso entre os provedores de internet para respeitarem essas decisões. A neutralidade pretende garantir que todos os conteúdos sejam tratados da mesma forma, independente de interesses comerciais de provedores e operadoras (CRIADOR..., 2013)

Apesar do apoio recebido, ainda há uma grande discussão com relação à sua aprovação, tendo em vista a falta de conhecimento dos parlamentares sobre a *internet* e seu funcionamento, além da pressão criada pelas empresas de telecomunicação e provedoras de serviço, que contestam pontos do projeto, como a privacidade dos usuários e a neutralidade no tratamento de dados (FALTA... 2013).

4.7 PREVENÇÕES

Existem várias medidas extrajudiciais que o usuário pode exercer para que não veja vítima de uma fraude eletrônica inerente ao *Internet Banking*. Desta forma, com o intuito de informatizar, segue lista dos principais cuidados que podem ser tomados por qualquer

usuário para defender-se destes perigos, com base na Cartilha de Segurança para *Internet* da Cert.br:

- Observar se o cabeçalho do *e-mail* é suspeito, bem como se aparenta estar incompleto;
- Verificar se no campo "assunto" do *e-mail* possui palavras com grafia errada ou suspeita, como no caso de utilizar símbolos ao invés de algumas letras ("fraude eletr&%nica", por exemplo), ou algum tipo de texto alarmante, vago demais, ou que chamem a atenção do usuário de algum modo suspeito ("parabéns, você ganhou R$ 1.000.000,00", por exemplo);
- Tomar cuidado com a opção de retirada do *e-mail* da lista de divulgação do remetente, pois o *link* pode remeter o usuário para o *download* do cavalo de tróia;
- Fazer uma filtragem das mensagens indesejadas, normalmente encontrados nos próprios correios eletrônicos, para que sejam automaticamente eliminadas ou que sejam encaminhadas para a caixa de *spam* ou lixo eletrônico do mesmo;
- Conferir se na pasta *spam* supracitada não possui mensagens legítimas que foram, erroneamente, classificadas como mensagens indesejadas;
- Analisar a real necessidade no fornecimento do *e-mail* (endereço eletrônico) do usuário ao *site*;
- Tomar um maior cuidado com as opções pré-selecionadas, encontradas normalmente no final de algum formulário disponibilizado pelo *site* acessado, como, por exemplo, quando se pergunta se o usuário deseja receber *e-mails* informativos do *site*;
- Não responder às mensagens indesejadas e não clicam nos *links* nelas inerentes;
- Criar outros endereços eletrônicos para disponibilizá-los em *sites* que aparentam encaminhar *spams*;
- Modificar as opções de privacidade nas redes sociais para diminuir o envio de mensagens, bem como para não deixar o endereço eletrônico utilizado visível a todos os outros usuários;
- Comunicar a instituição bancária sobre a tentativa de fraude, para que a mesma possa tomar a providências que achar cabíveis à situação;

- Manter-se informado através dos meios de comunicação sobre as tentativas de fraudes que ocorrem no cotidiano, como por meio de jornais que possuem seção de informática ou tecnologia num geral, *sites* bancários, bem como os que são criados para divulgação de listas de fraudes ocorridas no meio informático, tendo, como exemplo, o *site* "Monitor de Fraudes" (www.fraudes.org);
- Digitar corretamente o domínio do *site* da instituição financeira diretamente no navegador *Web*, não clicando, deste modo, em qualquer mensagem que contenha suposto *link* ou *download* de arquivo;
- Não pesquisar o *site* bancário desejado em *site* de busca (como "Google" – www.google.com);
- Sempre que possuir dúvida se existe possível fraude, entrar em contato com a central de atendimento do banco ou diretamente com seu gerente;
- Não realizar transações bancárias em computadores de terceiros ou em redes de *internet* públicas;
- Observar os extratos da conta bancária mensalmente para verificar se houve algum lançamento suspeito;
- Utilizar, de forma atualizada, métodos de segurança no computador, como um antivírus.

Observando as dicas supracitadas, o usuário da rede de computadores (*internet*) poderá "navegar", como é vulgarmente dito, de forma mais segura, evitando que os perigos da fraude eletrônica, que estão presentes no dia-a-dia de diversos computadores, relacionada com o *Internet Banking*, não lhe causem os malefícios estudados com o presente trabalho.

5 CONCLUSÃO

A fraude eletrônica, que significa a obtenção de proveito patrimonial de outrem através do uso ilícito de sistema informático ou telemático, está cada vez mais presente no *Internet Banking*, agindo através de mecanismos, sendo destacados o *scam*, o *phishing* e o *pharming*.

O primeiro diz respeito às mensagens que são encaminhadas em massa através de *e-mail*, por exemplo, ao usuário da *internet*, que contém um arquivo anexado ou um *link* para *download* de um arquivo, onde a vítima, ao executar este, acaba tendo seu computador contaminado por um cavalo de tróia (ou seja, um programa malicioso).

O segundo também trata de mensagens enviadas à vítima, porém estas objetivam iludir a mesma passando-se por empresas de grande nome, conhecidas por ela, tomando, desta forma, sua confiança.

Já o terceiro não necessita de encaminhamento de mensagens à vítima. Esta se depara com um *link* que, sem perceber que o domínio do mesmo encontra-se alterado, a redireciona a um *site* falso, mas que é muito similar ao *site* verdadeiro que o usuário lesado pretendia acessar.

Em todos os casos, o objetivo do criminoso é obter os dados da vítima a fim de acessar sua conta bancária, podendo, assim, subtrair valores que se encontram naquela como se fosse seu verdadeiro proprietário.

Antes da Lei 12.737/2012, estas condutas eram tipificadas ou em furto mediante fraude, ou em estelionato. Parte da doutrina e jurisprudência aplicava o primeiro crime tendo em vista que a subtração dos dados ou diretamente do dinheiro ocorre de forma imperceptível, não utilizando o criminoso, desta forma, de artifícios que induzam a vítima a erro. Já a outra parte entendia que não era o furto mediante fraude o tipo criminal cabível para a situação, mas sim o estelionato, pois, quando o autor do delito utiliza a senha do usuário que teve seu dado subtraído, e retira valores da conta bancária, a instituição financeira é iludida, possuindo, dessa forma, duas vítimas: o banco e seu cliente. Logicamente, as vítimas não gostam de perder o bem ora visado, ou seja, o dinheiro, e o fato de haver esta ilusão caracterizaria o estelionato.

Contudo, neste ano, entrou em vigor a Lei n.º 12.737/2012, comumente chamada de “Lei Carolina Dieckmann”, alterando o Código Penal Brasileiro, tipificando criminalmente os delitos informáticos. Foram delimitas tais condutas: invasão de dispositivo informático;

interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; e falsificação de cartão.

Para o tema abordado neste trabalho, a conduta que mais se destaca é a invasão de dispositivo informático, tendo em vista que o criminoso "desarma" o mecanismo de segurança existente no dispositivo, e, deste modo, pode coletar informações do proprietário da máquina, como os dados da conta bancária. Bom, para que este mecanismo de segurança seja desabilitado, o usuário pode utilizar-se de um *malware* para que haja sua infiltração no dispositivo, e este programa malicioso pode ter chegado até o usuário por meio de uma mensagem, por exemplo, caracterizando a prática do *scam*.

Uma comparação interessante feita por Márcio André Lopes Cavalcante, e que teve seu devido destaque no presente trabalho, é referente ao crime de invasão de dispositivo informático e o crime de furto mediante fraude. Restou claro que, uma possibilidade que poderá ser adotada, tanto doutrinaria quanto jurisprudencialmente, é que, por exemplo, quando ocorrer a subtração de dinheiro mediante coleta indevida dos dados do proprietário da conta bancária, permanecerá o entendimento de furto mediante fraude (lembrando que a comparação feita pelo autor excluiu o estelionato, possivelmente por fazer parte dos que preferem entender que a conduta aqui mencionada trata do estabelecido no art. 155, § 4º, II, do CP). Contudo, se ocorrer somente a subtração dos dados do usuário, sem que o dinheiro deste seja afetado, caracterizar-se-á, neste caso, o crime de invasão de dispositivo informático.

Mas ainda resta tratar sobre o *phishing* e o *pharming*. Estes, utilizando-se do raciocínio lógico, permaneceram no entendimento antigo, ou seja, a conduta se enquadrará ou no crime de furto mediante fraude, ou no crime de estelionato, dependendo do entendimento do julgador. Não se utiliza a "Lei Carolina Dieckmann" nestes casos, pois, a coleta de dados da vítima se dá mediante *site* ou mensagem falsa, que resulta no fornecimento das informações, não se utilizando, desta forma, da invasão no dispositivo informático, nem na interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (a menos que se enquadre neste caso), bem como da falsificação de cartão.

Infelizmente, por ter entrado em vigor em tão pouco tempo, não foi oportunizado entendimento jurisprudencial até o momento com relação à Lei n.º 12.737/2012. Ademais, não é só a jurisprudência que se mantém quieta com o assunto, mas a doutrina também. A razão para isto é que a população brasileira ainda não está totalmente adaptada aos costumes do ambiente virtual, como pode ser vislumbrado no crescimento progressivo dos delitos informáticos, e que, somente agora, está surgindo legislação competente para julgá-los

especifica e devidamente, como a própria lei já citada, assim como a Lei n.º 12.735/12 e o projeto de lei denominado como "Marco Civil da *Internet*", ambos conceituados nesta monografia.

Por fim, foram vislumbradas as medidas preventivas que os usuários da *internet* devem ficar atentos e obedecê-las sempre que possível (mas que, normalmente, passam despercebidas). É fundamental que a população brasileira tome ciência da importância na leitura atenciosa dos meios de comunicação proporcionados pela *internet*, como *e-mails* recebidos, formulários de *sites*, propagandas, entre outros. Também é importante que haja um intenso incentivo desta prática, para que as medidas preventivas tenham resultado.

Felizmente, como pôde ser vislumbrado neste trabalho, o Brasil tem se tornado um país cada vez mais preocupado com as condutas realizadas no ambiente virtual. Porém, ainda é necessário que as dúvidas sejam esclarecidas, e que as opiniões tornem-se únicas, para que haja a devida aplicação das penalidades, diminuindo, desta forma, a fraude eletrônica que se encontra no *Internet Banking*.

REFERÊNCIAS

ALECRIM, Emerson. **O que é dns (domain name system)?.** Disponível em: < http://www.infowester.com/dns.php>. Acesso em: 04 maio 2013.

AQUINO, Maria Clara. **Um resgate histórico do hipertexto:** o desvio da escrita hipertextual provocado pelo advento da Web e o retorno aos preceitos iniciais através de novos suportes. Disponível em: < http://www.bocc.ubi.pt/pag/aquino-maria-clara-resgate-historico-hipertexto.pdf>. Acesso em: 10 mar. 2013.

BANRISUL. **Home banking.** Disponível em: <http://www.banrisul.com.br/bob/link/bobw00hn_conteudo_detalhe2.aspx?secao_id=68>. Acesso em: 17 mar. 2013.

_____. **Office banking.** Disponível em: < http://www.banrisul.com.br/bob/link/bobw00hn_conteudo_detalhe2.aspx?secao_id=70>. Acesso em: 17 mar. 2013.

BARREIRA, Rafael dos Santos; LASALVIA, Vânia Cristina. **Comércio e marketing eletrônico.** Disponível em: <http://facape.br/textos/2008_008_COMERCIO_E_MARKETING_ELETRONICO.pdf>. Acesso em: 12 mar. 2013.

BITENCOURT, Cezar Roberto. **Tratado de direito penal.** 5. ed. São Paulo: Saraiva, 2009. v. 3.

BRASIL. Decreto-Lei n.º 2.848, de 07 de dezembro de 1940. **Código penal.** 12. ed. São Paulo: Saraiva, 2011.

_____. Lei n.º 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 maio 2013.

_____. Lei n.º 12.735, de 30 de novembro de **2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 18 maio 2013.

_____. Superior Tribunal de Justiça. **CC 67.343/GO.** Relatora: Min. Laurita Vaz. Brasília, DF, 28 de março de 2007. Disponível em: < http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=furto+fraude+eletr%F4nica&&b=ACOR&p=true&t=&l=10&i=10>. Acesso em: 02 mar. 2013.

_____. Tribunal Regional Federal da 3ª Região. **RSE 7720 SP 2010.61.02.007720-3**. Segunda Turma. Relator: Des. Fed. Cotrim Guimarães. São Paulo, SP, 16 de agosto de 2011. Disponível em: <www.trf3.jus.br>. Acesso em: 09 abr. 2013.

BARRETO, Ana Amélia Menna. **Correio eletrônico corporativo.** Disponível em: < http://www.nucleodedireito.com/correio-eletronico-corporativo/>. Acesso em: 11 mar. 2013.

BOGO, Kellen Cristina. **A história da internet –** como tudo começou... Disponível em: < http://www.jelapisdecor.com.br/downloads/seginternet/A_Historia_da_Internet.pdf>. Acesso em: 02 mar. 2013.

CABETTE, Eduardo Luiz Santos. **Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático.** Disponível em: < http://jus.com.br/revista/texto/23522/primeiras-impressoes-sobre-a-lei-no-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico/3>. Acesso em: 05 maio 2013.

CAPEZ, Fernando. **Curso de direito penal.** 7. ed. São Paulo: Saraiva, 2007. v. 2.

CASTRO, Sérgio Souza de. **Introdução ao correio eletrônico e webmail.** Disponível em: < http://www.juliobattisti.com.br/tutoriais/sergiocastro/correioeletronicoewebmail001.asp>. Acesso em: 11 mar. 2013.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático.** Disponível em: < http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 05 maio 2013.

CERT.br. Cartilha de segurança para internet. **CÓDIGOS maliciosos (malware).** Disponível em: < http://cartilha.cert.br/malware/>. Acesso em: 29 abr. 2013.

_____. **Estatísticas de notificações de spam reportadas ao cert.br.** Disponível em: < http://www.cert.br/stats/spam/>. Acesso em: 29 abr. 2013.

_____. Cartilha de segurança para internet. **GOLPES na internet.** Disponível em: < http://cartilha.cert.br/golpes/>. Acesso em: 04 maio 2013.

_____. Cartilha de segurança para internet. **SPAM.** Disponível em: < http://cartilha.cert.br/spam/>. Acesso em: 29 abr. 2013.

CRIADOR da web defende aprovação do marco civil da internet no Brasil. Disponível em: < http://adrenaline.uol.com.br/internet/noticias/16804/criador-da-web-defende-aprovacao-do-marco-civil-da-internet-no-brasil.html>. Acesso em: 18 maio 2013.

DAMASCENO, Leonardo Geraldo Baeta. **Aspectos penais sobre as transações bancárias indevidas via internet banking.** Disponível em: <http://jus.com.br/revista/texto/9697/aspectos-penais-sobre-as-transacoes-bancarias-indevidas-via-internet-banking>. Acesso em: 02 mar. 2013,

DAPONT, Pablo. **Curso de HTML com PHP:** HTML. Disponível em: < http://www.inf.ufrgs.br/pet/cursos/HTML/Curso%20de%20HTML%20com%20PHP%20(Pablo%20Dapont)/apostila%20HTML.pdf>. Acesso em: 11 mar. 2013.

EMC. **The year in phishing.** Disponível em: <http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf>. Acesso em: 04 maio 2013.

ESTRADA, Manuel Martin Pino. **A internet banking no Brasil, na América Latina e na Europa.** Disponível em: < http://egov.ufsc.br/portal/sites/default/files/anexos/32680-40136-1-PB.pdf>. Acesso em: 17 mar. 2013.

FALTA de conhecimento dos deputados impede a aprovação do marco civil da internet. Disponível : < http://adrenaline.uol.com.br/internet/noticias/15398/falta-de-conhecimento-dos-deputados-impede-a-aprovacao-do-marco-civil-da-internet.html>. Acesso em: 18 maio 2013.

FEBRABAN. CIAB FEBRABAN 2012. **A Sociedade conectada.** Disponível em: < http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Ciab12-Anuario%20Febraban%2006.07.pdf>. Acesso em 17 mar. 2013.

FRAUDES por mail – scam, transferência de fundos. Disponível em: <http://pt.kioskea.net/contents/attaques/scam.php3>. Acesso em: 16 abr. 2013.

FULLER, John. **Como funcionam os cavalos-de-troia.** Adaptado de How trojan horses works. Disponível em: <http://informatica.hsw.uol.com.br/cavalo-de-troia.htm>. Acesso em: 29 abr. 2013.

GIL, Antonio de Loureiro. **Fraudes informatizadas.** 2. ed. São Paulo: Atlas, 1999.

GUIZZO, Érico Marui. **Internet:** o que é: o que oferece: como conectar-se. São Paulo: Ática, 2002.

HISTÓRIA das redes no Brasil. Disponível em: <http://www.ime.usp.br/~is/abc/abc/node25.html>. Acesso em: 07 mar. 2013.

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

INTERNET, navegação, navegadores e pesquisa. Disponível em: < http://proinfodigital.pbworks.com/f/MODULO+3.pdf>. Acesso em: 11 mar. 2013.

KUROSE, James F.; ROSS, Ketih W. **Redes de computadores e a internet:** uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010.

LEITÃO JÚNIOR, Esdreas Avelino. **O e-mail como prova no direito.** Disponível em: < http://jus.com.br/revista/texto/3025/o-e-mail-como-prova-no-direito>. Acesso em: 11 mar. 2013.

LÔBO, Gino Sérvio Malta. **Saque fraudulento pela internet:** furto ou estelionato. Disponível em: <http://jus.com.br/forum/58068/saque-fraudulento-pela-internet-furto-ou-estelionato/>. Acesso em: 09 abr. 2013.

MACHADO, Jonathan D. **O que é keylogger?.** Disponível em: < http://www.tecmundo.com.br/spyware/1016-o-que-e-keylogger-.htm>. Acesso em: 29 abr. 2013.

MARCO civil da internet. Disponível em: <http://marcocivil.com.br/>. Acesso em: 18 maio 2013.

MARTINS, Elaine. **O que é backbone?.** Disponível em: <http://www.tecmundo.com.br/conexao/1713-o-que-e-backbone-.htm>. Acesso em: 02 mar. 2013.

MAZIERO, Carlos A. **O serviço dns.** Disponível em: < http://dainf.ct.utfpr.edu.br/~maziero/doku.php/espec:servico_dns>. Acesso em: 04 maio 2013.

MENEZES, Rodolfo Rosa Telles. **Nova visão sobre a aplicação do aumento de pena do furto noturno ao furto qualificado.** Disponível em: < http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10599&revista_caderno=3>. Acesso em: 18 maio 2013.

MICROSOFT. **O que é phishing?.** Disponível em: <http://www.microsoft.com/pt-br/security/resources/phishing-whatis.aspx>. Acesso em: 04 mai. 2013.

MINUTA de anteprojeto de lei para debate colaborativo. Disponível em: <http://culturadigital.br/marcocivil/debate/>. Acesso em: 18 maio 2013.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de direito penal.** 25. ed. São Paulo: Atlas, 2008. v. 2.

NEUBUSER, Ilmar et al. **A percepção dos clientes de um sistema de internet banking.** Disponível em: <http://www.ead.fea.usp.br/Semead/7semead/paginas/artigos%20recebidos/marketing/MKT40_-_Percep%E7%E3o_dos_clientes_de_um_sistema_I.PDF>. Acesso em: 17 mar. 2013.

NOGUEIRA, Sandro D'Amato. **Crimes de informática.** Leme: BH, 2008.

NORTON. **Fraude on-line:** pharming. Disponível em: <http://br.norton.com/cybercrime-pharming/promo>. Acesso em: 04 maio 2013.

NOVO malware altera boletos bancários gerados na web e desvia pagamentos. Disponível em: < http://adrenaline.uol.com.br/seguranca/noticias/16393/novo-malware-altera-boletos-bancarios-gerados-na-web-e-desvia-pagamentos.html>. Acesso em: 19 maio 2013.

NUNES, Sérgio. **World wide web.** Disponível em: < http://paginas.fe.up.pt/~ssn/2012/cdi/slides/04-web.pdf>. Acesso em: 10 mar. 2013

PADILHA, Ênio; CARVALHO, Cláudia Gomes; GALLAS, Juliana. **Marketing e comércio eletrônico.** 2. ed. Palhoça: UnisulVirtual, 2007.

PERSEGONA, Marcelo Filipe Moreira; ALVES, Isabel Teresa Gama. **História da internet:** Origens do E-Gov no Brasil. Disponível em: < http://ffb.virtual.ufc.br/solar/arquivos/curso/367/historia_da_internet.pdf>. Acesso em: 07 mar. 2013.

PINHEIRO, Patricia Peck. **Direito digital.** 4. ed. São Paulo: Saraiva, 2010.

PINHO, José Benedito. **Publicidade e vendas na internet:** técnicas e estratégias. São Paulo: Summus, 2000.

POPULARIZAÇÃO da internet: introdução ao uso de correio eletrônico e *web*. Disponível em: < http://www.rnp.br/_arquivo/documentos/ref0186.pdf>. Acesso em: 10 mar. 2013.

PRADO, Luiz Regis. **Curso de direito penal brasileiro.** 11. ed. São Paulo: Revista dos Tribunais, 2013, v. 2.

RNP. CAIS. **Catálogo de fraudes**. Disponível em: <http://www.rnp.br/cais/fraudes.php>. Acesso em: 04 maio 2013.

ROSA, Fabrízio. **Crimes de informática.** 2. ed. Campinas: Bookseller, 2005.

SÊMOLA, Marcos. **Internet banking:** o canal alternativo. Disponível em: < http://www.semola.com.br/disco/Coluna_IDGNow_F0.pdf>. Acesso em: 17 mar. 2013.

SILVA, Jean Paulo da et al. Internet banking. **Revista da Informática Aplicada**, v. 2, nº 02, jul/dez 2006. p. 76-85. Disponível em: < http://seer.uscs.edu.br/index.php/revista_informatica_aplicada>. Acesso em: 18 mar. 2013.

SIMON, Cláudio Antônio de Paiva. **Scam, phishing e pharming:** as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil. Disponível em: <http://www.alfa-redi.org/node/8970>. Acesso em: 02 mar. 2013.

STANTON, Michael. **A evolução das redes acadêmicas no Brasil:** parte 1 - da BITNET à internet. Adaptado de Non-commercial networking in Brazil. Disponível em: <http://www.rnp.br/newsgen/9806/inter-br.html>. Acesso em: 05 mar. 2013.

UOL. **Códigos maliciosos (malware).** Disponível em: <https://sac.uol.com.br/info/cartilha/malware/sec2.jhtm>. Acesso em: 29 abr. 2013.

ANEXOS

ANEXO A – *Phishing*

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama *online*
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
Sites com dicas de segurança	aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Tabela – Exemplos de tópicos e temas de mensagens de *phishing*. (Fonte: Cert.br, 2013)