UNIVERSIDADE DO SUL DE SANTA CATARINA

THÁBATA CLEZAR DE ALMEIDA

O ESTELIONATO DIGITAL NO *E-COMMERCE*: A FRAUDE DA LOJA VIRTUAL FANTASMA

Araranguá - SC

2013

THÁBATA CLEZAR DE ALMEIDA

O ESTELIONATO DIGITAL NO *E-COMMERCE*: A FRAUDE DA LOJA VIRTUAL FANTASMA

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. Esp. Diego Archer de Haro.

Araranguá

2013

THÁBATA CLEZAR DE ALMEIDA

O ESTELIONATO DIGITAL NO *E-COMMERCE*: A FRAUDE DA LOJA VIRTUAL FANTASMA

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.

_____

Prof. Diego Archer de Haro, Esp.
Universidade do Sul de Santa Catarina

_____

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

_____

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

Dedico este trabalho aos meus pais, Everaldo e Eunice, por me ensinarem que longe é um lugar que não existe e que o impossível é só uma questão de ponto de vista.

AGRADECIMENTOS

Ao meu orientador, professor e delegado Diego Archer de Haro, cuja experiência no tema em estudo sempre acompanhei e muito admirei enquanto estudante de Direito nesta cidade.

À professora Fátima Hassan Caldeira, pela paciência em me atender até mesmo em momentos cujos quais gozava de suas férias e pela experiência técnica passada.

Agradeço ao meu amor, Rangel Simon, pela paciência comigo, dedicação e amizade nas madrugadas regadas a café e, principalmente, por me fazer erguer a cabeça e persistir em meu sonho, mesmo quando ninguém mais acreditou que eu fosse capaz de realizar este trabalho.

Também aos meus pais, Everaldo Goulart de Almeida e Eunice Clezar de Almeida, por todo o amor e esforço dedicado para que eu pudesse chegar até aqui e continuasse a sonhar cada vez mais longe.

Ao meu irmão, Everaldo Goulart de Almeida Júnior, pela experiência científica que me deu mais segurança para começar este trabalho que mais parecia um Tiamat.

E aos meus queridos – e não menos importantes - Mayumi Arimura de Melo, Morgana Vargas Cândido, Cássio Cardoso Cândido e Lucas Tejada da Silva, pelas risadas e discussões acalouradas vividas, cujas amizades entrelaçaram sonhos, lágrimas e sorrisos, tão preciosos para que a serenidade pairasse nos olhos desta autora a cada momento em que o medo de falhar na conclusão deste trabalho surgia.

“O conformismo é o carcereiro da liberdade e o inimigo do crescimento” (John Fitzgerald Kennedy).

“E no meio do Aqui e Agora, não acha que podemos nos encontrar de vez em quando?” (Richard Bach).

RESUMO

A fraude da loja virtual fantasma, objeto do presente estudo, constitui-se na venda fraudulenta pela internet, através de um comércio virtual inidôneo, destinado a ludibriar aqueles que procuram produtos a preços mais baixos do que o mercado oferta e que pagam antecipado, mas nunca recebem que compraram. Isso gera problemas jurídicos que justificam o presente trabalho, tais como: a discussão sobre a possibilidade de aplicação do crime de estelionato a esse ato delituoso; se seria, outrossim, fato atípico ou, ainda, se seria necessário, em razão desse segundo argumento, tratamento criminal diferenciado, a fim de evitar a impunidade dos agentes. Nesse contexto, o presente estudo, baseando-se em julgados dos tribunais estaduais mais recentes e na doutrina sobre o tema, objetivou estudar a possibilidade da aplicação da lei penal já existente a essa fraude, sem a necessidade de novo tratamento criminal diferenciado. Para isso, partindo-se do método de abordagem dedutivo, utilizou-se da pesquisa exploratória para alcançar o objetivo proposto. Ainda, no tocante à coleta de dados, aplicou-se os tipos de pesquisa bibliográfica e documental, uma vez que foi feita a análise de livros, revistas, jornais, doutrinas e jurisprudências sobre o tema. Como resultado, foi possível descobrir que, hoje, é possível aplicar a lei penal existente, consubstanciada no crime de estelionato, como forma de persecução criminal para punir os agentes que cometam a fraude da loja virtual fantasma.

Palavras-chave: Estelionato. Fraude. Comércio eletrônico. Venda fraudulenta. Internet.

ABSTRACT

The virtual ghost fraud of store, object of the present study, constitutes in the fraudulent selling by the Internet through an untrusted virtual commerce, intended to deceive those who seek products at lower prices than the market offers and who pay anticipated, but they never receive what they bought. That generates legal problems that justify the present work, such as the discussion on the applicability of the crime of stellionate to that criminal act, if it would, moreover, atypical, or even if it would be necessary, because of that second argument, criminal differentiated treatment in order to avoid the impunity of the agents. In this context, the present study, based on state judged of the courts and the latest doctrine on the subject, aimed at studying the possibility of the application of criminal law existing to this fraud, without the need for new differentiated criminal treatment. For that, starting from the deductive approach it was used exploratory research to achieve the proposed objective. As far as the collection of data, it was applied the types of bibliographic and documental research, because the analysis was of books, magazines, newspapers, doctrines and jurisprudence on the subject. As a result, it was found that today it is possible to apply existing criminal law, consubstantiated in the crime of stellionate, as a form of criminal prosecution to punish agents who commit the virtual ghost fraud of store.

Keywords: Stellionate. Fraud. E-commerce. Fraudulent Selling. Internet.

SUMÁRIO

1 INTRODUÇÃO

O *e-commerce*, o qual, em tradução livre, significa comércio eletrônico teve sua origem durante a década de 1970, quando as primeiras descobertas sobre a possibilidade da transação de dados via rede começaram a surgir.

E foi assim que um dos primeiros modelos de comércio eletrônico foi criado. E ele nada mais é do que as operações comerciais realizadas pela tecnologia; ou seja, o mesmo comércio, mas cujo veículo de transação pode se dar por: telefone (*t-commerce)*, computador (e-commerce), *tablet* ou *smartphone* (*m-commerce)*, conectado à rede mundial de computadores (diga-se *internet*).

Esse avanço foi fantástico, se considerar que se pode, com isso, comprar a preços baixos, grande variedade de produtos e com informações detalhadas sobre eles, como uma câmera digital de outro país, por exemplo, ou, simplesmente, fazer as compras do mercado sem sair de casa, seja pela economia, seja pelo cansaço que, às vezes, o mau atendimento de um vendedor, numa loja física, pode proporcionar ao consumidor.

Ocorre que essa praticidade trouxe tanto bons quanto maus frutos, porque, junto com ela, começaram a se formar verdadeiras quadrilhas digitais. Agentes, em sua maioria, jovens e detentores de avançado conhecimento sobre tecnologia, passaram a se unir e, em conluio de esforços e acordo de vontades, com o ânimo de obter vantagens ilícitas de montantes altíssimos sobre esse fenômeno, passaram a se utilizar de dados de pessoas físicas e jurídicas inocentes e a criar páginas na internet com produtos à venda por preços atrativos, como se um *e-commerce* idôneo fosse, bem como criando contas correntes ou se utilizando de contas já existentes (laranjas) de outras pessoas para receber a vantagem.

Assim, o presente trabalho tem por objeto estudar essa forma de fraude, que ficou conhecida por loja virtual fantasma.

1.1 OBJETIVO

Nesse sentido, o objetivo da presente monografia é estudar a possibilidade da aplicação da lei penal já existente à fraude da loja virtual fantasma, como forma de estelionato, de modo que, em não sendo possível, procurar-se-á, elencar o que falta para ela se tornar aplicável.

1.2 JUSTIFICATIVA

Pelo fato de ainda se discutir sobre a possibilidade da aplicação do crime de estelionato à fraude da loja virtual fantasma na doutrina, em razão de a legislação penal brasileira não explicitar se esse seria um fato típico com novo modo de agir ou uma situação albergada pela atipicidade, isso gera uma sensação de impunidade aos agentes. E é exatamente por esse sentimento de impunidade diante de condutas praticadas na rede mundial de computadores que se faz proliferar o número de vítimas desses estelionatários virtuais, os quais se divertem à custa de ingênuos e à custa da morosidade da justiça.

Em doutrina, pouco se escreve sobre esse problema de consequências milhonárias, justamente em função da dormência legislativa em aprovar projetos de lei relacionados ao comércio eletrônico. Tamanho é o problema, que se estima que as perdas decorrentes de fraudes representem 0,4% do valor arrecadado com as operações efetuadas no comércio eletrônico (conforme CRESCEM..., 2013). E esse valor parece tímido, mas assusta, se considerar que o faturamento do setor fechou o ano de 2012 com o lucro de R$ 49,7 bilhões, por exemplo (segundo CONFIRA..., 2013).

Cientes disso, os legisladores brasileiros aprovaram modificações no Código de Defesa do Consumidor neste ano e estudam, ainda, a possibilidade de dar tratamento criminal diferente nessa hipótese de fraude por meio da internet. Mas ainda se discute se é realmente necessário ou se seria, atualmente, fato atípico, razão pela qual, necessário se faz estudar a fundo essa problemática neste trabalho.

1.3 ORGANIZAÇÃO DO TRABALHO

Para a produção deste trabalho, utilizar-se-á do método de abordagem dedutivo, utilizando-se da pesquisa exploratória para alcançar o objetivo proposto. Para tanto, tocante à coleta de dados, aplicar-se-á os tipos de pesquisa bibliográfica e documental, uma vez que será feita a análise de livros, revistas, jornais, doutrinas e jurisprudências sobre o tema.

A pesquisa foi desenvolvida a partir da hipótese de que, com a análise jurídica do que se tem de concreto em Direito Penal hoje, existe a possibilidade de aplicá-lo à nova modalidade de estelionato digital, consistente na fraude das lojas virtuais fantasmas, podendo os agentes serem punidos com os elementos probatórios virtuais.

Diante disso, o presente trabalho foi dividido em três capítulos, sendo que o primeiro foi dedicado ao *E-commerce*, seu histórico, definições e modalidades.

Já no segundo capítulo, tratar-se-á do Estelionato, bem como seu objeto jurídico, sujeitos do crime, tipo objetivo, tipo subjetivo, consumação e tentativa, torpeza bilateral, fraude penal e civil, formas de estelionato e um adendo sobre sua pena, majorante, ação penal e foro competente.

Por fim, no terceiro capítulo, enfrentar-se-á o fenômeno da fraude da loja virtual fantasma, passando-se, brevemente, por definições, modalidades da fraude, (in)aplicabilidade da pretensão punitiva aos agentes, alterações trazidas pela Lei n. 12.735/12, alterações trazidas pela Lei n. 12.737/12, alterações trazidas pela Decreto n. 7.962/13, bem como as possibilidade de mudanças com a reforma do Código de Defesa do Consumidor, com o projeto de lei do Marco Civil e com a futura adesão a acordos de cooperação internacional, além de outras providências para solucionar o problema.

2 *E-COMMERCE*

Ao tratar do e-commerce, também chamado de comércio eletrônico, considera-se como o conjunto de compra e venda de informações, bens e serviços por intermédio da rede mundial de computadores (internet). Segundo Crespo (2011, p. 193), "[...] é qualquer forma de transação comercial, onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da internet".

Este capítulo estudará o e-commerce, apresentando seu histórico, conceitos e definições, segundo a doutrina, bem como trazendo um diálogo com outras fontes, como alguns conceitos de tecnologia da informação e comunicação e de administração. Trará, ainda, os tipos de comércio eletrônico que se conhece hoje para facilitar a compreensão do tema neste trabalho em estudo.

2.1 HISTÓRICO

Turban e King (2004, p. 7) relatam que as primeiras aplicações do Comércio Eletrônico ocorreram no início da década de 1970, com novidades como a transferência eletrônica de fundos (TEF), na qual era possível transferir dinheiro eletronicamente, através da simples transferência de dados. Entretanto, essa transferência, exatamente por ser muito nova, acabava por ficar restrita a grandes corporações, dispostas a investir nessa tecnologia até então estranha e cara.

Posteriormente, surgiu o EDI, ou *Eletronic Data Interchange*, que, em tradução livre, significa troca eletrônica de dados, sendo essa, uma tecnologia capaz de transferir eletronicamente dados e documentos, como ordens de compra, faturas e pagamentos eletrônicos entre organizações. Os mesmos autores relatam, a título de exemplo, que tal avanço permitiu uma maior participação de empresas financeiras, de manufatura, de revenda e prestadora de serviços. Essas inovações foram chamadas de "sistemas interorganizacionais" (IOS em inglês ou *Interorganizational System*).

Segundo Felipini (2011), a origem do e-commerce propriamente dita remonta ao final da década de 1970, quando o empresário e inventor inglês Michael Aldrich descobriu que era possível criar sistemas de compras online. Esses sistemas, na época, ficaram conhecidos como *teleshopping*, tendo sido posteriormente denominado como *Internet Shopping*, até chegar ao *Eletronic Commerce* ou *E-commerce* que se tem hoje (ALDRICH, 2013a).

Outrossim, o comércio eletrônico, entre uma empresa e seus consumidores, como se conhece hoje, só se desenvolveu, de fato, a partir da década de 1990, com a popularização da internet e da World Wild Web (popularmente conhecida como *WWW) (*ALDRICH, 2013b*)*.

Entende-se por "World Wild Web", também chamado apenas de "Web" ou "WWW", o sistema capaz de interligar documentos dispostos na internet, tendo sido criado pelo cientista britânico Tim Bernes-Lee, em 1990, cujo foco foi facilitar o compartilhamento e a exploração das informações em documentos gráficos interligados por *hypertexto* (MACHADO, 2013).

Nesse sentido, Paioello e Furtado (2004, p. 1-2) melhor explicam:

> A Internet e a WWW permitiram que o Comércio Eletrônico ficasse mais acessível para um grande volume de novos usuários. E esse acesso, dependendo da natureza tecnológica da conexão, deve permitir uma interação mais segura, mais rápida e mais fácil.

Pouco se sabe sobre a origem exata do primeiro comércio eletrônico no Brasil, mas foi na década de 2000 que ele tomou fôlego e galgou andares em seu avanço, tendo expressão no país. Os primeiros comércios virtuais que se tem conhecimento surgiram já no ano de 1999, quando o Mercado Livre (GRUPO MERCADO LIVRE, 2013), a Submarino e as lojas Americanas lançaram suas respectivas páginas na internet destinadas ao fim comercial (GRUPO B2W, 2013).

2.2 DEFINIÇÕES

Para compreender melhor a fraude da loja virtual fantasma, deve-se entender o conceito de *e-commerce* ou comércio eletrônico. Albertin (2010, p. 3) ensina que é a "realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio". Nesse mesmo sentido, continua explicando o autor que os processos "podem ser realizados de forma completa ou parcial, incluindo as transações negócio-a-négocio, negócio-a-consumidor e intraorganizacional, numa infraestrutura predominantemente pública e de fácil e livre acesso e baixo custo".

Kalakota e Whinston *apud Turban e King* (2004, p. 3), acrescentam, ainda, que se pode definir o comércio eletrônico sob quatro perspectivas:

> **A perspectiva da comunicação**: o CE é a distribuição de produtos, serviços, informação ou pagamentos por meio de redes de computadores ou outros meios eletrônicos.
> **A perspectiva do processo comercial**: o CE é a aplicação de tecnologia para a automação de transações e do fluxo de trabalho.

> **A perspectiva de serviços:** o CE é uma ferramenta que satisfaz a necessidade de empresas, consumidores e administradores quanto à diminuição de custos e à elevação nos níveis de qualidade e agilidade de atendimento.
> **A perspectiva online:** o CE é a possibilidade de compra e venda de produtos e informações pela Internet e por outros serviços on-line (grifos do autor).

Há que se abrir um parêntese, ainda, para diferenciar *e-commerce* de *e-business*, uma vez que enquanto o primeiro significa o comércio eletrônico como a transação entre parceiros de negócios (bem como as fases anterior e posterior à transação econômica) em si, ao passo que o segundo é mais abrangente, englobando, segundo Norris et al (2001, p. 6), três estágios: o comércio eletrônico, o negócio eletrônico e as parcerias eletrônicas.

Pinheiro (2010, p. 89) entende que a sociedade digital, como ela é atualmente, já tomou para si o comércio eletrônico como um novo formato de negócios. Ainda, segundo a autora:

> Já existem o *e-commerce*, o *m-commerce* e o *t-commerce*, dependendo se o veículo de transação eletrônica é um computador, um celular ou dispositivo de comunicação móvel, ou a televisão. A tendência é que esse formato se amplie cada vez mais, conforme a tecnologia se torne mais acessível, a rede mais estável e as normas-padrão mais aplicáveis.

Explicados os conceitos preliminares necessários a este capítulo, passa-se agora para as modalidades de comércio eletrônico mais conhecidas, para se chegar ao objeto de estudo do presente trabalho.

2.3 MODALIDADES DE *E-COMMERCE*

Têm-se as seguintes modalidades de comércio eletrônico: *business to business* (ou empresa a empresa), *business to consumer* (ou empresa para consumidor), *consumer to business* (consumidor a empresa), *consumer to consumer* (consumidor para consumidor), *business to employees* (empresa a funcionários), bem como as modalidades que circunscrevem o *e-government* (governo eletrônico), quais sejam: *government to government* (governo a governo), *government to citizen* (governo para cidadão), *citizen to government* (cidadão a governo), *government to business* (governo para empresa) e *business to government* (empresa a governo), como se verá a seguir.

2.3.1 *Business to Business* (B2B) ou Empresa a Empresa

Sem dúvida, essa é a modalidade de comércio eletrônico mais antiga conhecida, onde há a transação econômica via internet de uma empresa para outra.

É comum, nesse caso, exemplos como comércio atacadista, compra de serviços, tecnologias, equipamentos, componentes ou mesmo transações financeiras, onde uma empresa-cliente compra de uma empresa-fornecedora, como a Ford e a General Motors, por exemplo, que utilizam-se dessa modalidade para o fornecimento de equipamentos, dados e serviços entre si.

Paioello e Furtado (2004, p. 2) ensinam que, na perspectiva do B2B, "o Comércio Eletrônico facilita as aplicações de negócios, beneficiando o gerenciamento de fornecedores, estoque, distribuição, canal e pagamento".

Segundo Pinheiro (2010, p. 93), nesse mercado B2B, "concentra-se o maior volume de transações da Internet: os metamercados, como são chamados os pontos de encontro virtuais entre empresas compradoras e fornecedoras", o que, segundo a autora, acaba por trazer uma grande redução de custos operacionais para seus participantes. Acrescenta, ainda, que funcionam como "pregões privados: muitas vezes o *site* pode ser equiparado à figura do corretor".

2.3.2 *Business to Consumer* (B2C) ou Empresa a Consumidor

Nessa modalidade, o contrato comercial se realiza quando um consumidor final visita a página da internet de uma empresa e nesse *site*, efetua uma transação comercial virtual.

Inicialmente mais utilizado para a compra de livros e CDs, atualmente, essa modalidade possui os mais variados setores, tais como alimentício, lazer, viagens, jogos, vestuário, eletrônico, literário, entre outros.

Turban e King (2004, p. 6), a título de exemplo, mencionam a norte-americana <www.amazon.com>, onde é possível uma pessoa física comprar qualquer produto listado no *site* da empresa. Esse tipo de comércio eletrônico é também chamado de varejo eletrônico (*e-tailing*), embora não seja essa sua nomenclatura mais popular.

No Brasil, exemplos como a <www.americanas.com.br>, a <www.submarino.com.br> e a <www.kabum.com.br> são exemplos de comércio eletrônico em que a transação eletrônica sempre se dá entre a empresa proprietária do domínio comercial virtual e o consumidor final.

2.3.3 *Consumer to Business* (C2B) ou Consumidor a Empresa

Nessa modalidade, ocorre o inverso da anterior; ou seja, nela, é o consumidor quem presta ou vende serviços ou produtos para organizações empresariais através da internet.

Conforme Turban e King (2004, p. 6), também pertence a essa modalidade a situação de "pessoas que procuram vendedores a fim de que ofereçam lances, para obter produtos ou serviços de que necessitam". É o chamado leilão reverso, onde, segundo os autores, os compradores enumeram os itens que gostariam de adquirir e os vendedores fazem seus lances, a fim de fornecer tais itens pelo menor preço.

Os autores usam o exemplo do *site* <www.priceline.com>, no qual o consumidor escolhe entre as opções de vôos, hotéis, aluguel de carros, pacotes de férias e cruzeiros, estabelecendo padrões como data de partida e chegada, destino e quanto se quer pagar. Posterior a isso, o site busca em diversas empresas, de modo que essas ofertam, conforme o padrão requerido pelo consumidor em sua pesquisa.

No Brasil, há exemplos como <www.hotelurbano.com>, <www.decolar.com>, <www.cvc.com.br> e <www.malapronta.com>, onde semelhantes serviços são oferecidos, em claro exemplo da modalidade C2B.

Toledo *et al* (2005, p. 32) explicam que, nessa modalidade, "o consumidor torna-se uma voz ativa no processo de compra de produtos ou serviços pela internet. É o cliente definindo como deseja ser atendido, a que preço e de que forma".

2.3.4 *Consumer to Consumer* (C2C) ou Consumidor a Consumidor

Nela, há a transação comercial entre pessoas físicas, onde um consumidor compra, diretamente de outro, através da internet, produtos, serviços, conhecimentos especializados de *freelancers* ou até mesmo dados (como a conta de um jogo de computador, por exemplo).

E exemplos não faltam sobre esse modelo no exterior, como no caso do <www.guru.com>, para procurar *freelancers* e do <www.ebay.com>, que é, basicamente, um mercado livre norte-americano, onde usuários podem colocar à venda produtos novos e usados para que outros consumidores adquiram.

No Brasil, há exemplos como o <www.mercadolivre.com.br>, semelhante ao e-bay e a <www.olx.com.br>, multinacional virtual, cujo *slogan* é "onde vendedores acham compradores", tendo características semelhantes às do mercado livre e às do e-bay, onde o *site* oferta espaços na internet para que terceiros vendam seus próprios produtos e serviços, após aceitação dos termos e condições de uso do *site*.

Ao anunciar um item para venda, o anunciante (consumidor-vendedor) estabelece os termos da oferta do bem, preço, categoria, condições de venda, entrega e pagamento, sem

qualquer interferência do *site* hospedeiro, passando, então, a ser divulgado o anúncio do produto, como se estivesse em uma página de classificados de um jornal.

Sem dúvida, essa modalidade é a que mais cresce nas redes sociais, principalmente pela facilidade que os consumidores têm de se comunicarem pela rede, criando uma página para a loja virtual vinculada ao perfil do usuário da rede social, como é o caso do <www.facebook.com>.

Dentro dessa modalidade existe também uma segunda, qual seja a *peer-to-peer* (P2P), na qual pessoas compartilham música, vídeo, *software*, entre outros produtos digitalizados, sem o intermédio de uma empresa e por meio de um *site*.

Nesse caso, existem exemplos de transações sem fins lucrativos - que geram, muitas vezes, problemas de lesão a direitos autorais, tais como o <www.megaupload.com> e o <www.4shared.com> - e com fins lucrativos, como é o caso da <www.napster.com>.

2.3.5 *Business to Employees* (B2E) ou Empresa a Funcionários

Nessa modalidade, há a transação eletrônica de dados, produtos, informações e serviços da empresa para seus funcionários ou de uma empresa que se especializa na capacitação de trabalhadores, como é o caso de *sites* especializados em aprendizado de idiomas como o <www.livemocha.com> e o <www.inglesonline.com.br>.

É uma modalidade bastante utilizada pelas empresas, que muitas vezes, criam *intranets* - redes internas em que os funcionários podem acessar, através de um nome de usuário e senha, na página principal da empresa – ou na própria página principal, em seções específicas para os funcionários.

A Intranet, combinada com outras tecnologias, dão azo ao modelo de negócio B2E. Hansen e Deimler *apud* Singh *et all* (2007, p. 98) ensinam que há três componentes principais integrando esse modelo, quais sejam: processos de negócio online, gestão de pessoas online e serviços online para o ambiente de trabalho.

A título de exemplo, no site <www.landesigners.com.br>, há a sessão “ACESSO RESTRITO”, onde somente funcionários e colaboradores, detentores de um nome de usuário e senha, podem ter acesso a dados e serviços exclusivos da empresa de Tecnologia da Informação aplicada a negócios.

2.3.6 E-Government: modalidades de CE com a Administração Pública

O *e-government* é a Administração Pública, direta ou indireta, em um dos polos do negócio, seja fornecendo dados, serviços ou produtos, seja adquirindo-os.

Nesse sentido, Pinheiro (2010, p. 185) assim explica:

> No âmbito do Direito Administrativo, os princípios de publicidade dos atos públicos e probidade administrativa fazem com que a Internet seja um meio extremamente adequado para não apenas publicar o que está sendo feito como também para funcionar como um canal direto de comunicação com cidadãos e contribuintes. Assim como para operações bancárias o uso de meios eletrônicos reduz muito o custo das transações, para o governo o meio eletrônico possibilita realizar a um baixo custo procedimentos licitatórios, além de dar maior transparência a eles.

Segundo Caldas (2010), também conhecido por "e-gov", o governo eletrônico é um fenômeno que adveio do uso intensivo das tecnologias da informação e comunicação (TIC). Ganhou destaque, principalmente, na campanha eleitoral do presidente norte-americano Barack Obama, quando este ganhou a corrida da disputa por um dos cargos mais importantes da atualidade se utilizando do uso maciço de canais e redes sociais, tais como *Twitter, blogs, Orkut, Likedin, Youtube* e *Facebook*. Mais do que inaugurar a era das campanhas políticas digitais, Obama sinalizou sua disposição pessoal em investir na construção de um novo modelo de gestão pública, balizado por um consistente programa de governo eletrônico.

Para Paioello *et all* (2004, p. 6), "os governos estão começando a reorganizar a administração dos sistemas públicos de arrecadação, proporcionando um prospecto considerável de transações de B2G". Os autores continuam dizendo que a tecnologia também está sendo usada para transmitir e receber transações na perspectiva do modelo G2B (governo a empresas), G2C (governo a cidadãos) e também para facilitar e reduzir os custos das formas de pagamento e restituições de impostos, na modalidade C2G (cidadão a governo).

Nesse sentido, as principais modalidades de comércio eletrônico em matéria de *e-gov* são o G2G (*Government to Government* ou Governo a Governo*),* G2C (*Government to Citizen* ou Governo a Cidadão), G2B (*Government to Business* ou Governo a Empresas), C2G (*Citizen to Government* ou Cidadão a Governo) e, por fim B2G (*Business to Government* ou Empresas a Governo).

1.3.1.1 *Government to Government* (G2G) ou Governo a Governo

Também chamado de Administração a Administração (*Administration to Administration* ou A2A), neste caso, conforme Turban e King (2004, p. 246), ocorre a transferência eletrônica de dados, serviços e informações entre duas Administrações Públicas,

podendo ser de mesma esfera ou não, entre órgãos e até mesmo entre governos de diversos países.

A exemplo disso, a Rede INFOSEG, no site <www.infoseg.gov.br>, da Secretaria Nacional de Segurança Pública, integra vários bancos de dados em um único programa, no qual, com o devido nome de usuário e senha, o gestor ou funcionário público pode acessar dados de uma pessoa com relação ao seu histórico de endereços residenciais, ao RENAJUD, Banco Nacional de Mandados de Prisão, aos antecedentes criminais, entre outras informações relevantes.

Inclusive, no mesmo site, tem-se o intercâmbio de informações internacionais, tais como a Base de Dados de Procurados pela INTERPOL e também o Sistema de Intercâmbio de Informações de Segurança do Mercosul – SISME.

1.3.1.2 *Government to Citizen* (G2C) ou Governo a Cidadão

Na modalidade G2C, que também é conhecida por *Administration to Citizen* ou A2C, é a Administração Pública quem oferece serviços, dados e acesso a informações aos seus administrados por meio de um endereço eletrônico disponível.

Nesse sentido, Nunes e Vendrametto (2009, p. 7) assim conceituam:

> O Government to Citzen ou G2C utiliza o canal da Internet e a tecnologia da informação para que o governo possa interagir diretamente com o cidadão. Para isto, são desenvolvidos portais ou sistemas, que permitem a interação do cidadão nas ações do governo.

No Brasil, é possível efetuar quase que na sua totalidade o procedimento da declaração do imposto de renda no próprio *site* da Receita Federal. No mesmo site, é possível expedir tributos, podendo o cidadão pagá-los sem sair de casa, utilizando-se o *internet banking* do banco que ele preferir, por exemplo.

1.3.1.3 *Government to Business* (G2B) ou Governo a Empresa

Já na modalidade G2B, a Administração oferece produtos, serviços, dados e acesso a informações a pessoas jurídicas, por meio de um *site*. Tal tipo também é chamada por *Administration to Business* ou A2B.

Assim, nas palavras de Nunes e Vendrametto (2009, p. 7), consiste esta modalidade no "relacionamento do Governo com empresas através da tecnologia da informação". Continuam os autores, acrescentando que esse relacionamento se desenvolveu "de forma transacional,

através de portais de compras eletrônicas via Internet, buscando a simplificação e desburocratização dos processos licitatórios e a racionalização do processo de interação entre o Governo e seus fornecedores".

No Brasil, na mesma página da internet da Receita Federal, há a sessão exclusiva para empresas, onde é possível fazer os mesmos serviços, mas oferecidos da Administração para uma pessoa jurídica.

1.3.1.4 *Citizen to Government* (C2G) ou Cidadão a Governo

Já na modalidade C2G, ocorre o inverso, uma vez que é o administrado quem vende ou oferece serviços à Administração Pública (SOUSA, 2013, p. 14). É também conhecida por *Citizen to Administraton, Consumer to Administration* ou C2A.

Na prática, essa modalidade é muito confundida com a modalidade G2C (a ser vista a seguir), havendo estudos que, inclusive usam os mesmos exemplos para ambas modalidades, o que não deve prosperar, ainda que não seja tão corriqueira no Brasil a presente modalidade analisada.

Exemplos que se poderia citar, hipoteticamente seria na hipótese de a Administração Pública abrir concurso público virtual para cidadãos enviarem hinos para a cidade ou até a formulação de uma página da internet de uma prefeitura, por exemplo, em que o vencedor ganharia uma contraprestação em dinheiro do órgão público. No Brasil, casos assim são mais utilizados com empresas (modalidade B2G), mas é perfeitamente possível a incidência de situações parecidas, em que haveria uma transparência e economia com atos burocráticos muito maior.

1.3.1.5 *Business do Government* (B2G) ou Empresa a Governo

Por outro lado, na modalidade B2G, são as empresas que oferecem seus produtos e serviços para que o Governo faça suas aquisições necessárias; garantindo, assim, maior publicidade e transparência dos seus atos. Essa modalidade também pode ser encontrada com a nomenclatura *Business to Administration* ou B2A.

Para Souza (2013, p. 14) essa modalidade engloba "todas as transacções realizadas on-line entre as empresas e a Administração Pública" [sic]. Continua o autor, dizendo que é uma área que "envolve uma grande quantidade e diversidade de serviços, designadamente nas áreas fiscais, segurança social, emprego, registos e notariado, etc".

Nesse sentido, os exemplos mais conhecidos são as licitações *online* (pregões eletrônicos), como no site < http://www.governoeletronico.gov.br/acoes-e-projetos/compras-eletronicas> e a Bolsa Eletrônica do Estado de São Paulo, disponível no site < http://www.bec.sp.gov.br>.

Além da vantagem da praticidade, é possível a maior transparência com relação às aquisições da Administração Pública.

No presente trabalho, discorrer-se-á, especificamente, sobre as situações de fraude nas modalidades *Business to Consumer (B2B)* – onde uma suposta empresa virtual oferece produtos e serviços a consumidores a preços atraentes, abaixo da média dos preços encontrados em outras lojas – e *Consumer to Consumer* (C2C) – na qual ocorre semelhante situação, mas que vem crescendo, ante à facilidade maior de criar a loja virtual por essa forma de comércio eletrônico, aliada à informalidade da relação bilateral. Mas, antes, convém apreciar acerca do tipo penal estelionato em si.

3 ESTELIONATO

Figura já consolidada no ordenamento jurídico brasileiro, o estelionato se trata de uma figura típica do Código Penal vigente, no qual contém um conceito já em seu *caput* do art. 171, como se vê a seguir:

> Art. 171. 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.
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2º - Nas mesmas penas incorre quem:
> **Disposição de coisa alheia como própria**
> I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> **Alienação ou oneração fraudulenta de coisa própria**
> II - 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;
> **Defraudação de penhor**
> III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
> **Fraude na entrega de coisa**
> IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> **Fraude para recebimento de indenização ou valor de seguro**
> V - 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;
> **Fraude no pagamento por meio de cheque**
> VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência (BRASIL, CP, 2013, grifo do autor).

Oriunda do latim, da palavra *stellionatus* (de *stellius*, que significa camaleão, animal que adapta as cores de suas escamas ao ambiente em que se encontra, para ludibriar seus predadores e presas), o que representaria, segundo Noronha (1996, p. 369), a natureza proteiforme do delito.

Fragoso (2006) *apud* Bitencourt (2011, p. 227) explicam que o tipo surgiu somente a partir do império (século II d.C.), aparecendo, inicialmente, como um tipo penal genérico e subsidiário, vindo a evoluir, já no século seguinte, como a forma mais grave de fraude, juntamente com a extorsão, o rapto, o aborto e a exposição de infante (FRAGOSO, 2006, p. 36).

Os mesmos autores acrescentam, ainda, que em alguns ordenamentos jurídicos, como nas Ordenações Filipinas, de 1603, tamanha era a importância que se dava ao prejuízo patrimonial, que se punia o estelionato (conhecido como “burla” ou “inliço”) com pena de morte, caso a vantagem ilícita indevida fosse superior a vinte mil-réis.

Segundo Prado (2013, p. 566), foi somente no século XIX que o estelionato obteve a autonomia como delito contra o patrimônio.

No Brasil, a tipificação penal do estelionato já surge a partir do primeiro código penal brasileiro, o Código Criminal do Império, promulgado em 16 de dezembro de 1830. Previsto no art. 264, estabelecia como pena o trabalho e multa de cinco a vinte por cento do valor da coisa. Veja-se:

> Art. 264. Julgar-se-ha crime de estellionato:
> 1º A alheação de bens alheios como proprios, ou a troca das cousas, que se deverem entregar por outras diversas.
> 2º A alheação, locação, aforamento, ou acarretamento da cousa propria já alheiada, locada, aforada, ou arretada á outrem; ou a alheiação da cousa propria especialmente hypothecada á terceiro.
> 3º A hypotheca especial da mesma cousa á diversas pessoas, não chegando o seu valor para pagamento de todos os credores hypothecarios.
> 4º Em geral todo, e qualquer artificio fraudulento, pelo qual se obtenha de outrem toda a sua fortuna, ou parte della, ou quasquer titulos.
> Penas – de prisão com trabalho por seis mezes a seis annos e de multa de cinco a vinte por cento do valor das cousas, sobre que versar o estellionato [sic](BRASIL, Código Criminal de 1830).

Seguindo a noção de que se precisaria de um tipo genérico semelhante ao item "4º" do supra referido artigo e, diante de novas fraudes que surgiam, sem que a proteção Estatal conseguisse enumerá-las no tipo penal, o Código Penal Republicano sobreveio, em 11 de outubro de 1890, trazendo no art. 338, onze modalidades exemplificativas de estelionato e adaptando o tipo genérico, como se observa no item "5º", este que seria o embrião do *caput* do atual art. 171 do Código Penal de 1940:

> Art. 338. Julgar-se-ha crime de estellionato:
> [...]
> 5º Usar de artificios para surpehender a boa fé de outrem, illudir a sua vigilancia, ou ganhar-lhe a confiança; e induzindo-o a erro ou engano por esses e outros meios astuciosos, procurar para si lucro ou proveito [sic](BRASIL, Decreto n. 847/90, 2013).

E não é só. Segundo Prado (2013, p. 567), o Código Penal brasileiro de 1940 também teve como fonte de inspiração basilar o Código Penal italiano de 1930. Veja-se:

> Art. 640.
> Truffa.
> Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.[...] (ITÁLIA, Codice Penale, 2013).

Então, nas palavras de Plantullo (2003, p. 60) e Mirabete e Fabbrini (2006, p. 287), haverá o crime de estelionato quando o agente empregar qualquer que seja o meio fraudulento capaz de induzir e manter em erro a vítima, numa falsa percepção de realidade, a fim de obter uma vantagem ilícita patrimonial indevida.

Assim, Noronha (1996, p. 369) resume o conceito ao seguinte polinômio: meio fraudulento, erro, vantagem ilícita, lesão patrimonial, os quais, cumulativamente, formam o estelionato.

3.1 OBJETO JURÍDICO

Como ensinam Mirabete e Fabbrini (2006, p. 289), no crime de estelionato, o que se pretende proteger é a violação do patrimônio da vítima e, também, "a boa-fé, segurança, fidelidade e veracidade dos negócios jurídicos patrimoniais, embora esta apareça em caráter secundário, já que o estelionato é um crime contra o patrimônio".

Nesse sentido, Manzini *apud* Bitencourt (2009, p. 228) ensinam que o estelionato "não é considerado como um fato limitado à agressão do patrimônio de Tício ou de Caio, mas antes como manifestação de delinqüência que violou o preceito legislativo, o qual veda o servir-se da fraude para conseguir proveito injusto com dano alheio", independentemente de quem for a vítima. Continuam os autores, expondo que "o estelionatário é sempre um criminoso, mesmo que tenha fraudado em relações que, por si mesmas, não merecem proteção jurídica, porque sua ação é, em qualquer caso, moral e juridicamente ilícita".

Ainda, Prado (2013, p. 571) e Noronha (1996, p. 372) complementam, justificando a necessidade da proteção penal contra a lisura e a má-fé nas relações econômicas e negociais como algo que é fundamental para a preservação da vida social e não por serem simples atividades individuais.

3.2 SUJEITOS DO CRIME

Com relação ao sujeito ativo, para Mirabete e Fabbrini (2006, p. 2), qualquer pessoa (tratando-se, portanto, de crime comum) pode ser o sujeito ativo do crime, admitindo-se, perfeitamente, o conluio de esforços e de vontades entre agentes, nos termos do art. 29 do Código Penal, não se exigindo para a incriminação do beneficiado, como acrescentam Noronha (1996, p. 372) e Prado (2013, p. 571), que intervenha materialmente na cena do crime. É possível que também o proveito patrimonial seja destinado a terceiro que, segundo os autores, só responde como co-autor ou partícipe se for comprovada sua má-fé e que, como também ensina Gonçalves (s/d) *apud* Capez (2008, p. 538), comprove-se que o terceiro induziu o agente a cometer o delito em proveito dele.

Ocorre que se esse terceiro, não participante da fraude, descobre a mesma antes de obter sua vantagem patrimonial e se, ainda assim, a recebe, ele incidirá no delito de receptação, previsto no art. 180 do Código Penal, observando-se, ainda, se sua conduta foi culposa ou dolosa; ou seja, se ele tinha conhecimento que a coisa seria produto de estelionato.

Tocante ao sujeito passivo, Bitencourt (2009, p. 228) ensina que pode ser, igualmente, qualquer pessoa, natural ou jurídica. Também esse tipo não impede que a vítima da vantagem ilícita e da fraude sejam pessoas diferentes, como no exemplo trazido pelo autor, em que o empregado sofre o golpe (fraude), mas quem arca com o prejuízo é seu empregador.

Sobre essa desnecessidade de nexo causal entre a vítima da fraude e a da lesão patrimonial propriamente dita, Noronha (1996, p. 372) ainda esclarece que "não há dúvida de que deve haver nexo causal entre o erro e a lesão ao patrimônio, porém isso não importa seja a mesma pessoa que os suporte".

É importante salientar que a vítima precisa ser pessoa certa e determinada, uma vez que, tratando-se de pessoas indeterminadas (como no caso de se descobrir um *e-commerce* fraudulento, mas que não se tem a ocorrência de vítimas concretas ainda), pode se configurar crime contra a economia popular ou contra as relações de consumo, dependendo da situação.

Além de certa e determinada, é preciso dizer que essa pessoa precisa ter capacidade de discernimento, uma vez que não há que se falar em crime de estelionato quando a vítima for criança ou quando tiver qualquer tipo de alienação ou debilidade mental previamente constatada. Caso a vítima se encaixe nessa situação, configurar-se-á o delito de abuso de incapazes, previsto no art. 173 do Código Penal. Se a vítima não tem, outrossim, sequer condições de ser ludibriada, como um ébrio em estado de coma, por exemplo, configurar-se-á o delito de furto, previsto no art. 155 do Código Penal (BITENCOURT, 2009 p. 229).

3.3 TIPO OBJETIVO

Consiste em obter vantagem ilícita (seja para si seja para outrem), em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. Esse, segundo Prado (2013, p. 572), é o tipo básico, simples, anormal e incongruente.

Bitencourt (2009, p. 231) sintetiza, dizendo que "a característica fundamental do estelionato é a *fraude*, utilizada pelo agente para *induzir* ou *manter* a vítima em *erro*, com a finalidade de obter vantagem patrimonial ilícita" (grifo do autor).

Jesus (2009, p. 649), Prado (2013, p. 572) e Bitencourt (2009, p. 231-232) concordam no sentido de que há, consequentemente, uma duplicidade de nexo causal, uma vez que, em um primeiro momento, a fraude praticada pelo autor é a causa do engano da vítima; enquanto que, em um segundo momento, há nova relação de nexo causal, em que o erro da vítima se torna a causa e a obtenção da vantagem ilícita; ou seja, o segundo efeito.

É importante frisar que deve haver a obtenção da vantagem patrimonial ilícita, uma vez que o fato de ter a vítima sido ludibriada e/ou mantida em erro pela fraude provocada pelo agente, sem que tenha sofrido um prejuízo financeiro concreto, não é causa suficiente para a deflagração da ação penal por parte do Estado.

Então, três são os elementos fundamentais para a caracterização do delito de estelionato, conforme Bitencourt (2009, p. 232):

> A configuração do crime de estelionato exige a presença dos seguintes requisitos fundamentais: 1) *emprego de artifício, ardil ou qualquer outro meio fraudulento*; 2) *induzimento ou manutenção da vítima em erro*; 3) *obtenção de vantagem patrimonial ilícita em prejuízo alheio* (grifo do autor).

Considerando os meios empregados trazidos pelo *caput* do art. 171 do Código Penal, convém, igualmente, explicá-los. Artifício é a capacidade de enganar; é a manha, o fingimento (MICHAELIS, 2013). Nas palavras de Mirabete e Fabbrini (2008, p. 289-290):

> Artifício existe "quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos, luz, etc".

Já o ardil, segundo Capez (2008, p. 536), "é fraude no sentido imaterial, intelectualizada, dirigindo-se à inteligência da vítima e objetivando excitar nela uma paixão, emoção ou convicção pela criação de uma motivação ilusória". O autor continua exemplificando com as situações de uma boa conversa, uma simulação de doença, "sem nenhum outro disfarce ou aparato, além da 'cara-de-pau'".

Convém mencionar a posição de Noronha (1996, p. 374) com relação a essa distinção entre o ardil e o artifício:

> Não nos parece tão segura e constante qualquer diferença entre o ardil e o artifício, e de qualquer modo, em face de nossa lei, toda diferença seria de valor relativo, uma vez que, após mencioná-los, alude a *qualquer outro meio fraudulento*, usando, assim, fórmula a mais ampla possível. Empregando essa expressão, ela se refere a qualquer atitude ou comportamento que provoque ou mantenha o erro, do qual advirão a vantagem ilícita e o dano patrimonial. Com o emprego do *meio fraudulento*, na oração, podia até a lei deixar de referir-se ao ardil e ao artifício, pois estes, sem dúvida, estão nele incluídos, tal o sentido compreensivo que tem (grifo do autor).

Com relação a "qualquer outro meio fraudulento", esse foi o meio genérico que o legislador procurou colocar na ação nuclear para quando não se encaixasse nem no ardil e tampouco no artifício. É como Mirabete e Fabbrini (2009, p. 290):

> Não é necessário [sic], assim, como previsto em outras legislações, a *mise-em-scène*, a encenação, a criação de um aparato que leve ao erro. Pode-se inserir, inclusive, o *silêncio* do agente, quando tem este o dever jurídico de esclarecer a verdade dos fatos, uma vez que, nos termos do art. 147 do CC, "nos negócios jurídicos bilaterais o silêncio intencional de uma das partes a respeito de fato ou qualidade que a outra parte haja ignorado, constitui omissão dolosa, provando-se que sem ela o negócio não se teria celebrado". [...]. Comprovado que, *ab initio*, o agente não desejava cumprir com o aventado, mas apenas obter a vantagem indevidamente, configurado está o estelionato (grifo do autor).

Então, concordando com os referidos autores, acrescentam Jesus (2009, p. 648) e Noronha (1996, p. 375) que em "qualquer outro meio fraudulento" também está inserida a mentira verbal, além do já citado silêncio do agente, dependendo do contexto fático.

Assim como já foi dito que a vítima tem que ter capacidade de discernimento, também o meio fraudulento empregado tem que possuir certa idoneidade; ou seja, ele precisa ser capaz de enganar o conceito de "homem médio", trazido por Manzini, ou também chamada de prudência natural das pessoas. No entanto, como entende Capez (2008, p. 537), "quando totalmente inapta a iludir, mesmo o mais ingênuo dos mortais, o fato será atípico".

Com relação ao segundo requisito fundamental (induzimento ou manutenção da vítima em erro), induzir, segundo o dicionário Michaelis (2013), significa persuadir à prática de alguma coisa. Para Mirabete e Fabbrini (2008, p. 291), o agente, nesse caso, "toma a iniciativa de causar o erro, levando a vítima à falsa representação da realidade". Já na manutenção da vítima em erro, continuam os autores, ela ocorre quando o erro acontece anteriormente (podendo a vítima ter praticado por acidente), mas o agente procura dar continuidade, prolonga essa falsa percepção de realidade da vítima, a fim de lucrar com isso.

Nesse sentido, abre-se parêntese para se conceituar a elementar típica "erro". Já foi dito aqui que ela consiste na falsa percepção da realidade, o que Capez (2008, p. 537) melhor explica:

> A situação na qual a vítima acredita [que] não existe. Houvesse o conhecimento verdadeiro dos fatos, jamais teria ocorrido a vantagem patrimonial ao agente, que, para obtê-la, provoca ou mantém a vítima em erro (nesta última [sic] hipótese, o autor aproveita uma situação preexistente, um erro espontâneo anterior por ele não provocado, e emprega manobras fraudulentas para manter esse estado e assim obter a vantagem ilícita).

Tocante ao terceiro e último requisito (obtenção da vantagem patrimonial ilícita em prejuízo alheio), a ação nuclear do tipo penal em estudo consiste em "obter", o que, segundo o dicionário Michaelis (2013), significa alcançar, lograr, conseguir coisa desejada ou pedida.

Vantagem ilícita consiste no objeto material do presente crime. Prado (2013, p. 572-573) acrescenta, ainda, que "*vantagem ilícita* é todo o benefício ou proveito contrário ao Direito, constituindo, portanto, elemento normativo jurídico do tipo de injusto" (grifo do autor).

Fragoso *apud* Mirabete e Fabbrini (2008, p. 291) e Damásio E. de Jesus *apud* Capez (2008, p. 537) concordam no sentido de que essa vantagem ilícita precisa ser econômica, uma vez que se trata de crime contra o patrimônio. Dessa forma, pelo entendimento desses autores, não se caracterizaria o crime de estelionato quando um agente, por exemplo, obtivesse as provas de um concurso público para um candidato que presta o gabarito naquele dia do exame, uma vez que embora seja a vantagem moralmente condenável, se não há prejuízo patrimonial alheio, não há que se falar em estelionato.

Entretanto, há quem discorde disso, como Bitencourt (2009, p. 235-237), seguidor do principal representante da corrente divergente nesse assunto, Edgard Magalhães Noronha. Segundo Noronha (1996, p. 381), malgrado o art. 171 estivesse dentro do capítulo que trata dos crimes contra o patrimônio, o legislador não especificou o tipo de vantagem ilícita que deveria ocorrer para que se caracterizasse o crime de estelionato, como assim a lei o fez com relação ao crime de extorsão, por exemplo, em que trata da "indevida vantagem econômica".

Assim, por esse argumento, caberia o crime de estelionato quando no caso do exemplo do parágrafo anterior. Ocorreria a lesão ao patrimônio público quando a pessoa aprovada em concurso público, mediante fraude, ingressasse efetivamente no cargo e começasse a receber a remuneração pelo serviço público.

Nesse sentido, em situação semelhante, já entendeu o Tribunal de Justiça de Santa Catarina:

> O dano ao erário decorrerá do recebimento de vencimento pelos "apadrinhados" aprovados em razão da fraude.
> O serviço, por sua vez, também sofrerá prejuízo por ser prestado por pessoas que não tenham sido selecionadas em razão de sua competência, gerando prejuízo à qualidade do serviço público (SANTA CATARINA, TJ, 2013a).

Ainda, Noronha (1996, p. 383) complementa, no sentido de que essa vantagem também deve ser juridicamente considerável, o que, segundo o autor, "[...] por certo, não impede sua pouquidade, mas indica a exigência de ser apreciável, isto é, suscetível de apreciação".

3.4 TIPO SUBJETIVO

Nesse caso, consiste na análise do dolo específico do agente; ou seja, nas palavras de Prado (2013, p. 579), é a "[...] consciência e vontade de enganar a outrem, mediante qualquer meio fraudulento, visando à concreção de vantagem ilícita em detrimento do patrimônio alheio".

Dessarte, é preciso que o agente tenha tanto a vontade livre e consciente de ludibriar alguém, quanto à intenção de obter lucro ou o proveito indevido, uma vez que, caso contrário, segundo Capez (2008, p. 540), não tendo o agente a consciência de que a vantagem almejada é ilícita, poderá ele responder por exercício arbitrário das próprias razões.

Dessa forma, não há que se falar em modalidade culposa com relação ao crime de estelionato.

Convém comentar a respeito do dolo com relação à modalidade de estelionato virtual que será estudada no presente trabalho, no próximo capítulo, uma vez que muito se discutiu nos tribunais acerca do dolo dos agentes (quando a vítima deposita o valor da compra para esses e, supostamente, tendo a posse de tal quantia, mesmo cientes de que não poderão cumprir com o negócio jurídico, deixando de restituir de restituir à vítima), se seria caso de apropriação indébita ou furto mediante fraude.

Entretanto, o entendimento de desclassificação para o delito de apropriação indébita seria mais cabível nas situações de lojas virtuais idôneas que, após a vítima cancelar a compra recém-feita de um produto, deixassem de restituir valores que ela tenha pagado, com o escopo específico de obter para si a vantagem indevida.

No caso da fraude da loja virtual fantasma, os agentes, associam-se (muitas vezes havendo, também, a incidência do crime de formação de quadrilha) para o fim específico de elaborar um *e-commerce* que pareça idôneo, induzindo e mantendo em erro as vítimas, para delas obter vantagens econômicas ilícitas indevidas; o que, nesse caso, configurar-se-ia o delito de estelionato.

Nesse sentido, Capez (2008, p. 511) assim distingue os dois delitos:

> Na apropriação indébita, a coisa é entregue livremente ao agente. Este não emprega nenhum artifício para obter a posse ou a detenção da coisa. *Não há o emprego de fraude iludente da vontade do proprietário. A posse e a detenção são obtidas de forma lícita*. No estelionato, o agente emprega artifícios que induzem a vítima em erro. Esta lhe entrega o bem sem saber que está sendo enganada. A posse ou a detenção pelo agente é ilícita (grifo nosso).

Com relação à classificação como delito de furto mediante fraude, a sexta turma do Superior Tribunal de Justiça, em 2009, analisando o fenômeno da compra fraudulenta pela internet (onde ocorre o inverso da situação a ser estudada no presente trabalho, uma vez que é o consumidor que, utilizando-se de cartões de crédito e dados de terceiros, realiza compras em comércios eletrônicos idôneos), entendeu de maneira que, na prática, acaba-se por aplicar também à venda fraudulenta por meio da internet. Veja-se:

> [...] o furto mediante fraude não pode ser confundido com o estelionato. No furto, a fraude é utilizada para burlar a vigilância da vítima, para lhe tirar a atenção. No

> estelionato, a fraude objetiva obter consentimento da vítima, iludi-la para que entregue voluntariamente o bem (COMPRA..., 2013).

Finalizado o comentário, passa-se para o próximo tópico, qual seja, a análise de quando se consuma o estelionato e se é admissível a tentativa nesse caso.

3.5 CONSUMAÇÃO E TENTATIVA

O estelionato, em sua forma fundamental, consuma-se a partir do momento em que, após ludibriada ou induzida em erro a vítima, ocorre a obtenção da vantagem ilícita em prejuízo alheio.

Nesse sentido, Bitencourt (2009, p. 239) entende que "não basta a existência do erro decorrente da fraude, sendo necessário que da ação resulte vantagem ilícita e prejuízo patrimonial de outrem".

Prado (2013, p. 579-580) ainda complementa, no sentido de que esse prejuízo alheio precisa ser de natureza patrimonial e efetiva pelo fato de que o estelionato "não é crime de perigo, mas sim de resultado. A lesão ao patrimônio do sujeito pode ocorrer tanto pela sua diminuição como por fator impeditivo de seu aumento". E Noronha (1996, p. 382), seguindo o mesmo raciocínio, acrescenta que "[...] exige modificação do mundo exterior, como conseqüência da ação, lesando o bem jurídico tutelado".

Ainda, Mirabete e Fabbrini (2008, p. 293) definem, também, que essa consumação não está condicionada ao "efetivo enriquecimento do agente, bastando apenas o dano patrimonial do ofendido". Continuam, dizendo é jurisprudência pacífica do Pretório Excelso, o entendimento de que o "ressarcimento do prejuízo não exclui o crime de estelionato, como ocorre no caso do pagamento de cheque sem suficiente provisão de fundos antes da denúncia", mas fará diferença tão somente quanto à aplicação da pena, servindo, essa reparação do dano, de causa de diminuição da pena.

Noronha (1996, p. 383) esclarece, também, "o proceder *gratuito* de quem concede a vantagem não exclui o dano" (grifo do autor), como no caso em que alguém doa ou subsidia uma suposta instituição beneficente, sem esperar uma contraprestação em troca. Nesse caso, se obtidos por fraude, acarretam vantagem indevida para o agente ou para terceiro e, por via de consequência, originam o dano e completam o crime.

Com relação aos atos jurídicos praticados pela vítima, resultantes de erro, dolo, coação, simulação ou fraude, a legislação civil os considera como anuláveis, mas o mesmo autor supracitado entende que "mesmo o ato nulo [...] não exclui o delito, uma vez que, produzindo efeitos, haja causado dano ao sujeito passivo" (idem).

Para Bitencourt (2009, p. 239), há que se frisar a importância da idoneidade da fraude, uma vez que, em caso de inidônea, como já visto, tratar-se-á de crime impossível. O autor ainda classifica a idoneidade como relativa ou absoluta, "sendo relativamente inidôneo o meio fraudulento para enganar a vítima, poderá configurar-se tentativa de estelionato" e a absoluta, naturalmente, encaixar-se-á na situação de crime impossível.

Já com relação à tentativa, é perfeitamente cabível, uma vez que, por se tratar de crime de natureza material, admite-se o seu fracionamento, quando "[...] o percurso do crime pode ser interrompido por motivos alheios à vontade do agente, desde o início da execução até quando está prestes a consumar-se, o que caracteriza a tentativa (art. 14, II)" (PRADO, 2013, p. 580).

Segundo Bitencourt (2009, p. 239), o estelionato requer a cooperação da vítima, uma vez que o início de sua execução se dá com o engano dela. Assim, continua o autor, não conseguindo o agente enganar a vítima, "o simples emprego de artifício ou ardil caracteriza apenas a prática de *atos preparatórios*, não podendo se cogitar de tentativa de estelionato" (grifo do autor). Lembrando que esse meio fraudulento precisa ser apto a enganar a vítima, uma vez que, senão, tratar-se-á de crime impossível.

Há que se mencionar, ainda, o comentário feito por Noronha, acerca da reparação do dano. Segundo ele, "[...] a reparação do dano não é elemento do delito, não entra em sua constituição", mas, sim, "é um fato posterior que não pode suprimir ou fazer desaparecer o que já se realizou no mundo externo" (1996, p. 387).

3.6 TORPEZA BILATERAL

Também conhecida como fraude bilateral ou, ainda, fraude recíproca, ocorre quando também se percebe a má-fé da vítima; ou seja, "a esperança de um proveito ilícito, o êxito fácil e ilegal, a avidez do lucro fazem com que ela caia no engodo armado pelo agente" (NORONHA, 1996, p. 384).

A grande questão desse tópico é se isso afeta a responsabilização do agente, em função do comportamento da vítima influenciar na consumação do crime de estelionato.

Para Nelson Hungria e Heleno Claudio Fragoso, principais representantes da corrente doutrinária minoritária sobre o assunto, isso não seria passível de punição, uma vez que, segundo eles, baseando-se no direito penal alemão e romano, "a torpeza pune a torpeza". Argumentavam, ainda, os autores, ao seu tempo (1980, p. 192-193) que:

> Não só os argumentos de ordem prática ou de política criminal, senão de rigorosa lógica jurídica justificam na espécie, a indiferença do direito penal. O patrimônio individual cuja lesão fraudulenta constitui o estelionato é o *juridicamente protegido*, e somente goza da proteção do direito o patrimônio que serve a um fim legítimo, dentro de sua função econômico-social. Desde o momento que ele é aplicado a um fim ilícito ou imoral, a lei, que é a expressão do direito como *mínimo ético* indispensável ao convívio social, retira-lhe o arrimo, pois, de outro modo, estaria faltando à sua [sic] própria finalidade (grifo do autor).

Entretanto, não é esse o entendimento dominante, representado por Noronha (1996, p. 385), Mirabete e Fabbrini (2008, p. 291), Nucci (2008, p. 787), entre outros, os quais entendem que há, sim, o estelionato, independentemente da análise da má-fé do ofendido.

E Capez (2008, p. 650) bem resume os argumentos mais apontados por estes expertos:

> [...] a) o autor revela maior temibilidade, pois ilude a vítima e lhe causa prejuízo; b) não existe compensação de condutas no Direito Penal, devendo punir-se o sujeito ativo e, se for o caso, também a vítima; c) a boa-fé do lesado não constitui elemento do tipo do crime de estelionato; d) o dolo do agente não pode ser eliminado apenas porque houve má-fé, pois a consciência e vontade finalística de quem realiza a conduta independe da intenção da vítima.

E é esse mesmo entendimento válido para os jogos de azar, os quais não excluem o estelionato, conforme Capez (2008, p. 542) e Jesus (2009, p. 650).

Nesse sentido, já decidiu o Tribunal de Justiça catarinense, baseando-se em decisão anteriormente prolatada pelo Tribunal de Justiça carioca:

> Comete o crime de estelionato quem com o propósito de locupletar-se ilicitamente, confecciona bilhetes de rifa, vende-os e não entrega o prêmio ao vencedor, nem devolve as quantias angariadas aos compradores de boa-fé.
> "A alegação de que o crime tem tipificação impossível, porque a rifa é considerada jogo de azar, não socorre a pretensão absolutória, porque, ainda que se admita torpeza na instituição de tais jogos, essa torpeza é, no caso, unilateral, do agente, já que a motivação dos adquirentes, por sua finalidade benemerente, é de nobreza, valendo acrescentar-se que, mesmo no jogo proibido, se ocorre a fraude, dela decorre a repressão penal" (TACrimRJ, AC 54.878/95, Comarca de Miracema - ac. un. - 3ª Câm. - rel. Juiz Índio Brasileiro Rocha - j. em 1º.6.95) (SANTA CATARINA, Tribunal de Justiça, 2013b).

Complementando esse entendimento, Noronha (1996, p. 386), ao seu tempo, também entendia que "[...] se a lei admite crime, quando o sujeito passivo comete também delito ou contravenção, não há razão para se excluir o estelionato, por ocorrer má-fé do iludido".

3.7 FRAUDE PENAL E FRAUDE CIVIL

Para Capez (2008, p. 542), Bitencourt (2011, p. 291) e Prado (2013, p. 578), em que pese a preocupação de alguns doutrinadores em distinguir a fraude penal da fraude civil, ambas, individualizadas, não existem, pois a fraude é uma só. A questão é a de se analisar se a conduta do agente é tão grave que mereça a punição do Estado em caráter *ultima ratio*; ou seja, o último

recurso, como o é o Direito Penal, e não tão somente a reparação de eventuais danos na esfera civil.

E para isso, Bitencourt (2011) acrescenta que é preciso analisar se todos os requisitos do estelionato estão presentes, pelo fato de que, embora a vítima possa se sentir enganada, não estando devidamente caracterizado o crime, a sua única alternativa será buscar o ressarcimento na vara cível competente para tanto.

Hungria e Fragoso (1980, p. 173) já diziam, ao seu tempo, que o Estado só deve recorrer à pena "quando a conservação da ordem jurídica não se possa obter com *outros meios de reação*, isto é, com os meios próprios do direito civil (ou de outro ramo do direito que não o penal)" (grifo dos autores).

Outrossim, Capez (2008) entende que "situações há em que, mesmo nos negócios civis ou comerciais, vislumbra-se o emprego de fraude configuradora do crime de estelionato". Como no caso do inadimplemento preordenado ou preconcebido, em que o agente simula realizar um negócio comercial com a intenção, desde o início, de não cumprir e obter, para si, uma vantagem ilícita. Para o autor, considerando-se que, nesse caso, o propósito do agente sempre foi o não adimplemento contratual, caracterizar-se-ia, sim, o delito de estelionato, dadas as circunstâncias fáticas e a comprovação do dolo do agente. Nesse caso, haveria a situação em que fraudes penal e civil se confundiriam, razão pela qual, caberia a sanção penal e o ressarcimento civil.

Noronha (1996, p. 387) e Capez (2008, p. 543), ensinam que, em tais casos, ante à dificuldade de se impor critérios para a distinção e devida responsabilização penal, caberá ao juiz analisar, no caso concreto, em qual fraude se encaixará.

3.7.1 Formas

Como se viu no início, o legislador brasileiro, seguindo a tendência dos códigos criminais anteriores, preocupou-se em estabelecer uma forma simples e genérica em seu *caput*, bem como trazendo outras sete condutas típicas, exemplificativas e equiparadas no parágrafo segundo do art. 171 do Código Penal. Veja-se a seguir.

3.7.2 Simples

Como já dito, é a forma estabelecida pelo *caput* do art. 171, o qual já foi analisado anteriormente e cuja pena-base foi estabelecida em reclusão, de 1 (um) a 5 (cinco) anos e multa.

3.7.3 Privilegiada

Prevista no parágrafo primeiro do referido artigo, estabeleceu-se que se o criminoso é primário e é de pequeno valor o prejuízo à vítima, o magistrado pode aplicar a pena conforme o disposto no art. 155, §2º, do Código Penal, que consiste na substituição da pena de reclusão pela de detenção, em razão da redução da pena de um a dois terços ou de aplicação de tão somente a pena de multa, conforme melhor entender o Magistrado, no caso concreto.

Nesse sentido, Capez (2008, p. 544) faz o seguinte comentário:

> Difere, porém, do furto privilegiado, pois neste exige-se que a coisa furtada seja de pequeno valor. No crime de estelionato, exige-se que seja pequeno o valor do prejuízo, o qual deve ser aferido no momento da consumação do crime [conforme entendimento do STF]. A jurisprudência considera como pequeno valor do prejuízo aquele que não ultrapassa um salário mínimo.

Para Mirabete e Fabbrini (2008, p. 295), "a razão da diminuição da pena é a pouca importância do fato e a reduzida periculosidade do agente".

Considera-se como primário o agente que, conforme se extrai da leitura dos arts. 63 e 64 do Código Penal, aquele que nunca cometeu um delito ou quando já se tenha transcorrido o lapso temporal de cinco anos entre a data do cumprimento ou a extinção da pena anterior e a nova infração posterior. Também enuncia o art. 64, I, do referido Código, que os crimes militares próprios e políticos não são considerados para efeitos de reincidência.

Com relação ao "pequeno valor" mencionado, segundo Prado, (2013, p. 599), "o valor do prejuízo deve ser aferido no momento em que se consumar o delito e, na tentativa, o valor do bem ou do lucro objetivado pelo agente". Além disso, com relação ao entendimento dos tribunais tendem a aplicar como parâmetro o salário mínimo vigente, o autor esclarece que se faz uma ressalva nesse assunto, uma vez que "tal valor, para um operário de baixa remuneração, é considerável e, portanto, na aferição, deve-se levar em consideração também a situação econômica da vítima".

Bitencourt (2011, p. 312) acrescenta que "a jurisprudência tem-se inclinado a beneficiar o réu quando há o ressarcimento do dano, mesmo durante a ação penal (RT 502/365)".

Prado (2013, p. 599), Noronha (1996, p. 391) e Mirabete e Fabbrini (2008, p. 295) concordam no sentido de que esse privilégio se aplica tanto quando o agente comete a conduta na forma simples do *caput* quanto nas formas especiais, estabelecidas no parágrafo segundo, em razão do início da oração "nas mesmas penas incorre...".

Encerrados os comentários, passa-se a analisar as formas equiparadas ao estelionato, estabelecidas no parágrafo segundo.

3.7.4 Equiparadas

Como já visto, as formas equiparadas ao estelionato foram estabelecidas no parágrafo segundo do art. 171 do Código Penal, atribuídas as mesmas penas e benesses que sejam cabíveis ao *caput* do referido artigo, pelos motivos já expostos. Ocorre, como mencionam Mirabete e Fabbrini (2008, p. 292-293), há também outras duas modalidades estabelecidas em legislação especial, como se verá a seguir:

a) disposição de coisa alheia como própria (inciso I);
b) alienação ou oneração fraudulenta de coisa própria (inciso II);
c) defraudação de penhor (inciso III);
d) fraude na entrega de coisa (inciso IV);
e) fraude no recebimento de indenização ou valor de seguro (inciso V);
f) fraude por meio de cheque (inciso VI);
g) comercialização proibida de café (art. 2º do Decreto-Lei n. 47, de 18 de novembro de 1966) e
h) aplicação indevida de créditos ou financiamentos governamentais ou provenientes de incentivos fiscais (art. 3º da Lei n. 7.134, de 26 de outubro de 1983).

Não serão aprofundados os estudos sobre tais modalidades, pelo fato de o escopo do presente trabalho ser a análise da possibilidade de aplicação da modalidade simples de estelionato ao fenômeno da fraude da loja virtual fantasma, e não o estudo aprofundado do crime de estelionato propriamente dito.

3.8 PENA, MAJORANTE, AÇÃO PENAL E FORO COMPETENTE

Como já visto, as penas cominadas são de reclusão, variando de um a cinco anos e multa. Caso seja o agente primário e de pequeno valor o prejuízo causado, modifica-se para a pena de reclusão, reduzindo-se a pena-base de um a dois terços, havendo a possibilidade de substituição por multa, conforme enuncia o §1º. Como bem lembra Prado (2013, p. 600), "admite-se a suspensão condicional do processo (art. 89, Lei 9.099/1995), ressalvada a hipótese de violência doméstica e familiar contra a mulher (art. 41, Lei 11.340/06)".

No §3º do art. 171 do Código Penal, o Legislador inovou, desde os últimos ordenamentos penais brasileiros, ao se preocupar em agravar a pena daquele que comete o crime

em detrimento de entidade de direito público (seja ela municipal, distrital, estadual ou federal) ou de instituto de economia popular, assistência social ou beneficiária.

Da mesma forma que o privilégio do §1º, também a presente causa de aumento de pena se aplica às modalidades equiparadas a estelionato, pelas mesmas razões para a aplicação do benefício tipificado.

Noronha (1996, p. 434), na década de 1980, assim já justificava a inovação dos legisladores:

> O fundamento da majoração inspira-se em motivos de interesse social. Refere-se o dispositivo a entidade de direito público, e, como tal, devem ser consideradas não só as pessoas jurídicas já enumeradas pelo código Civil, mas também as *autarquias* que são pessoas jurídicas de direito público. [...]. É, como dissemos, a lesão a um interesse diretamente social que determina a agravação, prejudicando a organização de serviços públicos, ou entidades cujo fim tem por objetivo a economia do povo, sua assistência ou amparo. Corresponde a agravante [sic] a maior periculosidade do agente também, que não vacilar em lesar interesses dessa ordem (grifo do autor).

E esse entendimento de Noronha foi pacificado onze anos depois pelo Superior Tribunal de Justiça, na Súmula n. 24, a qual determinou o seguinte: "aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da Previdência Social, a qualificadora do § 3º do Art. 171 do Código Penal" (BRASIL, STJ, 1991).

Como bem destaca Prado (2013, p. 600), "salta aos olhos que se assim não for *ad verbum*, transgrede-se de modo irremediável o princípio penal constitucional da legalidade dos delitos e das penas" (grifo do autor). Caso o crime seja em detrimento de qualquer outra entidade, não se aplicará a majorante em questão. Assim, se a vítima de estelionato for o Banco do Brasil, por exemplo, por se tratar de uma sociedade de economia mista e ter sido esta mencionada pelo texto da majorante, não poderá o magistrado aplicador da pena do delito em questão fazer incidir também o malefício do §3º do art. 171 do Código Penal.

A ação penal é pública incondicionada, exceto nas hipóteses trazidas pelo art. 182 do Código Penal, em que é exigida a representação.

Com relação ao foro competente, dispõe o art. 70 do Código de Processo Penal que "a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução".

Aliado a isso, o Superior Tribunal de Justiça definiu, em sua Súmula n. 48, que "compete ao juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque", o que, embora seja, aparentemente, uma disposição específica para o inciso VI do art. 171 do Código Penal, ela também é aplicada a todas as outras modalidades de estelionato na prática.

Entretanto, há situações em que mais de uma vítima é ludibriada e noticia o fato para que a Justiça desenvolva o devido processo legal, como acontece no tema de estudo do presente trabalho; havendo, assim, multiplicidade de foros competentes para o processamento da ação penal. Dessarte, o Tribunal de Justiça de Minas Gerais, um dos mais atuantes em matéria de crimes digitais, assim entendeu:

> EMENTA: APELAÇÃO CRIMINAL - ESTELIONATO - NULIDADE - INCOMPETÊNCIA DO JUÍZO - PRELIMINAR REJEITADA - VÍCIO SUPOSTAMENTE OCORRIDO NA FASE DE INQUÉRITO POLICIAL - NULIDADE - NÃO CABIMENTO - PRELIMINAR REJEITADA - DENÚNCIA FUNDAMENTADA EM PEÇAS DE INFORMAÇÃO OBTIDAS DIRETAMENTE PELO MINISTÉRIO PÚBLICO - VALIDADE - AUSÊNCIA DE INQUÉRITO POLICIAL - IRRELEVÂNCIA - INDEFERIMENTO DE DILIGÊNCIAS REQUERIDAS EM AUDIÊNCIA - CERCEAMENTO DE DEFESA - NÃO OCORRÊNCIA - ABSOLVIÇÃO PELA AUSÊNCIA DE PROVAS - IMPOSSIBILIDADE - PROVA TESTEMUNHAL EM CONSONÂNCIA COM A PROVA DOCUMENTAL E COM OS DEMAIS INDÍCIOS - SÓLIDO CONTEXTO PROBATÓRIO - LIVRE CONVENCIMENTO MOTIVADO - CONDENAÇÕES MANTIDAS - CIRCUNSTÂNCIAS JUDICIAIS DO ART. 59 DO CP - PERSONALIDADE - NECESSIDADE DE PROVA TÉCNICA PARA SUA AFERIÇÃO - REDUÇÃO DAS PENAS-BASE - PRIMEIRO RECURSO PROVIDO EM PARTE E SEGUNDO RECURSO NÃO PROVIDO.
> - Tratando-se de crimes praticados em sequência, através da internet, em diversas comarcas, o foro de qualquer delas é competente para o processamento e julgamento do feito, ficando preventa a competência do magistrado que primeiro praticar qualquer ato decisório, consoante o disposto no art. 83 do CPP; [...].(MINAS GERAIS, TJ, 2013)

Não destoa esse entendimento com relação à modalidade de estelionato em estudo no presente trabalho. Embora os delitos sejam praticados por meio da internet, a obtenção da vantagem ilícita se dá pelos depósitos em contas bancárias de pessoas físicas ou pagamento de boletos bancários cujo destino dos valores será a de uma agência de cidade específica, o que acaba por se encaixar em situação semelhante à fraude por meio do cheque, razão pela qual, a competência se dá de maneira semelhante. Mas isso será analisado mais detalhadamente no capítulo a seguir.

4 A FRAUDE DA LOJA VIRTUAL FANTASMA

Apesar de não estar legalmente regulamentada, jurisprudência e especialistas brasileiros entendem, pacificamente, com relação a sua existência. Segundo a Receita Federal, inexistência do vendedor, falta de entrega do produto, emissão de nota fiscal falsa são alguns dos exemplos mais comuns de indícios praticados (BRASIL, 2013).

Como já visto, literalmente, a fraude da loja virtual fantasma consiste num falso comércio estabelecido, geralmente, numa página da internet, de modo que será estudado, no presente trabalho, quando agentes agem, especificamente, no comércio eletrônico do tipo "*Business to Consumer*" (B2B) e "*Consumer to Consumer*"(C2C), por serem nestas modalidades onde mais ocorre a fraude em estudo no Brasil, tanto no que se refere a casos trazidos à Justiça, quanto à facilidade maior em criar uma loja virtual por essas duas espécies, aliada à informalidade da relação bilateral.

Não há como especificar uma data certa ou um termo inicial de quando essa conduta delitiva começou a ocorrer, mas é certo que ela nasceu e cresceu junto com a popularização do *e-commerce* no Brasil, em especial com a modalidade *Consumer to Consumer* (C2C), como no caso do <www.mercadolivre.com.br>.

Segundo Mercado... (2013), criado pelo argentino Marcos Galperín em 2 agosto de 1999, tendo chego ao Brasil somente em outubro do mesmo ano, o site engatinhava ainda nos seus mecanismos de fiscalização quanto à análise das contas dos usuários vendedores. Não se exigia muitos requisitos que provassem a idoneidade daqueles, tampouco limites mínimos de preços aos produtos postos à venda (principalmente pela ideia inicial de se tratar de um leilão virtual livre), sendo incalculável, dessa forma, o número de vítimas que se arriscavam a comprar sem qualquer segurança, conforme WILLY (2013).

Posterior ao surgimento dessa fraude, uma segunda modalidade criminosa desencadeou uma série de notícias nos meios de comunicação de um fenômeno que ganhou forma e endereços virtuais, a partir do final da década de 2000, qual seja, através da modalidade *Business to Consumer* (B2C). Com o aumento de denúncias sobre as fraudes praticadas pelos anúncios de ofertas fraudulentas no mercado livre e com o consequente amadurecimento da modalidade deste, bem como o aumento de meios de controle, os agentes resolveram criar suas próprias páginas fraudulentas de comércio eletrônico na internet, o que será objeto a ser estudado neste capítulo.

4.1 DEFINIÇÕES

Conforme definição do dicionário Michaelis (2010), fraude consiste no "ato ou efeito de fraudar, de modificar ou alterar um produto ou esconder a qualidade viciada deste, com o objetivo de lucro ilícito".

Assim, pode-se conceituar o tema em estudo da seguinte maneira:

> Sinteticamente o golpe envolve uma suposta venda, contra pagamento do valor integral ou de um adiantamento (se o valor for elevado). A mercadoria proposta sempre tem preço e/ou condições bem atraentes e são apresentadas muitas facilidades. A localização (ou suposta tal) sempre é longe das vítimas, para dificultar averiguações profundas. Na realidade a mercadoria não existe e nunca será entregue sendo que o objetivo dos golpistas é receber o pagamento do valor ou adiantamento e desaparecer (FRAUDES... 2013; PARODI, 2013, p. 185).

Convém mencionar que a venda fraudulenta pela internet não se confunde com a compra fraudulenta pela mesma, a qual, também é tipificada como estelionato, segundo entendimento do STJ (COMPRA..., 2013). Conforme o referido tribunal decidiu, há, igualmente, a relação bilateral consumerista existente na venda fraudulenta pela internet, mas é o consumidor quem age de má-fé, ludibriando uma loja virtual idônea, ao se utilizar de cartões e dados de terceiros.

Assim, Ramos Junior (s/d) *apud* Freitas (2013, p. 64) entendem da seguinte maneira:

> [...] comete o crime de estelionato o agente que cria página na Internet ou faz anúncios por intermédio de *sites* como o Mercado Livre, por exemplo, simulando a venda de produtos com o objetivo de induzir a vítima em erro ao efetuar o pagamento antecipado da suposta mercadoria, na ilusão de que está efetuando a sua compra e que irá recebê-la posteriormente, quando, na realidade, trata-se de golpe utilizado pelo agente para obter vantagem econômica indevida, aproveitando-se da boa-fé das pessoas para enganá-las e acarretar prejuízo ao patrimônio destas.

4.2 MODALIDADES DE FRAUDE

Diante da facilidade e da sensação de anonimato que a rede mundial de computadores proporciona aos agentes, bem como o amplo leque de modalidades delitivas que o estelionato abrange, também no tema da venda fraudulenta pela internet é possível observar diversas formas que, embora contenham, em sua essência, uma problemática que também precise ser analisada em um estudo específico, neste trabalho, será tratado apenas em linhas gerais, para fins de classificação e hermenêutica do tema central.

4.2.1 Fraude da conta falsa

Para efeito de conceito, Fraudes... (2013) e Parodi (2013, p. 184) assim enunciam:

> Conta no sistema de leilão virtual, aberta com dados e documentos falsos, ofertando mercadorias muito atrativas (como tipo e preço), com o único intuito de receber o pagamento adiantado, em uma conta também aberta com documentos falsos, prometendo o envio da mercadoria em seguida e depois sumir. Por demorar um tempo antes que o comprador/vítima se preocupe e denuncie, os golpistas tem uma vantagem e podem aplicar o golpe várias vezes antes de desaparecer. Neste caso normalmente a qualificação do golpista vendedor (ou seja a nota e o histórico que ele tem), no sistema de leilão virtual, é nula, pois as contas sempre são muito recentes.

Nesta primeira forma de fraude, ela se destaca, principalmente, dentro da modalidade de *e-commerce* "Consumidor a Consumidor" (C2C) e é um dos problemas mais comuns que sites como o <www.mercadolivre.com.br> enfrentam.

4.2.2 Fraude das páginas adulteradas

Outra forma de venda fraudulenta pela internet, Fraudes... (2013) e Parodi (2013, p. 184) explicam que são "ofertas publicadas utilizando falhas dos sistemas de leilão virtual, que fazem com que as ofertas apareçam como verdadeiras e com vendedor tendo qualificações elevadas", em razão de mais defeitos no sistema do leilão, como se fossem clones perfeitos da página da internet original. Os mesmos autores continuam, esclarecendo que, na realidade, "redirecionam a outro sistema ou a outro endereço onde é aplicado o golpe solicitando o pagamento adiantado, como sempre".

Não são raros os exemplos em leilões virtuais e também a clonagem de páginas de *internet banking* de entidades bancárias conceituadas brasileiras que, frequentemente, emitem notas públicas, anunciando a referida fraude e é nessas horas que o consumidor precisa ser muito cuidadoso em observar erros de português, endereços e telefones para contato da empresa responsável.

4.2.3 Fraude da Triangulação de pagamentos

Nessa fraude, há uma complexidade ainda maior do que na anterior. Nela, o golpista não se utiliza de contas bancárias alheias e é exatamente esse o principal motivo de ser uma fraude mais elaborada.

Nesse sentido, Fraudes... (2013) e Parodi (2013, p. 184-185) ensinam que há, resumidamente, quatro passos praticados pelos agentes nessa modalidade, quais sejam:

> A) negocia a compra de alguma mercadoria cara com alguma vítima que a esteja oferecendo, e solicita o número da conta para fazer o pagamento adiantado;
> B) oferece uma mercadoria inexistente para venda, outras vítimas respondem e ele pede para fazer o pagamento na conta que a primeira vítima forneceu;
> C) assim que for feito o pagamento solicita a entrega da mercadoria por parte da primeira vítima (normalmente com entrega no metrô ou em algum outro lugar público, sem fornecer endereço);
> D) quando as vítimas das vendas inexistentes denunciarem, a primeira vítima fica com o problema e pode acabar tendo que devolver o dinheiro e, portanto, perdendo sua mercadoria.

Nessa artimanha, muitas vezes, o agente exclui a conta em seguida de conclusa a fraude aplicada. E, aí, existe uma dificuldade imensa em identificá-lo, principalmente, porque a demora em identificar o endereço de seu computador (o *Internet Protocol* ou IP), pode resultar na perca de seus rastros, tornando prejudicado, assim, o posterior indiciamento.

4.2.4 Fraude do pagamento com fundos desviados

Nesse sentido, Fraudes... (2013) e Parodi (2013, p. 185) assim explicam:

> Fenômeno em franco crescimento em função do aumento das fraudes digitais do tipo phishing. Neste caso, hackers que invadiram contas bancárias através do roubo de senhas por meio de trojans ou sites falsos (phishing), usam este acesso ao dinheiro de terceiros para efetuar depósitos em pagamento de mercadorias (mais difíceis de serem rastreadas do que uma transferência para alguma conta deles) de particulares ou pequenas empresas. O vendedor terá depois problemas com os bancos e autoridades, sofrendo bloqueios de contas e eventuais inquéritos.

Embora não se encaixe como uma forma de venda fraudulenta pela internet e tampouco se caracterize como estelionato (mas sim como invasão de dispositivo informático), convém conceituá-lo, para que se entenda por quê ele não se encaixa na mesma classificação trazida por este estudo.

4.2.5 Fraude da loja virtual fantasma no e-commerce B2C

Nessa modalidade, os agentes, na maioria das vezes, organizados em quadrilha, montam uma loja online, com um design razoavelmente bem elaborado, o que acaba por dar a aparência de uma empresa sólida e confiável, passando a vender produtos abaixo do valor de mercado, conforme Willy (2013).

Ainda, tem-se que “muitas vezes, os golpistas simplesmente anunciam uma mercadoria aproveitando dados fictícios ou roubados, empresas laranjas ou fantasmas ou o bom nome de empresas verdadeiras”, conforme Fraudes... (2013) e Parodi (2013, p. 185), mas que nada têm a ver com o delito, trocando, os agentes, tão somente os telefones para contato.

Por vezes, há também o roubo de identidades de pessoas físicas para a consecução amda referida burla. Nesses casos, segundo o Pagseguro, as pessoas físicas se sujeito a tal risco, quando compram ou vendem a terceiros online. “O fraudador geralmente utiliza as informações obtidas para efetuar compras, conseguir linhas de crédito e fornecer referência bancária” (PAGSEGURO, 2013).

Segundo Willy (2013), “a grande sacada dos criminosos para não afugentar vítimas receosas quanto à seriedade da “loja”, é capturá-las por meio de sites bem conceituados de comparação de preços, entre os quais, Shopping UOL e Buscapé”. O autor continua, esclarecendo no sentido de que neles, a quadrilha cria diversos perfis de usuários falsos e passam a emitia boas avalições sobre a loja virtual fraudulenta no site comparador, mantendo sempre um bom conceito junto aos sites de busca.

Ainda, Fraudes... (2010) e Parodi (2013, p. 186) explicam que as mercadorias mais frequentemente propostas nesta modalidade fraudulenta são os “eletroeletrônicos (desde informática e câmeras digitais até TV de plasma e sistemas de som), remédios (sobretudo os contra disfunções sexuais ou os não autorizados no Brasil) e carros e motos (famoso o golpe do “carro fantasma”)”.

4.2.6 Fraude em suposto site de compras coletivas

Uma das fraudes mais recentes que se tem conhecimento sobre fraudes em lojas virtuais fantasmas tem ocorrido em compras coletivas, principalmente em razão do surgimento da última ser recente.

Segundo Felipini (2011, p. 2-3), uma das empresas a impulsionar o fenômeno da compra coletiva foi a chinesa <www.teambuy.com.cn>, em 2006, vindo a ser seguida pela norte-americana <www.groupon.com>, dois anos mais tarde. Mas foi justamente nos Estados Unidos, ainda conforme o referido autor, que o atual modelo de compra coletiva se firmou e passou a ser imitado pelo resto do mundo. No Brasil, inclusive, esse modelo ganhou notoriedade a partir de 2011.

O mesmo autor traz, ainda, três importantes conceitos para se entender a compra coletiva em si:

> **Sistema de compra coletiva (group buying model) –** Sistema de compra no qual um grupo de pessoas adquire um produto com desconto em razão da maior quantidade de compradores. A divulgação e a comercialização da oferta são realizadas pela internet.
> **Segmento de compra coletiva (group buying business)** – Novo segmento de negócios, no qual o empreendedor cria um site de divulgação e venda de produtos em

> oferta e atua como intermediador entre compradores e comerciantes. O modelo de negócio utilizado é o da corretagem.
> **Site de compra coletiva (group buying website)** – É a empresa que divulga e comercializa as ofertas dos anunciantes por meio da internet, entrega os cupons com desconto, recebe o pagamento e fica com um percentual do valor pago pelo comprador (FELIPINI, 2011, p. 9, grifos do autor).

Explicados os referidos conceitos, passa-se à breve análise da fraude ocorrida em sites de compra coletiva, de modo que três situações fraudulentas podem ser praticadas contra o consumidor.

A primeira delas, segundo o site Administradores (2013), trata-se de quando o consumidor compra um produto por intermédio de um site de compras coletivas, paga o preço acordado, mas nunca recebe, obtendo, como resposta da intermediadora da compra virtual, que esta não se responsabiliza pelo prejuízo sofrido. Como se não bastasse, ao tentar entrar em contato diretamente com a empresa que ofertou o produto comprado no referido site, a vítima percebe que os telefones para contato foram desativados e não obtém qualquer resposta aos seus e-mails enviados para a empresa. Não é a intermediadora quem age de má-fé, mas a suposta empresa virtual que ofereceu o produto naquela.

Outra fraude também conhecida é a entrega do produto com quantidade inferior à oferecida, quando a empresa fornecedora do produto ofertado e a empresa que intermedia as compras e vendas coletivas acordam em entregar quantidade menor para descontar no imposto devido, partilhando o lucro entre ambas e cobrando da vítima consumidora o valor inteiro do produto oferecido, conforme Ferreira (2013).

Ainda, o referido autor traz um terceiro tipo de fraude em compras coletivas, no caso de cotações diversas de um mesmo produto. Segundo ele, funciona da seguinte maneira:

> São feitas três cotações, o fornecedor A R$1000, o fornecedor B R$1200 e o fornecedor C R$1500. Seguindo esse raciocínio, as cotações são referentes a produtos idênticos, com a mesma qualidade, garantia e etc. A compra seria realizada com o fornecedor A, a única alteração seria em seu valor, no qual o valor do fornecedor A de R$1000 seria alterado R$1200 apresentados pelo fornecedor B, com a finalidade de obter descontos nos impostos. O restante ficaria com o comprador (FERREIRA, 2013).

Nesse caso, como no anterior, haveria a fraude, tendo como vítima tanto o comprador quando o fisco.

4.3 (IN)APLICABILIDADE DA PRETENSÃO PUNITIVA DOS AGENTES

Entendidas as definições, convém tratar sobre qual é o entendimento dos tribunais brasileiros com relação ao tema em estudo, uma vez que há duas correntes doutrinárias distintas sobre a tipicidade com relação à fraude da loja virtual fantasma.

Nesse sentido, Natarelli (2013) explica que a primeira corrente entende que não se deve aplicar a legislação penal em condutas criminosas cometidas através de um computador. Segundo a autora, "o primeiro argumento é baseado no princípio da reserva legal que obriga que a legislação tipifique determinado fato como criminoso, uma vez que, sem lei, não há crime (art. 1º do CPP e [art.] 5º, XXXIX da CF)".

Como segundo argumento para a primeira corrente, a autora explica que a doutrina mais tradicional entende não ser possível a analogia e a interpretação extensiva quando para prejudicar o julgamento do acusado, razão pela qual, por essa corrente, os crimes digitais, inclusive a fraude da loja virtual fantasma, seriam atípicos, sendo impossível, portanto, punir seus agentes com base na legislação penal atual.

Natarelli (2013) traz, ainda, a segunda corrente doutrinária (inclusive defendida pelos deputados Eduardo Azeredo e Paulo Teixeira, como se verá nos items seguintes, através de suas recentes leis aprovadas que serão também estudadas aqui). Nela, em contrapartida, defende-se que "a punição baseia-se [sic] no fato de que os crimes praticados pela via eletrônica são os mesmos tratados pelo Código Penal, com a peculiaridade de serem apenas versões modernas do tipo, ou seja, a modificação ocorreria apenas no *modus operandi*", o que, segundo a autora, por via de consequência, "não teria o condão de mudar o tipo penal que enseja a punição penal".

Nessa matéria, não existe ainda um entendimento dominante, razão pela qual, atualmente, necessária é a análise dos tribunais estaduais e do STJ quanto ao assunto, uma vez que, enquanto o Legislativo começa a abrir os olhos para a promulgação de leis referentes a realidades e problemáticas digitais, o Judiciário precisa dar uma resposta aos casos concretos emergentes.

Nesse sentido, o Tribunal de Justiça de Santa Catarina tem entendido pela aplicação da segunda corrente doutrinária supramencionada, senão, veja-se:

> APELAÇÃO CRIMINAL. CRIME CONTRA O PATRIMÔNIO. ESTELIONATO (ART. 171, CAPUT, DO CÓDIGO PENAL). SENTENÇA CONDENATÓRIA. RECURSO DA DEFESA.ABSOLVIÇÃO. INVIABILIDADE. MATERIALIDADE E AUTORIA DELITIVAS DEVIDAMENTE COMPROVADAS. CONTEXTO PROBATÓRIO FIRME E COERENTE APTO A DEMONSTRAR QUE O APELANTE, MEDIANTE PROMESSA DE ENTREGA DE PRODUTO OFERTADO NA INTERNET, OBTEVE VANTAGEM ILÍCITA EM PREJUÍZO ALHEIO AO NÃO EFETUAR A ENTREGA DA MERCADORIA COMPRADA PELA VÍTIMA. **RECONHECIMENTO DE MERO ILÍCITO CIVIL. IMPOSSIBILIDADE. CLARA INTENÇÃO DO APELANTE DE OBTER PARA SI VANTAGEM ILÍCITA EM PREJUÍZO ALHEIO. DOLO ESPECÍFICO EVIDENCIADO. CONDUTA PRATICADA QUE SE AMOLDA AO TIPO PENAL PREVISTO NO ART. 171, CAPUT, DO CP**. APLICAÇÃO DO PRINCÍPIO DA INSIGNIFICÂNCIA. NÃO ACOLHIMENTO. PREJUÍZO SOFRIDO PELA VÍTIMA EM VALOR SUPERIOR AO SALÁRIO-MÍNIMO VIGENTE À ÉPOCA DOS FATOS. REQUISITO OBJETIVO NÃO PREENCHIDO. MANUTENÇÃO DA

> SENTENÇA QUE SE IMPÕE. RECURSO CONHECIDO E DESPROVIDO (SANTA CATARINA, TJ, 2013c, grifo nosso).

É certo que o tribunal catarinense entende assim por uma questão de garantia da ordem pública e da credibilidade da Justiça para com o povo, uma vez que a simples inovação do *modus operandi* do estelionato (diante de toda a comprovação fática que pode haver), num caso de fraude de loja virtual fantasma, não é suficiente e tampouco razoável para que se absolva os agentes, uma vez que a sensação de impunidade os leva a quase inevitável reincidência.

Assim, também não destoa o entendimento do Tribunal de Justiça gaúcho:

> ESTELIONATO. VENDA ATRAVÉS DA INTERNET DE PROCESSADOR AVARIADO. ABSOLVIÇÃO**. Não cabe a absolvição do acusado, eis que a prova é inconteste quanto à autoria e a ocorrência do delito**. PENA. DOSIMETRIA. REDIMENSIONADA. APELO DEFENSIVO PARCIALMENTE PROVIDO. EXTINÇÃO DA PUNIBILIDADE PELA PRESCRIÇÃO DECLARADA, POR MAIORIA. (RIO GRANDE DO SUL, TJ, 2010, grifo nosso).

Em que pese neste julgado ter havido, ainda assim, a extinção da punibilidade, resta claro não ser o entendimento do referido tribunal aplicar a primeira corrente doutrinária nos casos trazidos a sua Justiça.

De igual forma, entende o Tribunal de Justiça paranaense:

> APELAÇÃO CRIMINAL. CONDENAÇÃO PELO CRIME DE ESTELIONATO. **PLEITO QUE VISA À ABSOLVIÇÃO. NÃO ACOLHIMENTO. ELEMENTOS CONSTITUTIVOS DO DELITO PLENAMENTE DEMONSTRADOS**. AGENTE QUE INDUZIU A VÍTIMA EM ERRO MEDIANTE VENDA PELA INTERNET DE PRODUTOS QUE SABIA DE ANTEMÃO NÃO PODER ENTREGÁ- LOS. CONJUNTO PROBACIONAL COESO E HARMÔNICO APONTANDO PARA A CONFIGURAÇÃO DO DELITO. SENTENÇA MANTIDA. RECURSO NÃO PROVIDO (PARANÁ, TJ, 2011, grifo nosso).

E esse entendimento não é uniforme somente no sul do país. A exemplo do Tribunal de Justiça de São Paulo, onde resta claro a posição do referido tribunal em punir os agentes que pratiquem os fatos em estudo, se provada a materialidade e a autoria delitivas no caso concreto:

> ESTELIONATO Crime praticado pela internet Venda de produto que não foi entregue - Autoria e materialidade evidenciadas Inexistência de dúvida que justifica o decreto condenatório Reparação do dano antes do recebimento da denúncia Irrelevância Crime patrimonial que se consuma com a obtenção da vantagem indevida **Atipicidade da conduta e ausência de dolo afastados** Inaplicabilidade da Súmula 554 do STF Sentença mantida Art. 252 do RITJSP PENA - Réu tecnicamente primário Súmula 444 do STJ Redução ao mínimo legal Arrependimento posterior do art. 16 do CP mantido - Privilégio do §1º do art. 171 do CP afastado Valor do bem - Substituição por pena de multa adequado ao caso Regime aberto adequado - Recurso parcialmente provido (SÃO PAULO, TJ, 2013, grifo nosso).

Infelizmente, é somente pela representação desses cinco tribunais de justiça que se pode visualizar a realidade brasileira, uma vez que, em que pese a consulta realizada em todos os vinte e sete tribunais de justiça deste país para a realização deste trabalho, percebeu-se que somente nos tribunais do sul e sudeste se viu casos da fraude em estudo levadas ao reexame em

segundo grau, em função da melhor estrutura e maior experiência com crimes cibernéticos que esses entes federados ainda detém (o que faz com que mais processos sejam finalizados com condenações concretas, evitando-se a prescrição pela falta de destreza dos operadores em investigá-los).

Mas esse cenário tende a mudar, com as reformas trazidas pela Lei n. 12.735/12, que será estudada adiante.

4.4 ALTERAÇÕES TRAZIDAS PELA LEI Nº 12.735/12

Após trezes anos sendo discutida pelo Congresso Nacional, essa lei foi sancionada no mesmo dia que a Lei n. 12.737/12, oriunda do Projeto de Lei n. 84/99, de autoria do deputado Eduardo Azeredo, cujo sobrenome batizou a lei sancionada.

Através dessa lei, foi possível alterar os Códigos Penal e Penal Militar, bem como a Lei n. 7.716/89, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, bem como a determinação de que "os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado" (BRASIL, Lei n. 12.735/12, 2013).

Com isso, garantiu-se o início de um suporte legal para o incentivo ao desenvolvimento de aplicadores do Direito melhor preparados para a era digital e mais capacitados para investigar delitos informáticos, sem que estes acabem prescritos quando conclusas as investigações e remetidas ao Poder Judiciário, como é a triste realidade da maioria dos inquéritos policiais que se tem até hoje sobre esses crimes.

4.5 ALTERAÇÕES TRAZIDAS PELA LEI Nº 12.737/12

Popularmente conhecida como "Lei Carolina Dieckmann" – em razão do nome da atriz que teve seu computador invadido e, a partir dele, divulgadas fotos íntimas suas –, essa lei foi sancionada em 30 de novembro de 2012 e é proveniente do Projeto de Lei n. 2.793/11, de autoria do deputado Paulo Teixeira.

Essa lei também altera o Código Penal, dispondo sobre, entre outras providências, a criação do delito de invasão de dispositivo informático, qual seja:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de

> obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, Lei n. 12.737/12, 2013).

Segundo o autor do projeto de lei que levou à criação da referida, Paulo Teixeira, essa nova legislação foi responsável pela punição para crimes nos casos de roubos de senhas bancárias e pela defesa de cidadãos que compram pela internet, mas que nunca recebem os produtos (LEI..., 2013).

Ocorre que, em que pese as declarações do autor da referida lei e que, embora ela seja extremamente relevante para o ordenamento jurídico brasileiro, a tipificação do delito de invasão de dispositivo informático em nada acrescenta no que toca à proteção jurídica necessária e cabível às fraudes de loja virtual fantasma. Pelas razões que se verá a seguir.

Segundo Prado, no crime de invasão de dispositivo informático, o bem jurídico tutelado, diferentemente do estelionato, é a liberdade individual, e não o patrimônio da vítima, especificamente, "a privacidade no tocante a dados e informações, de cunho pessoal ou profissional, contidas em dispositivo informático, cuja segurança deve ser de alguma forma quebrada sem a autorização do titular" (2013, p. 407).

Assim, como se viu nas formas de fraudes da loja virtual fantasma, não há qualquer tipo de invasão de dispositivo informático, embora ambos crimes se utilizem da informática para a consecução de seus tipos penais.

Também não há qualquer tipo de instalação de vulnerabilidades (como vírus, por exemplo) no computador da vítima que compra um produto pela internet e que nunca o recebe. O agente cria o site aparentemente idôneo e espera até que vítimas acessem e depositem os valores

na conta definida no site, sem nunca receber, outrossim, o produto comprado, razão pela qual, os dois crimes não se confundem.

4.6 ALTERAÇÕES TRAZIDAS PELO DECRETO Nº 7.962/13

Preocupada com o crescimento do comércio eletrônico nos últimos anos e as consequências jurídicas que ele tem trazido consigo, a presidenta Dilma Rousseff, no dia mundial de direitos do consumidor (15 de março) deste ano, lançou um pacote de medidas destinadas a proteger o consumidor, bem como garantiu maior autonomia aos Procons. Esse programa ficou conhecido como "Plandec" (Plano Nacional de Consumo e Cidadania) e, dentre as suas medidas, incluiu a instituição do Decreto n. 7.962, datado de mesma data.

Com ele, foi possível antecipar parte da atualização do Código de Defesa do Consumidor que ainda está em discussão desde 2012 e que veremos no item seguinte, e foi fundamental para regulamentar a contratação no comércio eletrônico, sob o ponto de vista do consumidor.

Já em seu art. 1º, o referido decreto mostra a preocupação do legislador em regulamentar o Código de Defesa do Consumidor (Lei n. 8.078/90), no que se refere à contratação no comércio eletrônico, abrangendo os aspectos seguintes: "I – informações claras a respeito do produto, serviço e do fornecedor; II – atendimento facilitado ao consumidor; e III – respeito ao direito de arrependimento" (BRASIL, Decreto n. 7.962/13, 2013). E é justamente no inciso I do referido artigo que se vê o primeiro indício de que o legislador quis estabelecer um conjunto mínimo de dados disponíveis ao consumidor na página de comércio virtual para se evitar fraudes como as do estudo deste trabalho.

Tanto é, que os arts. 2º e 3º, do mesmo diploma legal, destinaram-se, exclusivamente, a estabelecer informações que devem estar presentes em local "de destaque e de fácil visualização", no que concerne a sítios de comércio eletrônico ou de ofertas de compras coletivas, bem como demais meios utilizados para a oferta ou conclusão de contrato de consumo.

Nesse sentido, convém enunciá-las aqui, no que concerne aos sítios de comércio eletrônico, disposto no art. 2º:

> I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;
> II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;
> III - características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;

> IV - discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;
> V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e
> VI - informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta (BRASIL, Decreto n. 7.962, 2013).

Ainda, além das anteriormente mencionadas, quando se tratar de compras coletivas, no site que fizer as ofertas, deverá conter mais três elementares, dispostas no art. 3º:

> I - quantidade mínima de consumidores para a efetivação do contrato;
> II - prazo para utilização da oferta pelo consumidor; e
> III - identificação do fornecedor responsável pelo sítio eletrônico e do fornecedor do produto ou serviço ofertado, nos termos dos incisos I e II do art. 2º (BRASIL, Decreto n. 7.962, 2013).

Com essas disposições, o legislador mostrou claro esforço em combater as fraudes de loja virtuais mais grosseiras, ou seja, aquelas em que não há a utilização indevida de dados de pessoas físicas e jurídicas inocentes nas informações sobre a suposta empresa virtual.

Também merece destaque o inciso IV do art. 4º do mesmo ordenamento jurídico, com relação ao dever do fornecedor em dar toda a assistência que o consumidor precisar para resolver eventuais problemas decorrentes de atendimento ou do produto:

> manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato; [...] (BRASIL, Decreto n. 7.962/13, 2013).

Não obstante, ainda precavendo-se para evitar mais fraudes e informar o consumidor, a fim de que ele não seja mais uma vítima de estelionato, o legislador estabeleceu o seguinte no art. 6º do mesmo diploma: “as contratações no comércio eletrônico deverão observar o cumprimento das condições da oferta, com a entrega dos produtos e serviços contratados, observados prazos, quantidade, qualidade e adequação" (BRASIL, Decreto n. 7.962/13, 2013).

E é justamente em razão dessa introdução legislativa que o Legislador estabeleceu a possibilidade de aplicação das sanções administrativas já previstas no art. 56 do Código de Defesa do Consumidor, quais sejam:

> Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:
> I - multa;
> II - apreensão do produto;
> III - inutilização do produto;
> IV - cassação do registro do produto junto ao órgão competente;
> V - proibição de fabricação do produto;
> VI - suspensão de fornecimento de produtos ou serviço;
> VII - suspensão temporária de atividade;
> VIII - revogação de concessão ou permissão de uso;
> IX - cassação de licença do estabelecimento ou de atividade;
> X - interdição, total ou parcial, de estabelecimento, de obra ou de atividade;
> XI - intervenção administrativa;

> XII - imposição de contrapropaganda.
> Parágrafo único. As sanções previstas neste artigo serão aplicadas pela autoridade administrativa, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo (BRASIL, Lei n. 8.078/90, 2013).

Pela interpretação analógica do artigo supramencionado, é certo que, no caso da fraude da loja virtual fantasma, uma medida cabível seria a retirada da página da internet de circulação, mediante determinação judicial ao provedor responsável pelo domínio.

Por fim, no art. 9º do Decreto n. 7.962/13, estabeleceu-se o prazo de sessenta dias para que os comércios virtuais se adequem a essas regras, com a consequente entrada em vigor desse diploma legal.

É bem verdade que, em que pese a crítica nos veículos de comunicação à época da promulgação desse decreto sobre a excessiva abordagem no que se refere ao comércio eletrônico, convém ressaltar a extrema importância que isso serviu tanto para o consumidor como para a legislação brasileira, uma vez que, dessa forma, positivou-se a intenção de equiparar a prática do comércio virtual com os direitos e deveres que um comércio físico deve atender, como já se entendia com relação à equiparação ao crime de Estelionato para as fraudes que ocorrerem também no mundo comercial virtual.

4.7 POSSIBILIDADE DE MUDANÇAS COM O PROJETO DE REFORMA DO CDC

Desde o ano de 2012, o Senado discute um Projeto de Lei que prevê a reforma da Lei n. 8.078/90, diga-se o Código de Defesa do Consumidor, reforma essa parcialmente antecipada com a aprovação do Decreto n. 7.962/13 (ante à urgência do tratamento jurídico do comércio eletrônico).

Nele, entre outras modificações relevantes, caso aprovado, acrescentará um décimo terceiro inciso no art. 56 do referido Código, com a seguinte redação: "XIII – suspensão temporária ou proibição de oferta e de comércio eletrônico" (vide ANEXO B).

Não obstante, cientes de que essa medida administrativa pode não ser suficiente, também acrescentam um quarto parágrafo ao art. 59 do referido diploma legal, que disporá, caso aprovado o projeto:

> § 4º Caso o fornecedor por meio eletrônico ou similar descumpra a pena de suspensão ou de proibição de oferta e de comércio eletrônico, sem prejuízo de outras medidas administrativas ou judiciais de prevenção de danos, o Poder Judiciário determinará, a pedido da autoridade administrativa ou do Ministério Público, no limite estritamente necessário para a garantia da efetividade da sanção, que os prestadores de serviços financeiros e de pagamento utilizados pelo fornecedor, de forma alternativa ou conjunta, sob pena de pagamento de multa diária:

> I - suspendam os pagamentos e transferências financeiras para o fornecedor de comércio eletrônico;
> II - bloqueiem as contas bancárias do fornecedor (vide ANEXO B).

Se essa reforma se concretizar, uma das maiores deficiências dos Procons vai ser sanada, uma vez que, ao invés de apenas emitir listas anuais de sites de lojas virtuais fantasmas, poderá o órgão administrativo também requerer ao Juiz a devida suspensão ou proibição de oferta e de comércio eletrônico, dando maior efetividade a sua função fiscalizadora.

4.8 POSSIBILIDADE DE MUDANÇAS COM O PROJETO DO MARCO CIVIL

Lançado em 2009, outro projeto ainda em discussão no Congresso Nacional é o Projeto de Lei n. 2.126/2011, chamado "Marco Civil da Internet", que também foi apelidado como a "Constituição da Internet" (MARCO..., 2013), em razão de seu conteúdo estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, bem como determinando diretrizes para a atuação dos Entes Federativos em relação à matéria.

Tamanha foi a preocupação do Legislador com o tema, que se manteve espaço aberto para que os internautas brasileiros discutissem, juntamente com o Congresso Nacional, o tema em um blog mantido pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa (vide item "11" do ANEXO B), bem como através do aplicativo "Marco Civil" disponível para *download* em *smartphones* e *tablets*, a fim de que pudessem tomar conhecimento do que se trata o projeto e interagir.

Se aprovado, as principais novidades e mais relevantes para o tema em estudo neste trabalho são referentes ao armazenamento dos registros de conexão, conforme dispõe o art. 11 do referido projeto:

> Art. 11. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa poderá requerer cautelarmente a guarda de registros de conexão por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido impetrado no prazo previsto no § 3º (BRASIL, Projeto de Lei n. 2.126/2011, 2013).

Antes disso, o Legislador procurou conceituar as novas terminologias que pretende trazer no próprio projeto de lei referido. Em seu art. 4º, III, assim conceituou como administrador de sistema autônomo:

> Administrador de sistema autônomo - pessoa física ou jurídica que administra blocos de endereço Internet Protocol – IP - específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País (BRASIL, Projeto de Lei n. 2.126/2011, 2013).

Não obstante, acrescentou, ainda, no art. 4º, IV, que se entende por registro de conexão o "conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço de IP utilizado pelo terminal para o envio e recebimento de pacote de dados" (BRASIL, Projeto de Lei n. 2.126/2011, 2013).

Isso seria um passo fundamental para a preservação probatória, em matéria de crimes praticados na esfera digital, uma vez que, atualmente, muitos inquéritos policiais não conseguem apontar uma autoria para o crime de venda fraudulenta pela internet, por exemplo, em razão de os provedores de conexão se mostrar neutros em relação ao armazenamento de dados, quando muito, armazenando por um curto período de tempo, não superior a seis meses, como no caso da Microsoft, com relação aos endereços de IP que acessam o seus serviços de buscador, através da ferramenta Bing (IDG NEWS SERVICE, 2013), mas que constantemente cria óbices para o fornecimento dos dados à justiça, solicitando o envio de cartas rogatórias para a central norte-americana, atrasando e prejudicando a instrução criminal.

Outrossim, essa questão ainda é muito discutida, uma vez que há quem entenda que essa medida seja ineficaz, como Renato Ópice Blum, uma vez que não obriga também os provedores de conteúdo (donos dos sítios) a guardarem seus registros de acesso dos usuários aos sites e aos aplicativos (MARCO..., 2013), constando no projeto, atualmente, apenas como facultativo.

Ainda, em razão disso, no mesmo projeto de lei, poderá ser requerida uma nova espécie de quebra de sigilo de dados informáticos, como se fosse um "grampo" telemático, com relação aos registros de conexão, conforme os §§ 2º e 3º do art. 13:

> § 2º Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na Seção IV deste Capítulo.
> § 3º Observado o disposto no § 2º, a autoridade policial ou administrativa poderá requerer cautelarmente a guarda dos registros de aplicações de Internet, observados o procedimento e os prazos previstos nos §§ 3ºe 4º do art. 11 (BRASIL, Projeto de Lei nº 2.126/2011, 2013).

E não é só. Também a parte interessada poderá requerer ao juiz essa quebra de sigilo, seja em caráter autônomo ou no curso do processo, seja em ação civil (de reparação de danos pela venda fraudulenta pela internet, por exemplo) ou em ação penal (como no caso do estelionato digital em e-commerce). Isso é o que dispõe o art. 17:

> Art. 17. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet (BRASIL, Projeto de Lei nº 2.126/2011, 2013).

4.9 POSSIBILIDADE DE MUDANÇAS POR ACORDOS DE COOPERAÇÃO INTERNACIONAL

Até o momento, não se tem notícia na jurisprudência sobre fatos criminosos referentes ao tema em estudo com atos realizados fora do país. Ainda assim, o Deputado Federal e autor da Lei n. 12.735/12, Eduardo Azeredo, assevera para a importância de que o Brasil se preocupe em firmar acordos de cooperação internacional para que se efetive um mais acirrado combate aos crimes que não respeitem fronteiras. Segundo o autor, "é urgente a adesão do Brasil à Convenção Internacional contra o Cibercrime (Convenção de Budapeste) para termos uma legislação mais eficaz" (AZEREDO, 2013).

E com razão o autor entende. No que se refere ao tema em estudo, um dispositivo contido no referido acordo internacional seria de grande relevância para a abordagem do tema em estudo:

> **Artigo 7º - Falsidade informática**
> Cada parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e legítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não diretamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal [sic] (vide ANEXO C, grifo do autor).

Caso o país aderisse à referida Convenção, ter-se-ia maior influência internacional para o aperfeiçoamento da estrutura necessária para a apuração de crimes como a fraude da loja virtual fantasma, principalmente quando esse atingisse outros países, como é provável que já aconteça, em que pese a inexistência de julgados nesse sentido nos Tribunais Regionais Federais Brasileiros.

5 CONCLUSÃO

Como se vê nos exemplos diários, seja entre pessoas, seja em comércios físicos, o crime de estelionato não é mais exclusivo aos primeiros, uma vez que, como a sociedade evoluiu, também o crime assim o fez, ganhando novos modos de fazer, que ultrapassam limites físicos e não necessitam de liames geográficos muito além do que o depósito em uma conta bancária para se provar a obtenção da vantagem ilícita pelo agente criminoso que se utilizou da internet para enganar sua vítima.

É preocupante a estimativa de prejuízos causados por aqueles que se escondem por trás de páginas da internet para lucrar ilicitamente com o consumismo virtual alheio. Além disso, em que pese o susto que causem os números já trazidos na Introdução deste trabalho, muito pouco ainda se escreve no Direito Brasileiro, em inversa proporção ao número de vítimas que os noticiários apresentam. No pouco que se escreve, duas teorias digladiam espaço nas mãos do doutrinador brasileiro. Uma, fecha os olhos para a realidade e nega a aplicação da lei já existente, como se ainda faltassem elementos para caracterizar o crime de estelionato. A outra, mais flexível, estende a palma punitiva para aqueles que se aproveitam do anonimato que uma loja virtual lhe garante para ludibriar inocentes. E é disso que surge a necessidade de aprofundar o tema.

Com a finalidade de estudar a possibilidade da aplicação da lei penal já existente sobre essa nova modalidade de estelionato, utilizou-se da doutrina e da jurisprudência para se chegar à resposta se seria possível aplicar o Código Penal vigente nessa modalidade de fraude virtual, ante ao argumento de que o tipo penal do estelionato parece muito genérico para alguns doutrinadores e o tema ainda é debatido no que se refere à tipicidade.

Durante os dois anos de pesquisa documental que levaram à conclusão deste trabalho, viu-se que o próprio legislador, em anteprojetos de reforma ao Código Penal Brasileiro, em 2011, chegou a propor uma modalidade específica de estelionato digital, mas essa redação foi suprimida, em claro entendimento de que não haveria necessidade para um novo tipo penal específico que já se encaixa no genérico *caput* do art. 171 do referido diploma legal. Na dificuldade de encontrar a fonte oficial, decidiu-se por só comentar essa informação na conclusão, uma vez que o atual projeto de lei de reforma do Código Penal em nada inovou para o tema em estudo.

Em que pesasse um dos entendimentos de que seria esse um fato atípico, no decorrer da elaboração desta obra, chegou-se à conclusão de que seria perfeitamente típico, inovando, tão somente, no modo de agir criminoso, como se verá na conclusão a seguir.

Utilizando-se de ensinamentos de expertos em *e-commerce*, como Efraim Turban e David King, bem como os clássicos do Direito Penal, como Edgard de Magalhães Noronha e Heleno Cláudio Fragoso, trazendo ainda, o olhar contemporâneo de Luiz Regis Prado e de Fernando Capez, procurou-se entender como o estelionato virtual no *e-commerce* surge.

Mas esse entendimento ainda não era suficiente para responder ao questionamento inicial. Para tanto, foi preciso conhecer o que ensinavam outros especialistas em fraudes, como Talita Vanessa Penariol Natarelli e Lorenzo Parodi, para se entender o que diziam as correntes doutrinárias e o porquê de não se encaixar a atipicidade, ante às modalidades de fraudes existentes.

Após esse estudo detalhado, restou clara a resposta ao questionamento proposto inicialmente neste trabalho: é possível aplicar a lei penal já existente à fraude da loja virtual fantasma como forma de estelionato, porque essa burla em nada fere a tipicidade do fato delituoso estudado.

Isso porque, como foi abordado no terceiro capítulo, ainda que uma das correntes doutrinárias entendesse ser esse um fato atípico, impassível, portanto, de punição Estatal, em pesquisa a todos os Tribunais de Justiça brasileiros, chegou-se à conclusão de que é pacífico o entendimento jurisprudencial de que não há nada que impeça a aplicação do tipo penal do Estelionato ao caso em estudo, seja pela inteligência do legislador ao elaborar um *caput* capaz de abarcar uma infinidade de condutas criminosas (não ferindo, assim, o princípio da taxatividade da lei penal), seja por entenderem ser a venda fraudulenta praticada pela internet apenas um modo mais atual de se praticar o crime, sendo perfeitamente possível serem punidos os agentes com as palavras da vítima e o seu histórico de e-mails trocados com os criminosos.

Assim, concluiu-se de forma positiva ao questionamento proposto, mas esse é somento um esboço, a ponta do *iceberg* que é o mundo criminoso virtual. Ainda há muito o que se aprofundar no tema e, sem dúvida, o Direito e a Justiça esperam de braços abertos por novas dúvidas e outros pontos de vista jurídicos..

REFERÊNCIAS

ADMINISTRADORES. **Consumidores protestam contra suposta fraude envolvendo site de compras coletivas:** Cerca de 300 clientes adquiriram um produto há quatro meses que nunca foi entregue; situação acende debate sobre segurança e prudência no e-commerce. Notícia publicada em 4 jan. 2012. Disponível em: <http://www.administradores.com.br/noticias/tecnologia/consumidores-protestam-contra-suposta-fraude-envolvendo-site-de-compras-coletivas/51143/>. Acesso em: 1 maio 2013.

ALBERTIN, Alberto Luiz. **Comércio eletrônico**: modelo, aspectos e contribuições de sua aplicação. 6. ed. São Paulo: Atlas, 2010.

ALDRICH, Michael. **Acknowledgements**. 2011. Disponível em: <http://www.aldricharchive.com/acknowledgements.html>. Acesso em: 08 jan. 2013a.

_____. **History of online shopping**. 2011. Disponível em: <http://www.aldricharchive.com/shopping_history.html>. Acesso em: 14 jan. 2013b.

ARTIFÍCIO. In: MICHAELIS. São Paulo: Melhoramentos. Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=artif%EDcio&CP=18764&typeToSearchRadio=exactly&pagRadio=50>. Acesso em: 20 fev. 2013.

AZEREDO, Eduardo. **Legislação carolina dieckmann na verdade são duas leis distintas e complementares**. Artigo publicado no jornal Estado de Minas do sábado, 13 de abril. Disponível em: <http://blogdoazeredo.wordpress.com/2013/04/16/nova-legislacao-de-crimes-digitais/>. Acesso em: 17 abr. 2013.

BITENCOURT, Cezar Roberto. **Tratado de direito penal, 3**: parte especial. 7.ed. São Paulo: Saraiva, 2011.

BRASIL. Câmara dos Deputados. Projeto de lei nº 2.126, de 2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>**.** Acesso em 21 abr. 2013.

_____. Código Criminal. **Manda executar o Código Criminal.** Lei de 16 de dezembro de 1830. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LIM/LIM-16-12-1830.htm>. Acesso em: 11 fev. 2013.

_____. Código Penal. **Promulga o Código Penal.** DECRETO N. 847 – DE 11 DE OUTUBRO DE 1890. Disponível em: <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=66049>. Acesso em: 11 fev. 2013.

_____. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro, RJ. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 8 fev. 2013.

_____. Decreto nº 7.962, de 15 de março de 2013. **Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico**. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em 21 abr. 2013.

_____. Lei nº 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**. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em 21 abr. 2013.

_____. Lei n. 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 21 abr. 2013.

_____. Receita Federal. **Alerta:** Fraudes e Ilicitudes no Comércio Eletrônico. Disponível em: <http://www.receita.fazenda.gov.br/aduana/FraudesIlicitudes.htm>. Acesso em: 17 abr. 2013.

_____. Senado Federal. Projeto de lei do Senado nº 281, de 2012. Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=112481&tp=1>**.** Acesso em 21 abr. 2013.

_____. Superior Tribunal de Justiça. Súmula n. 24. Aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da Previdência Social, a qualificadora do §3º do Art. 171 do Código Penal. In: PINTO, Antônio Luiz Toledo; WINDT, Márcia Cristina Vaz dos Santos; CÉSPEDES, Lívia. Vade mecum saraiva. 11.ed. atual. ampl. São Paulo: Saraiva, 2011, p. 1909.

CALDAS, Sergio Tulio. A dianteira brasileira: ainda há muito a ser feito no e-gov nacional, mas o país já lidera rankings internacionais e tem esforço reconhecido pela ONU. **Revista CGI.BR**, n. 2, 2010. Disponível em: <http://www.cgi.br/publicacoes/revista/edicao02/txt.htm>. Acesso em: 26 jan. 2013.

CANEDO, Mônica Maria Leal; ALMEIDA, Adiel Teixeira de. **Governo eletrônico:** abordagem multicritério para a priorização de projetos G2C em organizações de meio ambiente. XXVIII ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO Rio de Janeiro, RJ, Brasil, 13 a 16 de outubro de 2008. Disponível em: <http://www.abepro.org.br/biblioteca/enegep2008_TN_STO_074_525_11425.pdf>. Acesso em: 21 jan. 2013.

CAPEZ, Fernando. **Curso de direito penal**: parte especial: dos crimes contra a pessoa a dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212). 8.ed. de acordo com a Lei n. 11.464/2007. São Paulo: Saraiva, 2008. v. 2.

COMPRA fraudulenta pela internet deve ser julgada pela justiça do local do crime. **Coordenadoria de Radio do STJ**. Notícia publicada em 8 de maio de 2009. Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=448&tmp.texto=91914&tmp.area_anterior=44&tmp.argumento_pesquisa=compra%20fraudulenta%20pela%20internet>. Acesso em: 25 mar. 2013.

CONFIRA os números do e-commerce brasileiro na 27ª edição do relatório WebShoppers **Revista E-commerce Brasil: excelência em e-commerce**. Notícia publicada em 21 mar. 2013.. Disponível em: <http://www.ecommercebrasil.com.br/noticias/confira-os-numeros-do-e-commerce-brasileiro-na-27a-edicao-do-relatorio-webshoppers/>. Acesso em: 21 maio 2013.

CONVENÇÃO sobre o cibercrime Budapeste. Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 1 maio 2013.

CRESCEM tentativas de fraude no comércio eletrônico Supermercado moderno. Notícia publicada em 22 nov. 2012. Disponível em: <http://www2.sm.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=19286&sid=5>. Acesso em: 21 maio 2013.

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

FERREIRA, Felipe. **Cuidado com fraudes em compra coletiva.**Notícia publicada em 11 mar. 2011.. Disponível em: <http://www.artigosenoticias.com.br/internet/e-commerce/cuidado-com-fraudes-em-compra-coletiva>. Acesso em: 1 maio 2013.

FELIPINI, Dailton. **Conheça um pouco da história do e-commerce [infográfico]**. E-Commerce News. Disponível em: <http://ecommercenews.com.br/noticias/balancos/conheca-um-pouco-da-historia-do-e-commerce-infografico>. Acesso em: 06 jan. 2013.

_____. **Compra coletiva:** um guia para o comprador, o comerciante e o empreendedor. Rio de Janeiro: Brasport, 2011. Disponível em: <http://books.google.com.br/books?hl=en&lr=&id=08om5JdDt_IC&oi=fnd&pg=PA1&dq=compras+coletivas+%2B+fraude&ots=jv0iJ-1h5O&sig=iW9PMLuzuEOdqYWNdkj1Rq6kPg4#v=onepage&q=fraude&f=false>. Acesso em: 1 maio 2013.

FRAGOSO, Heleno Cláudio. **Lições de direito penal**: parte geral. 17.ed. rev. e atual. Rio de Janeiro: Forense, 2006.

FRAUDE. In: MICHAELIS. São Paulo: Melhoramentos. Disponível em: < http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=fraude>. Acesso em: 19 abr. 2013.

FRAUDES diversas e tecnológicas: golpes nos sites de vendas, anúncios e leilões virtuais. Disponível em: <http://www.fraudes.org/showpage1.asp?pg=74>. Acesso em: 7 maio 2013.

FREITAS, Riany Alves de. Segurança digital. **Mpmg Jurídico**: Informações variadas, Minas Gerais, v. 17, n. , p.63-65. Julho, Agosto e Setembro de 2009. Disponível em:

<https://aplicacao.mp.mg.gov.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3>. Acesso em: 17 abr. 2013.

GRUPO B2W. **Marcas.** Disponível em: <http://www.b2winc.com/institucional/marcas>. Acesso em: 08 jan. 2013.

GRUPO MERCADO LIVRE. **Sobre mercado livre.** Disponível em: <http://www.mercadolivre.com.br/institucional>. Acesso em: 08 jan. 2013.

HUNGRIA, Nélson; FRAGOSO, Heleno Cláudio. **Comentários ao código penal**, volume VII: arts. 155 a 196. 4.ed. Rio de Janeiro: Forense, 1980.

IDG NEWS SERVICE. **Microsoft vai reduzir tempo de armazenamento de dados do Bing:** Prazo para guardar endereços IP do buscador cairá de 18 meses para seis meses, atendendo a demandas de privacidade da União Europeia.. Notícia publicada em 19 jan. 2010. Disponível em: <http://idgnow.uol.com.br/internet/2010/01/19/microsoft-vai-reduzir-tempo-de-armazenamento-de-dados-do-bing/>. Acesso em: 1 maio 2013.

Induzir. In: MICHAELIS. São Paulo: Melhoramentos. Disponível em: < http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=induzir&CP=92789&typeToSearchRadio=exactly&pagRadio=50> Acesso em: 25 fev. 2013.

ITÁLIA. **Dei delitti contro il patrimonio:** Codice penale , Libro II, Titolo XIII, agg. al 07.12.2012**.** Disponível em: <http://www.altalex.com/index.php?idnot=36775>. Acesso em: 20 fev. 2013.

JESUS, Damásio de. **Código penal anotado**. 19.ed.rev., atual. e ampl. São Paulo: Saraiva, 2009.

KHALIFA, Mohamed; WALLS, Joseph. Construindo as aplicações e a infra-estrutura do comércio eletrônico. In: TURBAN, Efraim; KING, David. **Comércio eletrônico**: estratégia e gestão. São Paulo: Prentice Hall, 2004. cap. 12, p. 1-23. Disponível em <http://wps.prenhall.com/wps/media/objects/1159/1187029/cap12.zip>. Acesso em 17 jan. 2013.

LEI carolina dieckmann sobre crimes virtuais entra em vigor nesta terça. Notícia publicada em 2 abr. 2013. Disponível em: <http://tecnologia.terra.com.br/internet/lei-carolina-dieckmann-sobre-crimes-virtuais-entra-em-vigor-nesta-terca,ef90009a79acd310VgnVCM10000098cceb0aRCRD.html>. Acesso em: 21 abr. 2013.

MACHADO, Jonathan D. Como foi criada a internet: descubra como projetos militares e científicos formaram a maior rede pública de computadores do mundo. **Tecmundo**, Curitiba, 13 ago. 2012. Disponível em: <http://www.tecmundo.com.br/internet/28279-como-foi-criada-a-internet.htm>. Acesso em: 12 mar. 2013.

MARCO civil: conheça as propostas do projeto de lei considerado a "Constituição" da internet. Notícia publicada em 13 nov. 2012. Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2012/11/13/marco-civil-conheca-as-propostas-do-projeto-de-lei-considerado-a-constituicao-da-internet.htm>. Acesso em: 7 maio 2013.

MERCADO livre: onde você encontra de tudo. Artigo publicado em 27 de abril de 2007. Disponível em: <http://mundodasmarcas.blogspot.com.br/2007/04/mercadolivre-onde-voc-encontra-de-tudo.html>. Acesso em: 7 maio 2013.

MINAS GERAIS. Tribunal de Justiça. **Apelação Criminal n. 1.0024.10.059960-4/001**. Comarca de Belo Horizonte. Primeira Câmara Criminal. Rel. Des. Alberto Deodato Neto. Julgado em 28 ago. 2012. Publicado em 12 set. 2012. Disponível em: < http://www5.tjmg.jus.br/jurisprudencia/pesquisaPalavrasEspelhoAcordao.do?&numeroRegistro=2&totalLinhas=11&paginaNumero=2&linhasPorPagina=1&palavras=estelionato%20E%20internet&pesquisarPor=ementa&pesquisaTesauro=true&orderByData=1&referenciaLegislativa=Clique%20na%20lupa%20para%20pesquisar%20as%20refer%EAncias%20cadastradas...&pesquisaPalavras=Pesquisar&>. Acesso em: 20 abr. 2013.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. **Manual de direito penal, volume 2:** parte especial, arts. 121 a 234 do CP. 25.ed.rev. e atual. até 31 de dezembro de 2006.São Paulo: Atlas, 2008.

NATARELLI, Talita Vanessa Penariol. **Ocorrência de delitos no comércio eletrônico:** quais os reais inimigos na era da informação?. Âmbito Jurídico: o seu portal jurídico da internet. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10275&revista_caderno=8>. Acesso em: 21 abr. 2013.

NORONHA, Edgard de Magalhães. **Direito penal**. 28.ed. rev. e atual. v.2. São Paulo: Saraiva, 1996.

NORRIS, Grant, et al. **E-business e erp**: transformando as organizações. Rio de Janeiro: Qualitymark, 2001.

NUCCI, Guilherme de Souza. **Código penal comentado**. 9.ed.rev.atual. e ampl. São Paulo: Revista dos Tribunais, 2008.

NUNES, Rodolfo Mondrigais Strauss; VENDRAMETTO, Oduvaldo. **Os negócios eletrônicos como instrumento de aperfeiçoamento entre redes de organizações**: um estudo sobre o portal de compras do governo federal brasileiro. Simpois Anais 2009. Disponível em: <http://www.simpoi.fgvsp.br/arquivo/2009/artigos/E2009_T00388_PCN14015.pdf>. Acesso em: 27 mar. 2013.

Obter. In: MICHAELIS. São Paulo: Melhoramentos. Disponível em: < http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=obter>. Acesso em: 25 fev. 2013.

PAOLIELLO, Cláudio de Mello; FURTADO, Antonio Luz. **Sistemas de informação para comércio eletrônico.** PUC-RioInf.MCC27/04 Julho, 2004. Disponível em: <ftp://ftp.inf.puc-rio.br/pub/docs/techreports/04_27_paoliello.pdf>. Acesso em: 08 jan. 2013.

PAGSEGURO. **Proteção contra fraudes.** Disponível em: <https://pagseguro.uol.com.br/para_voce/protecao_contra_fraudes.jhtml#rmcl>. Acesso em: 1 maio 2013.

PARANÁ. Tribunal de Justiça. **Apelação Criminal n. 748706-5.** Comarca de Foz do Iguaçu. Quarta Câmara Criminal. Rel. Des. Luiz Zarpelon. Julgado em 26 maio 2011. Publicado no DJ n. 653, em 15 jun. 2011. Disponível em: <http://portal.tjpr.jus.br/jurisprudencia/publico/imprimirPesquisa.do?tjpr.url.crypto=8a6c53f8698c7ff7be4b80f414624b3f33113488aa693b6bf8d4ed6d3aa664dfd7b4ef811c669b3a>. Acesso em: 30 abr. 2013.

PARODI, Lorenzo. **Manual das fraudes.** 2.ed. Rio de Janeiro: Brasport: 2008. Disponível em: <http://books.google.com.br/books?id=0lGTAkLxt0AC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 7 maio 2013.

PINHEIRO, Patrícia Peck. **Direito digital**. 4 ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**: parte especial – arts. 121 a 249. 11.ed.rev.atual. e ampl. São Paulo, Revista dos Tribunais, 2013. v.2

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Crime n. 70028777555**. Comarca de Lajeado. Quinta Câmara Criminal. Rel. Desa. Genacéia da Silva Alberton. Julgado em 16 dez. 2009. Publicado no DJ 26 jan. 2010. Disponível em: < http://google7.tjrs.jus.br/search?q=cache:www1.tjrs.jus.br/site_php/consulta/consulta_processo.php%3Fnome_comarca%3DTribunal%2Bde%2BJusti%25E7a%26versao%3D%26versao_fonetica%3D1%26tipo%3D1%26id_comarca%3D700%26num_processo_mask%3D70028777555%26num_processo%3D70028777555%26codEmenta%3D3326546+venda+pela+internet+estelionato&site=ementario&client=buscaTJ&access=p&ie=UTF-8&proxystylesheet=buscaTJ&output=xml_no_dtd&oe=UTF-8&numProc=70028777555&comarca=Comarca+de+Lajeado&dtJulg=16-12-2009&relator=Genac%E9ia+da+Silva+Alberton>. Acesso em 30 abr. 2013.

SÃO PAULO. Tribunal de Justiça. **Apelação Criminal n. 0001652-03.2010.8.26.0196**. Comarca de Franca. Décima Sexta Câmara Criminal. Rel. Des. Newton Neves. Julgado em 5 mar. 2013. Publicado no DJ em 7 mar. 2013. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=6554635>. Acesso em: 30 abr. 2013.

SANTA CATARINA. Tribunal de Justiça. **Agravo de Instrumento n. 2010.024383-8**. Comarca de Caçador. Primeira Câmara de Direito Público. Rel. Des. Paulo Henrique Moritz Martins da Silva. Julgado em 30 nov. 2010. Disponível em: <http://app6.tjsc.jus.br/cposg/pcpoSelecaoProcesso2Grau.jsp?cbPesquisa=NUMPROC&Pesquisar=Pesquisar&dePesquisa=20100243838>. Acesso em 20 mar. 2013a.

_____. Tribunal de Justiça. **Apelação Criminal n. 98.015071-0**. Comarca de Lages. Rel. Des. Roberto Roberge. Julgado em 24 fev. 1999. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/4955744/apelacao-criminal-apr-150710/inteiro-teor>. Acesso em 20 mar. 2013b.

_____. Tribunal de Justiça. **Apelação Criminal n. 2012.047161-5**. Comarca de Balneário Camboriú. Primeira Câmara Criminal. Rel. Desa. Marli Mosimann Vargas. Julgado em 5 mar. 2013. DJ s/d. Disponível em: <http://app.tjsc.jus.br/jurisprudencia/html.do?q=estelionato%20internet&only_ementa=&frase=&id=AAAbmQAACAABLA8AAC&categoria=acordao>. Acesso em: 30 abr. 2013c.

SINGH, Mohini; WADDELL, Dianne. **Business to employee (b2e) e-business model**: a service to employees or organizational management? IADIS International Conference e-Society 2007. Disponível em: <www.iadis.net/dl/final_uploads/200703L013.pdf>. Acesso em: 18 jan. 2013.

SOUZA, Miguel. **Fundamentos de e-commerce.** Universidade lusíada de Angola, departamento de Informática. Luanda, 2010. Disponível em: <http://pt.scribd.com/doc/57584211/15/Consumer-to-Administration-C2A-ou-C2G>. Acesso em: 27 mar. 2013.

TOLEDO, Luciano Augusto; CAIGAWA, Sidney Maçazzo; SILVA, Newton Siqueira da. Negócios empresariais e a internet: o caso Bosio Brasil**. Revista FAE**, Curitiba, v.8, n.1, p.27-38, jan./jun. 2005. Disponível em: <http://www.unifae.br/publicacoes/pdf/revista_da_fae/rev_fae_v8_n1/rev_fae_v8_n1_03.pdf>. Acesso em: 16 jan. 2013.

TURBAN, Efraim; KING, David. **Comércio eletrônico**: estratégia e gestão. São Paulo, Prentice Hall, 2004.

UNIÃO EUROPEIA. Convenção sobre o cibercrime. **Série de tratados europeus, 185**. Budapeste: 2001. Disponível em:< http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/downloadFile/attachedFile_f0/STE_185.pdf>. Acesso em 21 maio 2013.

WILLY, Aldrin. Lojas fantasmas praticam o estelionato virtual. **Imprensa Popular,** Porto Velho, 01 mar. 2010. Disponível em: <http://www.imprensapopular.com/see.asp?codnews=4262&categoria=reportagem&chamada=Lojas+fantasmas+praticam+o+estelionato+virtual>. Acesso em: 17 abr. 2013.

ANEXOS

ANEXO A – Projeto de reforma ao Código de Defesa do Consumidor

SENADO FEDERAL
PROJETO DE LEI DO SENADO
Nº281, DE 2012

Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico.

O CONGRESSO NACIONAL decreta:

Art. 1º A lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), passa a vigorar com as seguintes alterações:

"Art. 1º .....

Parágrafo único. As normas e os negócios jurídicos devem ser interpretador e integrados da maneira mais favorável ao consumidor. (NR)"

"**Art. 5º .....**

VI – o conhecimento de ofício pelo Poder Judiciário, no âmbito do processo em curso e assegurado o contraditório, e pela Administração Pública de violação a normas de defesa do consumidor;
VII – a interpretação e a integração das normas e negócios jurídicos da maneira mais favorável ao consumidor.
..... (NR)"

"**Art. 6º .....**
.....
XI – a autodeterminação, a privacidade e a segurança das informações e dados pessoais prestados ou coletados, por qualquer meio, inclusive o eletrônico;
XII – a liberdade de escolha, em especial frente a novas tecnologias e redes de dados, sendo vedada qualquer forma de discriminação e assédio de consumo. (NR)"

"**Art. 7º .....**
§1º **.....**
§2º Aplica-se ao consumidor a norma mais favorável ao exercício de seus direitos e pretensões. (NR)"

"Seção VII

Do Comércio Eletrônico

Art. 45-A. Esta seção dispõe sobre normas gerais de proteção do consumidor no comércio eletrônico, visando a fortalecer a sua confiança e assegurar tutela efetiva, com a diminuição da assimetria de informações, a preservação da segurança nas transações, a proteção da autodeterminação e da privacidade dos dados pessoais.
Parágrafo único. As normas desta Seção aplicam-se às atividades desenvolvidas pelos fornecedores de produtos ou serviços por meio eletrônico similar.

Art. 45-B. Sem prejuízo do disposto nos arts. 31 e 33, o fornecedor de produtos e serviços que utilizar meio eletrônico ou similar deve disponibilizar em local de destaque e de fácil visualização:
I – seu nome empresarial e número de sua inscrição no cadastro geral do Ministério da Fazenda;
II – seu endereço geográfico e eletrônico, bem como as demais informações necessárias para a sua localização, contato e recebimento de comunicações e notificações judiciais e extrajudiciais;
III – preço total do produto ou do serviço, incluindo a discriminação de quaisquer eventuais despesas, tais como a de entrega e seguro;
IV – especificidades e condições da oferta, inclusive as modalidades de pagamento, execução, disponibilidade ou entrega;
V – características essenciais do produto ou do serviço;
VI – prazo de validade da oferta, inclusive do preço;
VII – prazo da execução do serviço ou da entrega ou disponibilização do produto.

Art. 45-C. É obrigação do fornecedor que utilizar o meio eletrônico ou similar:
I – manter disponível serviço adequado, facilitado e eficaz de atendimento, tal como o meio eletrônico ou telefônico, que possibilite ao consumidor enviar e receber comunicações, inclusive notificações, reclamações e demais informações necessárias à efetiva proteção de seus direitos;
II – confirmar imediatamente o recebimento de comunicações, inclusive a manifestação de arrependimento e cancelamento do contrato, utilizando o mesmo meio empregado pelo consumidor ou outros costumeiros;

III – assegurar ao consumidor os meios técnicos adequados, eficazes e facilmente acessíveis que permitam a identificação e correção de eventuais erros na contratação, antes de finalizá-la, sem prejuízo do posterior exercício do direito de arrependimento;
IV – dispor de meios de segurança adequados e eficazes;

V – informa aos órgãos de defesa do consumidor e ao Ministério Público, sempre que requisitado, o nome e endereço eletrônico e demais dados que possibilitem o contato do provedor de hospedagem, bem como dos seus prestadores de serviços financeiros e de pagamento.

Art. 45-D. É verdado enviar mensagem eletrônica não solicitada ao destinatário que:
I – não possua relação de consumo anterior com o fornecedor e não tenha manifestado consentimento prévio em recebe-la;
II – esteja inscrito em cadastro de bloqueio de oferta; ou
III – tenha manifestado diretamente ao fornecedor a opção de não recebê-la.
§1º Se houver prévia relação de consumo entre o remetente e o destinatário, admite-se o envio de mensagem não solicitada, desde que o consumidor tenha tido oportunidade de recusá-la.
§2º O fornecedor deve informar ao destinatário, em cada mensagem enviada:
I – o meio adequado, simplificado, seguro e eficaz que lhe permita, a qualquer momento, recusar, sem ônus, o envio de novas mensagens eletrônicas não solicitadas; e
II – o modo como obteve os dados do consumidor.
§3º O fornecedor deve cessar imediatamente o envio de ofertas e comunicações eletrônicas ou de dados a consumidor que manifestou a sua recusa em recebe-las.
§4º Para os fins desta seção, entende-se por mensagem eletrônica não solicitada a relacionada a oferta ou publicidade de produto ou serviço e enviada por correio eletrônico ou meio similar.
§5º É também vedado:
I – remeter mensagem que oculte, dissimule ou não permita de forma imediata e fácil a identificação da pessoa em nome de quem é efetuada a comunicação e a sua natureza publicitária.
II – veicular, hospedar, exibir, licenciar, alienar, utilizar, compartilhar, doar ou de qualquer forma ceder ou transferir dados, informações ou identificadores pessoais, sem expressa autorização e consentimento informado do seu titular, salvo exceções legais.”

.....

“Art. 49. O consumidor pode desistir da contratação a distância, no prazo de sete dias a contar da oferta ou do recebimento ou disponibilidade do produto ou serviço, o que ocorrer por último.
§ 1º **.....**
§ 2º Por contratação a distância, entende-se aquela efetivada fora do estabelecimento, ou sem a presença física simultânea do consumidor e fornecedor, especialmente em domicílio, por telefone, reembolso postal, por meio eletrônico ou similar.
§ 3º Equipara-se à modalidade de contratação prevista no § 2º deste artigo aquela em que, embora realizada no estabelecimento, o consumidor não teve a prévia oportunidade de conhecer o produto ou serviço, por não se encontrar em exposição ou pela impossibilidade ou dificuldade de acesso a seu conteúdo.
§ 4º Caso o consumidor exerça o direito de arrependimento, os contratos

acessórios de créditos são automaticamente rescindidos, sem qualquer custo para o consumidor;
§ 5º Sem prejuízo da iniciativa do consumidor, o fornecedor deve comunicar de modo imediato a manifestação do exercício de arrependimento à instituição financeira ou à administradora do cartão de crédito ou similar, a fim de que:
I – a transação não seja lançada na fatura do consumidor;
II – seja efetivado o estorno do valor, caso a fatura já tenha sido emitida no momento da comunicação;
III – caso o preço já tenha sido total ou parcialmente pago, seja lançado o crédito do respectivo valor na fatura imediatamente posterior à comunicação.
§ 6º Se o fornecedor de produtos ou serviços descumprir o disposto no § 1º ou no § 5º, o valor pago será devolvido em dobro.
§ 7º O fornecedor deve informar, de forma clara e ostensiva, os meios adequados, facilitados e eficazes disponíveis para o exercício do direito de arrependimento do consumidor, que devem contemplar, ao menos, o mesmo modo utilizado para a contratação.
§ 8º O fornecedor deve enviar ao consumidor confirmação individualizada e imediata do recebimento da manifestação de arrependimento.
§ 9º O descumprimento dos deveres do fornecedor previstos neste artigo e nos artigos da Seção VII do Capítulo V do Título I desta lei enseja a aplicação pelo Poder Judiciário de multa civil em valor adequado à gravidade da conduta e suficiente para inibir novas violações, sem prejuízo das sanções penais e administrativas cabíveis e da indenização por perdas e danos, patrimoniais e morais, ocasionados aos consumidores. (NR)”

“**Art. 56.** .....
.....
XIII – suspensão temporária ou proibição de oferta e de comércio eletrônico.
..... (NR)”

“**Art. 59.** .....
.....
“§ 4º Caso o fornecedor por meio eletrônico ou similar descumpra a pena de suspensão ou de proibição de oferta e de comércio eletrônico, sem prejuízo de outras medidas administrativas ou judiciais de prevenção de danos, o Poder Judiciário determinará, a pedido da autoridade administrativa para a garantia da efetividade da sanção, que os prestadores de serviços financeiros e de pagamento utilizados pelo fornecedor, de forma alternativa ou conjunta, sob pena de pagamento de multa diária:
I – suspendam os pagamentos e transferências financeiras para o fornecedor de comércio eletrônico;
II – bloqueiem as contas bancárias do fornecedor. (NR)”

"**Art. 72-A.** Veicular, hospedar, exibir, licenciar, alienar, utilizar, compartilhar, doar ou de qualquer forma ceder ou transferir dados, informações ou identificadores pessoais, sem a expressa autorização de seu titular e consentimento informado, salvo exceções legais.
Pena – Reclusão, de um a quatro anos, e multa."

"**Art. 101.** Na ação de responsabilidade contratual e extracontratual do fornecedor de produtos e serviços, inclusive no fornecimento a distância nacional e internacional, sem prejuízo do disposto nos Capítulos I e II deste Título:
I – será competente o foro do domicílio do consumidor, nas demandas em que o consumidor residente no Brasil seja réu e que versem sobre relações de consumo;
II – o consumidor, nas demandas em que seja autor, poderá escolher, além do foro indicado no inciso I, o do domicílio do fornecedor de produtos ou serviços, o do lugar da celebração ou da execução do contrato ou outro conectado ao caso;
III – são nular as cláusulas de eleição de foro e de arbitragem celebradas pelo consumidor.
Parágrafo único. Aos conflitos decorrentes do fornecimento a distância internacional, aplica-se a lei do domicílio do consumidor, ou a norma estatal escolhida pelas partes, desde que mais favorável ao consumidor, assegurando igualmente o seu acesso à Justiça. (NR)"

Art. 2º Esta Lei entra em vigor na data da sua publicação.

JUSTIFICAÇÃO

O projeto de lei objetiva atualizar a Lei nº 8.078, de 1990 (Código de Defesa do Consumidor), a fim de aperfeiçoar as disposições do capítulo I e dispor sobre o comércio eletrônico.

A crescente complexidade das relações de consumo demanda a previsão de princípios que reforcem a proteção do consumidor frente a novos desafios, principalmente os relacionados com o diálogo com outras fontes normativas, a segurança nas transações, bem como a proteção, bem como a proteção da autodeterminação e privacidade de seus dados.

É igualmente imprescindível a introdução de uma seção específica sobre a proteção dos consumidores no âmbito do comércio eletrônico, em razão da sua expressiva utilização. Se, à época da promulgação do Código de Defesa do Consumidor, o comércio eletrônico nem sequer existia, atualmente, é o meio de fornecimento a distância mais utilizado, alcançando sucessivos recordes de faturamento. Porém, ao mesmo tempo ocorre o aumento exponencial do número de demandas dos consumidores. As normas projetadas atualizam a lei de proteção ao consumidor a esta nova realidade, reforçando, a exemplo do que já foi feito na Europa e nos Estados Unidos, os direitos de informação, transparência, lealdade, autodeterminação, cooperação e segurança nas relações de consumo estabelecidas através do comércio eletrônico.

Busca-se ainda a proteção do consumidor em relação a mensagens eletrônicas não solicitadas (spams), além de disciplinar o exercício do direito de arrependimento.

A evolução do comércio eletrônico, se, por um lado, traz inúmeros benefícios, por outro, amplia a vulnerabilidade do consumidor. Assim, é essencial que se cumpra o comando constitucional do art. 5º, XXXII, e do art. 170, V, da Constituição Federal, e se criem normas que, efetivamente, ampliem a sua proteção no comércio eletrônico, a fim de que a evolução tecnológica alcance os objetivos que todos desejam: o desenvolvimento social e econômico, o aperfeiçoamento das relações de consumo e a prevenção de litígios.

Sala de sessões,

Senador José Sarney

Fonte: BRASIL, Projeto de Lei do Senado Federal nº 281/2012, 2013.

ANEXO B – Projeto de Lei nº 2.126/1011 (Marco Civil)

PROJETO DE LEI

Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O CONGRESSO NACIONAL decreta:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da Internet no Brasil tem como fundamentos:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração; e

V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição;

II - proteção da privacidade;

III - proteção aos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade da rede, conforme regulamentação;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; e

VII - preservação da natureza participativa da rede.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio, relacionados à matéria, ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da Internet no Brasil tem os seguintes objetivos:

I - promover o direito de acesso à Internet a todos os cidadãos;

II - promover o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III- promover a inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - promover a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - Internet - o sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal - computador ou qualquer dispositivo que se conecte à Internet;

III - administrador de sistema autônomo - pessoa física ou jurídica que administra blocos de endereço Internet Protocol – IP - específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

IV - endereço IP - código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

V - conexão à Internet - habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão - conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de Internet - conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e

VIII - registros de acesso a aplicações de Internet - conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei, serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos:

I - à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

II - à não suspensão da conexão à Internet, salvo por débito diretamente decorrente de sua utilização;

III - à manutenção da qualidade contratada da conexão à Internet, observado o disposto no art. 9º;

IV - a informações claras e completas constantes dos contratos de prestação de serviços, com previsão expressa sobre o regime de proteção aos seus dados pessoais, aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar a qualidade dos serviços oferecidos; e

V - ao não fornecimento a terceiros de seus registros de conexão e de acesso a aplicações de Internet, salvo mediante consentimento ou nas hipóteses previstas em lei.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET
Seção I
Do Tráfego de Dados

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo vedada qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação.

Parágrafo único. Na provisão de conexão à Internet, onerosa ou gratuita, é vedado monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, ressalvadas as hipóteses admitidas em lei.

Seção II
Da Guarda de Registros

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar as informações que permitam a identificação do usuário mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo.

§ 2º As medidas e procedimentos de segurança e sigilo devem ser informados pelo responsável pela provisão de serviços de conexão de forma clara e atender a padrões definidos em regulamento.

§ 3º A violação do dever de sigilo previsto no caput sujeita o infrator às sanções cíveis, criminais e administrativas previstas em lei.

Subseção I
Da Guarda de Registros de Conexão

Art. 11. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa poderá requerer cautelarmente a guarda de registros de conexão por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido impetrado no prazo previsto no § 3º.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet

Art. 12. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet.

Art. 13. Na provisão de aplicações de Internet é facultado guardar os registros de acesso dos usuários, respeitado o disposto no art. 7º.

§ 1º A opção por não guardar os registros de acesso a aplicações de Internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

§ 2º Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na SeçãoIV deste Capítulo.

§ 3º Observado o disposto no § 2º, a autoridade policial ou administrativa poderá requerer cautelarmente a guarda dos registros de aplicações de Internet, observados o procedimento e os prazos previstos nos §§ 3ºe 4º do art. 11.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 14. O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros.

Art. 15. Salvo disposição legal em contrário, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.

Parágrafo único. A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

Art. 16. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 15, caberá ao provedor de aplicações de Internet informar-lhe sobre o cumprimento da ordem judicial.

Seção IV
Da Requisição Judicial de Registros

Art. 17. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 18. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, vida privada, honra e imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 19. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil:

I - estabelecimento de mecanismos de governança transparentes, colaborativos e democráticos, com a participação dos vários setores da sociedade;

II - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e níveis da federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

III - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes níveis federativos e diversos setores da sociedade;

IV - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

V - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VI - otimização da infraestrutura das redes, promovendo a qualidade técnica, a inovação e a disseminação das aplicações de Internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VII - desenvolvimento de ações e programas de capacitação para uso da Internet;

VIII - promoção da cultura e da cidadania; e

IX - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso.

Art. 20. Os sítios e portais de Internet de entes do Poder Público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 21. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção de cultura e o desenvolvimento tecnológico.

Art. 22. As iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 23. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas referentes ao uso e desenvolvimento da Internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 24. A defesa dos interesses e direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 25. Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Brasília,

EMI Nº 00086 - MJ/MP/MCT/MC

Brasília, 25 de abril de 2011

Excelentíssima Senhora Presidenta da República,

- Submetemos à elevada consideração de Vossa Excelência o anexo anteprojeto de lei que estabelece princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no país, e dá outras providências. Tal projeto foi construído em conjunto com a sociedade, em processo que ficou conhecido sob a denominação de Marco Civil da Internet.

2. Dados recentes da Pesquisa Nacional por Amostra de Domicílios – PNAD referente ao ano de 2009 realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) apontam a existência de sessenta e oito milhões de internautas, com taxa de crescimento de mais de um milhão a cada três meses. Ao mesmo tempo em que empolgam, esses números expressam a

dimensão dos diversos desafios para que a Internet realize seu potencial social. Um desses desafios é harmonizar a interação entre o Direito e a chamada cultura digital, superando uma série de obstáculos críticos, presentes tanto nas instituições estatais quanto difusos na sociedade.

3. No âmbito legislativo, diversos projetos de lei tramitam desde 1995, ano do início da oferta comercial de conexões no país. No entanto, passados quinze anos, ainda não existe um texto de lei específico para o ambiente cibernético que garanta direitos fundamentais e promova o desenvolvimento econômico e cultural.

4. Para o Poder Judiciário, a ausência de definição legal específica, em face da realidade diversificada das relações virtuais, tem gerado decisões judiciais conflitantes, e mesmo contraditórias. Não raro, controvérsias simples sobre responsabilidade civil obtêm respostas que, embora direcionadas a assegurar a devida reparação de direitos individuais, podem, em razão das peculiaridades da Internet, colocar em risco as garantias constitucionais de privacidade e liberdade de expressão de toda a sociedade.

5. Também a Administração Pública é submetida a dificuldades para promover o desenvolvimento da Internet, em temas tão variados como infraestrutura e padrões de interoperabilidade. Diversas políticas públicas de governo bem sucedidas ainda carecem de um amparo legal integrado para sua adoção, como políticas de Estado, que permitam, nos diversos níveis federativos, uma abordagem de longo prazo para cumprir o objetivo constitucional de redução das desigualdades sociais e regionais.

6. Por fim, a crescente difusão do acesso enseja novos contratos jurídicos, para os quais a definição dos limites fica a cargo dos próprios contratantes, sem a existência de balizas legais. A seguir essa lógica, a tendência do mercado é a de que os interesses dos agentes de maior poder econômico se imponham sobre as pequenas iniciativas, e que as pretensões empresariais enfraqueçam os direitos dos usuários.

7. Os riscos são, portanto, a) da aprovação desarticulada de propostas normativas especializadas, que gerem divergência e prejudiquem um tratamento harmônico da matéria; b) de prejuízos judiciais sensíveis, até que a jurisprudência se adeque às realidades da sociedade da informação; c) de desencontros ou mesmo omissões nas políticas públicas; e d) de violação progressiva de direitos dos usuários pelas práticas e contratos livremente firmados.

8. Esse quadro de obstáculos faz oportuna a aprovação de uma lei que, abordando de forma transversal a Internet, viabilize ao Brasil o início imediato de um melhor diálogo entre o Direito e a Internet. Uma norma que reconheça a pluralidade das experiências e que considere a riqueza e a complexidade dessa nova realidade.

9. Com esse propósito, a Secretaria de Assuntos Legislativos do Ministério da Justiça - SAL/MJ, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, desenvolveu a iniciativa denominada Marco Civil da Internet no Brasil, a fim de construir, de forma colaborativa, um anteprojeto de lei que estabelecesse princípios, garantias e direitos dos usuários de Internet. A proposta delimita deveres e responsabilidades a serem exigidos dos prestadores de serviços e define o papel a ser exercido pelo poder público em relação ao desenvolvimento do potencial social da rede.

10. Com vistas ao diálogo entre normas jurídicas e a rede mundial de computadores, partiu-se de duas óbvias inspirações: o texto constitucional e o conjunto de recomendações apresentadas pelo Comitê Gestor da Internet no Brasil - CGI.br - no documento "Princípios para a governança e uso da Internet" (Resolução CGI.br/RES/2009/003/P). Para o seu desenvolvimento, o projeto se valeu de inovador debate aberto a todos os internautas.

11. Uma discussão ampla foi realizada com a sociedade pela própria Internet, entre outubro de 2009 e maio de 2010, por meio de um blog hospedado na plataforma Cultura Digital (uma rede social mantida pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa - RNP). Esse processo de participação popular resultou em mais de dois mil comentários diretos, incontáveis manifestações sobre o "#marcocivil" em ferramentas virtuais, como os microblogs Identi.ca e Twitter, além de dezenas de documentos institucionais, oriundos do Brasil e do exterior.

12. A dinâmica adotada teve como meta usar a própria Internet para, desde já, conferir mais densidade à democracia. Por meio da abertura e da transparência, permitiu-se a franca expressão pública de todos os grupos sociais, por meio de um diálogo civilizado e construtivo.

13. Resultado desse processo, o anteprojeto ora proposto se estrutura em cinco capítulos: disposições preliminares, direitos e garantias do usuário, provisão de conexão e de aplicações de Internet, atuação do poder público e disposições finais.

14. No primeiro capítulo, são indicados os fundamentos, princípios e objetivos do marco civil da internet, além da definição de conceitos e de regras de interpretação. Entre os fundamentos, enumeram-se elementos da realidade jurídica do uso da Internet que servem de pressupostos para a proposta. Por sua vez, entre os princípios figuram os pontos norteadores que devem sempre informar a aplicação do direito em relação à matéria. Já no âmbito dos objetivos, apontam-se as finalidades a serem perseguidas de forma permanente, não apenas pelo Estado, mas por toda a sociedade.

15. No capítulo sobre os direitos e garantias do usuário, o acesso à internet é reconhecido como um direito essencial ao exercício da cidadania. Ainda são apontados direitos específicos

a serem observados, tais como a inviolabilidade e o sigilo das comunicações pela internet e a não suspensão da conexão.

16. No terceiro capítulo, ao tratar da provisão de conexão e de aplicações de internet, o anteprojeto versa sobre as questões como: o tráfego de dados, a guarda de registros de conexão à Internet, a guarda de registro de acesso a aplicações na rede, a responsabilidade por danos decorrentes de conteúdo gerado por terceiros e a requisição judicial de registros. As opções adotadas privilegiam a responsabilização subjetiva, como forma de preservar as conquistas para a liberdade de expressão decorrentes da chamada Web 2.0, que se caracteriza pela ampla liberdade de produção de conteúdo pelos próprios usuários, sem a necessidade de aprovação prévia pelos intermediários. A norma mira os usos legítimos, protegendo a privacidade dos usuários e a liberdade de expressão, adotando como pressuposto o princípio da presunção de inocência, tratando os abusos como eventos excepcionais.

17. No capítulo referente às atribuições do Poder Público, fixam-se diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil, além de regras para os sítios públicos, para a Educação, para o fomento cultural e para a avaliação constante do resultado das políticas públicas. Confere-se à Administração Pública um parâmetro para o melhor cumprimento dos objetivos do Marco Civil.

18. Finalmente, o último capítulo prevê expressamente a possibilidade de que a defesa dos interesses e direitos pertinentes ao uso da Internet seja exercida de forma individual ou coletiva, na forma da Lei.

19. No panorama normativo, o anteprojeto representa um primeiro passo no caminho legislativo, sob a premissa de que uma proposta legislativa transversal e convergente possibilitará um posicionamento futuro mais adequado sobre outros importantes temas relacionados à internet que ainda carecem de harmonização, como a proteção de dados pessoais, o comércio eletrônico, os crimes cibernéticos, o direito autoral, a governança da internet e a regulação da atividade dos centros públicos de acesso à internet, entre outros. A despeito das mencionadas lacunas normativas, a solução que se submete à avaliação de Vossa Excelência faz jus ao potencial criativo e inovador característico do povo brasileiro, alçando o país à posição de protagonista mundial na garantia das novas liberdades da cultura digital.

Ante todo o exposto, Senhora Presidenta, a proposta que institui o marco civil da internet no Brasil deve, a nosso ver, ser incorporada ao direito positivo pátrio, a fim de estabelecer princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no país.

Respeitosamente,

Assinado por: José Eduardo Martins Cardozo, Miriam Aparecida Belchior, Aloizio Mercadante Oliva e Paulo Bernardo Silva.

Fonte: BRASIL, Projeto de lei nº 2.126/2011, 2013.

ANEXO C – Convenção internacional contra o cibercrime

CONVENÇÃO SOBRE
O CIBERCRIME

Budapeste, 23.11.2001

Preâmbulo

Os Estados-Membros do Conselho da Europa e os restantes Estados signatários da presente Convenção,

Considerando que o objectivo do Conselho da Europa é o de realizar uma união mais estreita entre os seus membros;

Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes na Convenção;

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum que vise proteger a sociedade da criminalidade no ciberespaço, nomeadamente através da adopção de legislação adequada e da melhoria da cooperação internacional;

Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

Preocupados com o risco de que as redes informáticas e a informação electrónica sejam, igualmente, utilizadas para cometer infracções penais e de que as provas dessas infracções sejam armazenadas e transmitidas através de tais redes;

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate ao cibercrime, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias de informação;

Acreditando que uma luta efictiva contra o cibercrime requer uma acrescida, rápida e eficaz cooperação internacional em matéria penal;

Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados, bem como a utilização fraudulenta de tais sistemas, prevendo a incriminação desses comportamentos tal como descritos na presente Convenção, e a adopção de medidas que permitam o combate eficaz de tais infracções facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e ao prever medidas materiais com vista ao estabelecimento de uma cooperação internacional rápida e fiável;

Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do homem, tal como garantidos pela Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950), pelo Pacto Internacional relativo aos Direitos Civis e Políticos das Nações Unidas (1966), bem como por outros tratados internacionais aplicáveis em matéria de direitos do Homem, que reafirmam o direito à liberdade de opinião sem ingerências, bem como o direito à liberdade de expressão, incluindo a liberdade de procurar, receber e transmitir informações e ideias de qualquer natureza, independentemente de fronteiras, bem como o direito ao respeito pela vida privada;

Tendo, igualmente, presente o direito à protecção de dados pessoais, tal como é conferido pela Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, assinada em 1981;

Considerando a Convenção das Nações Unidas sobre os Direitos da Criança, assinada em 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil , assinada em 1999;

Tendo em conta as Convenções do Conselho da Europa sobre a cooperação em matéria penal, bem como outros tratados similares celebrados entre os Estados-Membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas Convenções de modo a tornar mais eficazes as investigações e os

procedimentos criminais relativos a infracções relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas por meio electrónico de uma infracção penal;

Congratulando-se com os recentes desenvolvimentos destinados a melhorar o entendimento e a cooperação internacionais no combate à criminalidade no ciberespaço, nomeadamente as acções empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

Recordando as Recomendações do Comité de Ministros Nº R (85) 10 relativa à aplicação prática da Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal no tocante às cartas rogatórias para intercepção de telecomunicações, Nº R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio dos direitos de autor e direitos conexos, Nº R (87) 15 visando regulamentar a utilização de dados de 4 carácter pessoal no sector da polícia , Nº R (95) 4 sobre a protecção de dados de carácter pessoal no domínio dos serviços de telecomunicações, designadamente os serviços telefónicos, e Nº R (89) 9 sobre a criminalidade informática que estabelece, para os legisladores nacionais, directrizes para a definição de certos crimes informáticos, e ainda a Nº R (95) 13 relativa a problemas processuais penais relacionados com a tecnologia de informação;

Tendo em consideração a Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), a qual recomendava ao Comité de Ministros o apoio ao trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) sobre o cibercrime, a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios de investigação eficazes em matéria de crimes informáticos, bem como a Resolução n.º 3 adoptada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), a qual incentiva as partes intervenientes nas negociações a prosseguirem os seus esforços no sentido de serem encontradas soluções que permitam ao maior número possível de Estados tornarem-se partes da Convenção, e reconhece a necessidade de se dispor de um mecanismo rápido e eficaz de cooperação internacional que tenha devidamente em conta as exigências específicas da luta contra o cibercrime;

Tendo, igualmente, em consideração o Plano de Acção adoptado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11

de Outubro de 1997), visando encontrar respostas comuns face ao desenvolvimento das novas tecnologias de informação assentes nas normas e nos valores do Conselho da Europa;

Acordaram no seguinte:

Capítulo I – Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

a) A expressão «*sistema informático*» designa qualquer dispositivo isolado ou conjunto de dispositivos interconectados ou relacionados entre si, sendo que um ou vários desses dispositivos asseguram, em execução de um programa, o tratamento automatizado de dados;

b) A expressão «*dados informáticos*» designa qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa que permita a um sistema informático executar uma função;

c) A expressão «*fornecedor de serviços*» designa:

   i. qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem através de um sistema informático;

   ii. qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicações ou dos utilizadores desse serviço.

d) A expressão "*dados relativos ao tráfego*" designa quaisquer dados informáticos relacionados com uma comunicação efectuada através de um sistema informático e produzidos por este enquanto elemento da cadeia de comunicação, contendo indicação da origem, do destino, do percurso, da hora, da data, do volume e da duração da comunicação, ou do tipo de serviço subjacente.

Capítulo II - Medidas a serem tomadas a nível nacional

Secção 1 .- Direito penal material

Título 1 – Infracções penais contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos

Artigo 2º - Acesso ilegítimo

Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, quando praticado intencionalmente, o acesso ilegítimo a todo ou a parte de um sistema informático. Qualquer Parte poderá subordinar a tipificação da infracção penal à existência de violação das medidas de segurança com a intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3º - Intercepção ilegítima

Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para que seja tipificada como infracção penal, no seu direito interno, quando praticada intencionalmente, a intercepção ilegítima, efectuada através de meios técnicos, de dados informáticos em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo as emissões electromagnéticas provenientes de um sistema informático que transporte tais dados informáticos. Qualquer Parte poderá subordinar a infracção penal à existência de dolo ou à sua relação com um sistema informático conectado com outro sistema informático.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracções penais, no seu direito interno, quando praticados intencionalmente, os actos ilegítimos de danificar, apagar, deteriorar, alterar ou suprimir dados informáticos.

2. Qualquer Parte poderá reservar-se o direito de exigir que da conduta prevista no n.º 1 do presente artigo resultem danos graves.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, quando praticada intencionalmente, a interferência ilegítima no funcionamento de um sistema informático através da introdução, da

transmissão, da danificação, da eliminação, da deterioração, da alteração ou da supressão de dados informáticos.

Artigo 6º - Uso indevido de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracções penais, no seu direito interno, quando praticadas de forma intencional e ilegítima:
   a. A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
      i. um dispositivo, incluindo um programa informático, essencialmente concebido ou adaptado para permitir a prática de uma das infracções previstas nos artigos 2º a 5º da presente Convenção;
      ii. uma palavra-passe, um código de acesso, ou dados similares que permitam o acesso a todo ou a parte de um sistema informático, visando a sua utilização na prática de qualquer uma das infracções previstas nos artigos 2º a 5º da presente Convenção;
   b. A posse de um dos elementos referidos na alínea a) (i) ou (ii) do presente artigo, desde que utilizados com a intenção de cometer qualquer uma das infracções penais previstas nos artigos 2º a 5º da presente Convenção. Qualquer Parte poderá subordinar a previsão da responsabilidade criminal à existência de um determinado número desses requisitos.

2. O presente artigo não poderá ser interpretado como prevendo responsabilidade criminal quando a produção, a venda, a obtenção para utilização, a importação, a distribuição ou outras formas de disponibilização referidas no n.º 1 do presente artigo não visem a prática de uma infracção penal prevista nos artigos 2º a 5º da presente Convenção, tal como ensaios autorizados ou a protecção de um sistema informático.

3. Cada Parte poderá reservar-se o direito de não aplicar o disposto no n. º1 do presente artigo, desde que tal reserva não diga respeito à venda, à distribuição ou a qualquer outra forma de disponibilização dos elementos referidos no n.º1, a), (ii) do presente artigo.

Título 2 – Infracções penais relacionadas com computadores

Artigo 7º - Falsidade informática

Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracções penais, no seu direito interno, quando praticadas de forma intencional e ilegítima, a introdução, a alteração, a eliminação ou a supressão de dados informáticos que resultem em dados não autênticos, com o intuito de que tais dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Qualquer Parte poderá subordinar a previsão de responsabilidade criminal à existência de intenção fraudulenta ou outra similar. 8

Artigo 8º - Burla informática

Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, quando praticado de forma intencional e ilegítima, o acto de causar perda de bens a terceiros mediante:

a) Qualquer introdução, alteração, eliminação ou supressão de dados informáticos;
b) Qualquer interferência no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.

Título 3–Infracções penais relacionadas com o conteúdo

Artigo 9º - Infracções penais relacionadas com a pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracções penais, no seu direito interno, quando praticadas de forma intencional e ilegítima, as seguintes condutas:
   a) Produção de pornografia infantil visando a sua difusão através de um sistema informático;
   b) Oferta ou disponibilidade de pornografia infantil através de um sistema informático;
   c) Difusão ou transmissão de pornografia infantil através de um sistema informático;
   d) Obtenção de pornografia infantil através de um sistema informático, para si próprio ou para terceiros;
   e) Posse de pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

2. Para os fins do n.º 1 do presente artigo, a expressão «*pornografia infantil*» designa qualquer material pornográfico que represente visualmente:
   a) Um menor envolvido num comportamento sexualmente explícito;
   b) Uma pessoa, aparentando ser menor, envolvida num comportamento sexualmente explícito;
   c) Imagens realistas representando um menor envolvido num comportamento sexualmente explícito.

3. Para efeitos do n.º2 do presente artigo, a expressão «menor» designa uma pessoa com idade inferior a 18 anos. Qualquer Parte poderá exigir/impor um limite de idade inferior, que não poderá, contudo, ser inferior a 16 anos.

4. Qualquer Parte poderá reservar-se o direito de não aplicar, no todo ou em parte, o disposto nas alíneas d) e e) do n.º1 e nas alíneas b) e c) do n.º2 do presente artigo.

Título 4– Infracções penais relacionadas com a violação do direito de autor e direitos conexos

Artigo 10º - Infracções penais relacionadas com a violação do direito de autor e dos direitos conexos

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, a violação do direito de autor conforme definido pela legislação dessa Parte, nos termos das obrigações por esta assumidas em aplicação da Convenção Universal sobre Direito de Autor, revista em Paris a 24 de Julho de 1971, bem como da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos Comerciais do Direito de Autor e do Tratado da OMPI sobre Direito de Autor, com excepção de quaisquer direitos morais consignados nessas Convenções, quando tais actos sejam praticados de forma intencional, numa escala comercial e por meio de um sistema informático.

2. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, a violação dos direitos conexos

definidos na legislação da referida Parte, nos termos das obrigações por esta assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma), bem como do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de quaisquer direitos morais consignados nessas Convenções, quando tais actos sejam praticados de forma intencional, a uma escala comercial e por meio de um sistema informático.

3. Qualquer Parte poderá, em circunstâncias claramente definidas, reservar-se o direito de não determinar a responsabilidade criminal nos termos dos números 1 e 2 do presente artigo, desde que se encontrem disponíveis outros meios eficazes e tal reserva não prejudique as obrigações internacionais assumidas por essa Parte por força dos instrumentos internacionais referidos nos números 1 e 2 do presente artigo.

Título 5– Outras formas de responsabilidade e sanções

Artigo 11º - Tentativa e cumplicidade

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, a cumplicidade quando cometida intencionalmente com vista à prática de qualquer uma das infracções penais previstas em aplicação do disposto nos artigos 2º a 10º da presente Convenção, com a intenção de que tal infracção seja cometida.

2. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para tipificar como infracção penal, no seu direito interno, a tentativa intencional de cometer qualquer uma das infracções penais previstas nos artigos 3º a 5º , 7º, 8º e nas als. a) e c) do n.º 1 do artigo 9º da presente Convenção.

4. Cada Parte poderá reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

Artigo 12º - Responsabilidade das pessoas colectivas

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para garantir a responsabilização das pessoas colectivas pela prática de infracções penais previstas na presente Convenção, sempre que tais infracções sejam cometidas, em seu benefício, por qualquer pessoa singular agindo quer individualmente quer como membro de um órgão da pessoa colectiva, que exerça, no seu seio, uma posição de direcção, com base em:
   a) Poder de representação da pessoa colectiva;
   b) Autoridade para tomar decisões em nome da pessoa colectiva;
   c) Autoridade para exercer controlo no seio da pessoa colectiva.

2. Para além dos casos já previstos no n.º 1 do presente artigo, cada Parte adoptará as medidas que se mostrem necessárias para garantir a responsabilização de uma pessoa colectiva quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 do presente artigo, tenha tornado viável a prática das infracções previstas na presente Convenção, em benefício da referida pessoa colectiva e agindo sob a autoridade desta.

3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser de natureza criminal, civil ou administrativa.

4. Tal responsabilidade é determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção.

Artigo 13º - Sanções e medidas

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para assegurar que as infracções penais estabelecidas nos termos dos artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo as penas privativas de liberdade.

2. Cada Parte assegurará que as pessoas colectivas consideradas responsáveis por força da aplicação do artigo 12º sejam objecto de sanções ou de medidas, penais ou não penais, eficazes, proporcionadas e dissuasivas, incluindo sanções pecuniárias.

Secção 2 .- Direito processual

Título 1 – Disposições comuns

Artigo 14º - Âmbito de aplicação das disposições processuais

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento criminal específico.

2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e os procedimentos previstos no n.º 1 do presente artigo:
   a) Às infracções penais previstas nos artigos 2º a 11º da presente Convenção;
   b) A outras infracções penais cometidas através de um sistema informático; e
   c) À recolha de meios de prova em suporte electrónico, relativamente à prática de qualquer infracção penal.

3.a) Cada Parte poderá reservar-se o direito de só aplicar as medidas previstas no artigo 20º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto de tais infracções ou categorias de infracções não seja mais reduzido que o conjunto de infracções a que aplica as medidas previstas no artigo 21º. Cada Parte procurará limitar tal reserva por forma a permitir a aplicação mais ampla possível da medida prevista no artigo 20º.

b) Sempre que uma Parte, por força das restrições impostas pela sua legislação vigente à data da adopção da presente Convenção, não se encontrar em condições de aplicar as medidas previstas nos artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que:
   i. esteja em funcionamento para benefício de um grupo fechado de utilizadores;
   ii. não utilize as redes públicas de telecomunicações e que não se encontre ligado a outro sistema informático, público ou privado, tal Parte poderá reservar-se o direito de não

aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar uma tal reserva por forma a permitir a aplicação mais ampla possível das medidas previstas nos artigos 20º e 21º.

Artigo 15º - Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos na presente secção serão sujeitos às condições e salvaguardas previstas no seu direito interno, o qual deverá garantir uma protecção adequada dos direitos do Homem e das liberdades, designadamente dos direitos estabelecidos em conformidade com as obrigações assumidas pela Parte em aplicação da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950) e do Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos direitos do Homem, e deverá incorporar o princípio da proporcionalidade.

2. Sempre que tal se mostrar apropriado face à natureza do poder ou do procedimento em causa, as referidas condições e salvaguardadas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a delimitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos previstos na presente Secção sobre os direitos, as responsabilidades e os interesses legítimos de terceiros.

Título 2 – Conservação expedita de dados informáticos armazenados

Artigo 16º - Conservação expedita de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para permitir às respectivas autoridades competentes ordenar ou impor de outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativo ao

tráfego, armazenados através de um sistema informático, nomeadamente nos casos em que se possa pensar que tais dados são particularmente susceptíveis de perda ou alteração.

2. Sempre que uma Parte fizer aplicar o disposto no n.º 1 do presente artigo, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que se encontrem na sua posse ou sob o seu controlo, tal Parte adoptará as medidas legislativas e outras que se mostrem necessárias para obrigar essa pessoa a conservar e a proteger a integridade dos referidos dados por um período tão longo quanto o necessário, até ao máximo de 90 dias, por forma a permitir às autoridades competentes a obtenção da sua divulgação. Qualquer Parte poderá prever a subsequente renovação de tal injunção.

3. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para obrigar a pessoa responsável pelos dados, ou qualquer outra pessoa encarregue de os conservar, a manter segredo sobre a implementação dos referidos procedimentos por um período previsto no seu direito interno.

4. Os poderes e procedimentos referidos no presente artigo deverão ser sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

Artigo 17º - Conservação expedita e divulgação parcial de dados relativos ao tráfego

1. Por forma a assegurar a conservação dos dados relativos ao tráfego, em aplicação do artigo 16º, cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para:
   a. Assegurar a conservação rápida dos dados relativos ao tráfego, independentemente do número de fornecedores de serviço que tenham participado na transmissão de tal comunicação;
   b. Assegurar a divulgação rápida à autoridade competente da Parte, ou a qualquer pessoa designada por essa autoridade, de uma quantidade suficiente de dados relativos ao tráfego que permita a identificação dos fornecedores de serviços e da via através da qual a comunicação foi transmitida.

2. Os poderes e procedimentos referidos no presente artigo deverão ser sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

Título 3 – Injunção

Artigo 18º - Injunção

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a ordenar:
   a) A uma pessoa que se encontre no seu território a comunicar dados informáticos específicos na sua posse ou sob o seu controlo e armazenados num sistema informático ou num suporte de armazenamento de dados informáticos; e
   b) A um fornecedor de serviços que preste os seus serviços no território da Parte a comunicar os dados que tenha na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a tais serviços.

2. Os poderes e procedimentos previstos no presente artigo ficarão sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

3. Para efeitos do presente artigo, a expressão «dados relativos aos assinantes» designa quaisquer dados, apresentados sob a forma de dados informáticos ou sob qualquer outra forma, que sejam detidos por um fornecedor de serviços e que digam respeito a subscritores dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:
   a) O tipo de serviço de comunicação utilizado, as medidas de natureza técnica tomadas a esse respeito e o período de serviço;
   b) A identidade, a morada postal ou geográfica e o número de telefone do subscritor e qualquer outro número de acesso, os dados relativos à facturação e ao pagamento, disponíveis com base num contrato ou num acordo de serviços;
   c) Qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou num acordo de prestação de serviços.

Título 4 – Busca e apreensão de dados informáticos armazenados

Artigo 19º - Busca e apreensão de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a procederem a buscas ou a acederem de modo similar:
   a) A um sistema informático, ou a parte dele, bem como aos dados informáticos aí armazenados; e
   b) A um suporte que permita armazenar dados informáticos, no seu território.

2. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para assegurar que, sempre que as suas autoridades procedam a 16buscas ou acedam de modo similar a um sistema informático específico ou a parte dele, em conformidade com o disposto na al. a) do n.º 1 do presente artigo, e tenham razões para crer que os dados procurados se encontram armazenados noutro sistema informático ou em parte dele, situado no território da Parte, e que tais dados são legalmente acessíveis a partir do sistema inicial ou estão disponíveis através desse sistema inicial, as referidas autoridades estejam em condições de estender, de forma expedita, a busca ou o acesso de modo similar ao outro sistema.

3. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a apreender ou a aceder de modo similar aos dados informáticos relativamente aos quais o acesso foi efectuado em aplicação do disposto nos n.ºs 1 ou 2 do presente artigo. Tais medidas incluem as seguintes prerrogativas:
   a) Apreender ou obter de modo similar um sistema informático ou parte deste, ou um suporte de armazenamento de dados informáticos;
   b) Efectuar e conservar uma cópia de tais dados informáticos;
   c) Preservar a integridade dos dados informáticos pertinentes armazenados;
   d) Tornar inacessíveis ou remover tais dados informáticos do sistema informático acedido.

4. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados

informáticos nele contidos , que forneça todas as informações razoavelmente necessárias para permitir a aplicação das medidas previstas nos n.ºs 1 e 2 do presente artigo.

5. Os poderes e procedimentos referidos no presente artigo deverão estar sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

Título 5 – Recolha, em tempo real, de dados informáticos

Artigo 20º - Recolha, em tempo real, de dados informáticos relativos ao tráfego

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a:
   a) Recolher ou registar, através da aplicação dos meios técnicos existentes no seu território; e
   b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica, a:
      i. recolher ou registar, através da aplicação dos meios técnicos existentes no seu território, ou
      ii. prestar às autoridades competentes o seu apoio e a sua assistência na recolha ou no registo, em tempo real, dos dados relativos ao tráfego associados a comunicações específicas transmitidas no seu território através de um sistema informático.

2. Sempre que uma Parte, por força dos princípios estabelecidos na sua ordem jurídica, não possa adoptar as medidas enunciadas na al. a) do n.º 1 do presente artigo, poderá, em alternativa, adoptar as medidas legislativas e outras que se mostrem necessárias para garantir a recolha ou o registo, em tempo real, dos dados relativos ao tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos efectivos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para obrigar um fornecedor de serviços a manter em sigilo o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como sobre qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo deverão ser sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

Artigo 21º - Intercepção de dados relativos ao conteúdo

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes, relativamente a um conjunto de infracções graves a definir no âmbito do seu direito interno, a:
   a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território;
   b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica, a:
      i. recolher ou registar, através da aplicação dos meios técnicos existentes no seu território, ou
      ii. prestar às autoridades competentes o seu apoio e a sua assistência na recolha ou no registo, em tempo real, dos dados relativos ao conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático.

2. Quando uma Parte, por força dos princípios estabelecidos no seu direito interno, não puder adoptar as medidas enunciadas na al. a) do n.º 1 do presente artigo, poderá, em alternativa, adoptar as medidas legislativas e outras que se mostrem necessárias para assegurar a recolha ou o registo, em tempo real, dos dados relativos ao conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para obrigar um fornecedor de serviços a manter em sigilo o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo deverão ser sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

Secção 3 - Competência

Artigo 22º - Competência

1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para estabelecer a sua competência relativamente à prática de qualquer infracção penal prevista nos artigos 2º a 11º da presente Convenção, sempre que a infracção for cometida:
    a) no seu território; ou
    b) a bordo de um navio arvorando o pavilhão dessa Parte;
    c) a bordo de uma aeronave matriculada nessa Parte e segundo as suas leis;
    d) por um dos seus cidadãos nacionais, caso a infracção seja criminalmente punível no lugar onde foi praticada ou não for da competência territorial de qualquer Estado .

2. Cada Parte poderá reservar-se o direito de não aplicar, ou de apenas aplicar em casos e condições específicas, as regras de competência definidas nas als. b) a d) do n.º 1 do presente artigo ou em qualquer parte dessas alíneas.

3. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para estabelecer a sua competência relativamente à prática de qualquer uma das infracções referidas no n.º 1 do artigo 24º da presente Convenção, sempre que o presumível autor da infracção se encontrar no seu território e não possa ser extraditado para outra Parte com base na sua nacionalidade, após um pedido de extradição.

4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.

5. Quando mais que uma Parte reivindicar a competência relativamente a uma presumível infracção prevista na presente Convenção, as Partes interessadas consultar-se-ão, se tal se mostrar oportuno, por forma a decidir qual a jurisdição mais apropriada para instaurar o procedimento criminal.

<u>Capítulo III – Cooperação internacional</u>

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Artigo 23º - Princípios gerais relativos à cooperação internacional

As Partes cooperarão entre si, em conformidade com o disposto no presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas e dos respectivos direitos internos, na medida mais ampla possível, para efeitos de investigação ou procedimento relativamente a infracções penais relacionadas com sistemas e dados informáticos, ou para recolha de provas sob a forma electrónica relativamente à prática de uma infracção penal.

Título 2 – Princípios relativos à extradição

Artigo 24º - Extradição

1.a) O presente artigo é aplicável à extradição entre as Partes relativamente às infracções penais previstas nos artigos 2º a 11º da presente Convenção, desde que sejam puníveis, nos termos da legislação das duas Partes interessadas, com pena privativa de liberdade por um período máximo de, pelo menos, um ano ou com uma pena mais grave;

b) Quando for exigida uma pena mínima diferente, nos termos de um tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE n.º 24), ou num convénio celebrado com base em legislações uniformes ou recíprocas, será aplicável a pena mínima prevista nesse tratado ou convénio.

2. As infracções penais descritas no n.º 1 do presente artigo serão consideradas como infracções passíveis de extradição previstas em qualquer tratado de extradição existente entre duas ou mais Partes. As Partes comprometem-se a incluir tais infracções em qualquer tratado de extradição a celebrar entre si como infracções passíveis de extradição.

3. Sempre que uma Parte condicionar a extradição à existência de um tratado e receber um pedido de extradição de outra Parte com a qual não tenha celebrado qualquer tratado de extradição, poderá considerar a presente Convenção como base jurídica para a extradição relativamente a qualquer infracção penal referida no n.º 1 do presente artigo.

4. As Partes que não condicionem a extradição à existência de um tratado reconhecerão, entre si, as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição.

5. A extradição ficará sujeita às condições previstas no direito interno da Parte requerida ou nos tratados de extradição aplicáveis, incluindo os fundamentos de recusa da extradição pela Parte requerida.

6. Se a extradição por uma infracção penal referida no n.º 1 do presente artigo for recusada unicamente com base na nacionalidade da pessoa reclamada ou porque a Parte requerida se considera competente relativamente a essa infracção, a Parte requerida remeterá o processo, a pedido da Parte requerente, às suas autoridades competentes para fins de procedimento criminal e informará a Parte requerente, em tempo útil, do resultado do processo. As autoridades em causa tomarão a sua decisão e conduzirão a investigação e o procedimento do mesmo modo que em relação a qualquer outra infracção de natureza comparável, em conformidade com a legislação da Parte requerida.

7-a) Em caso de ausência de tratado, cada Parte comunicará ao Secretário-Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, o nome e a morada de cada autoridade responsável pelo envio ou pela recepção de um pedido de extradição ou de prisão preventiva;

b) O Secretário-Geral do Conselho da Europa criará ou manterá actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deverá assegurar a constante actualização dos dados constantes do registo.

Título 3 – Princípios gerais relativos ao auxílio mútuo

Artigo 25º - Princípios gerais relativos ao auxílio mútuo

1. As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativamente a infracções penais relacionadas com sistemas e dados informáticos , ou para efeitos de recolha de provas sob a forma electrónica relativamente a uma infracção penal.

2. Cada Parte adoptará, igualmente, as medidas legislativas e outras que se mostrem necessárias para cumprir as obrigações enunciadas nos artigos 27º a 35º.

3. Cada Parte poderá, em caso de urgência, submeter um pedido de auxílio mútuo ou as comunicações conexas, através de meios de comunicação rápidos, tais como o fax ou o correio electrónico, desde que tais meios ofereçam condições suficientes de segurança e autenticação (incluindo a encriptação, se necessário), com confirmação oficial posterior se o Estado requerido o exigir. O Estado requerido aceitará o pedido e responderá através de qualquer um desses meios de comunicação rápidos.

4. Salvo disposição expressa em contrário prevista nos artigos que se seguem do presente Capítulo, o auxílio mútuo ficará sujeito às condições fixadas no direito 22interno da Parte requerida ou em tratados de auxílio mútuo aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar o cooperação. A Parte requerida não deverá exercer o seu direito de recusa de auxílio mútuo relativamente às infracções previstas nos artigos 2º a 11º baseada apenas no fundamento de que o pedido visa uma infracção que considera ser de natureza fiscal.

5. Sempre que, em conformidade com o disposto no presente Capítulo, a Parte requerida estiver autorizada a subordinar o auxílio mútuo à existência de dupla incriminação, esta condição será considerada preenchida se os actos constitutivos da infracção, relativamente à qual o auxílio mútuo é requerido, forem tipificados como infracção penal pelo direito interno dessa Parte, quer o seu direito interno classifique ou não a infracção na mesma categoria de infracções prevista no direito interno da Parte requerente, ou a designe ou não segundo a mesma terminologia.

Artigo 26º - Informação espontânea

1. Qualquer Parte poderá, dentro dos limites previstos no seu direito interno e não se verificando existência de um pedido prévio, comunicar a outra Parte informações obtidas no quadro das suas próprias investigações, sempre que considerar que tal poderá ajudar a Parte destinatária a iniciar ou a efectuar investigações ou procedimentos por força da prática de infracções penais previstas na presente Convenção, ou sempre que tais

informações possam originar um pedido formulado por essa Parte nos termos do presente Capítulo.

2. Antes de comunicar tais informações, a Parte que as fornecer poderá solicitar que permaneçam confidenciais ou que só sejam utilizadas sob determinadas condições. Se a Parte destinatária não puder dar satisfação a tal pedido, deverá informar a outra Parte de tal facto, a qual deverá, então, determinar se as informações em causa deverão, não obstante, ser fornecidas. Se a Parte destinatária aceitar as informações nas condições estipuladas, tal Parte ficará vinculada por elas.

Título 4 – Procedimentos relativos a pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis

Artigo 27º - Procedimentos relativos aos pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis

1. Na falta de tratado de auxílio mútuo ou de convénio baseado nas legislações uniformes ou recíprocas em vigor entre a Parte requerente e a Parte requerida, será aplicável o disposto nos n.ºs 2 a 9 do presente artigo. Tais disposições não serão aplicáveis caso se verifique a existência de um tratado, de um convénio ou de legislação desse tipo, excepto se as Partes envolvidas decidirem aplicar parte ou a totalidade do disposto no presente artigo, em sua substituição.

2.a) Cada Parte designará uma ou várias autoridades centrais encarregadas de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes para a sua execução;

b) As autoridades centrais comunicarão directamente entre si;

c) No momento da assinatura ou do depósito dos seus instrumentos de ratificação, aceitação, aprovação ou adesão, cada Parte comunicará ao Secretário-Geral do Conselho da Europa os nomes e as moradas das autoridades designadas em aplicação do presente número;

d) O Secretário-Geral do Conselho da Europa criará e manterá um registo actualizado das autoridades centrais designadas pelas Partes. Cada Parte assegurará, permanentemente, a exactidão dos dados constantes desse registo.

3. Os pedidos de auxílio mútuo referidos no presente artigo serão executados em conformidade com os procedimentos especificados pela Parte requerente, salvo se forem incompatíveis com a legislação da Parte requerida.

4. Além das condições ou dos motivos de recusa previstos no n.º 4 do artigo 25º, o auxílio mútuo poderá ser recusado pela Parte requerida se:
   a) O pedido respeitar a uma infracção que a Parte requerida entenda ser de natureza política ou conexa a uma infracção de natureza política; ou
   b) A Parte requerida entender que a satisfação do pedido poderá atentar contra a sua soberania, a sua segurança, a sua ordem pública ou contra outros interesses essenciais.

5. A Parte requerida poderá adiar a execução do pedido sempre que tal execução puder prejudicar investigações ou procedimentos conduzidos pelas suas autoridades.

6. Antes de recusar ou adiar a sua cooperação, a Parte requerida verificará, após ter consultado a Parte requerente, se for caso disso, se está em condições de satisfazer o pedido parcialmente ou sujeitá-lo às condições que entender necessárias.

7. A Parte requerida informará, rapidamente, a Parte requerente do seguimento que entender dar ao pedido de auxílio mútuo. Deverá fundamentar a sua eventual recusa ou o eventual adiamento de execução do pedido. A Parte requerida informará, igualmente, a Parte requerente de quaisquer motivos que tornem impossível a execução do auxílio mútuo ou o retardem de forma significativa.

8. A Parte requerente poderá solicitar à Parte requerida que mantenha confidenciais o facto e o objecto de qualquer pedido submetido nos termos do presente Capítulo, excepto na medida necessária à sua execução. Caso não possa satisfazer o pedido de confidencialidade, a Parte requerida deverá informar a Parte requerente com celeridade, a qual decidirá se, ainda assim, o pedido deverá ser executado.

9.a) Em caso de urgência, as autoridades judiciárias da Parte requerente poderão dirigir os pedidos de auxílio mútuo ou as comunicações a eles conexas às suas homólogas da

Parte requerida. Nesses casos, será dirigida, em simultâneo, uma cópia às autoridades centrais da Parte requerida através da autoridade central da Parte requerente.

b) Qualquer pedido ou comunicação feito nos termos do presente número poderá ser efectuado por intermédio da Organização Internacional de Polícia Criminal (Interpol).

c) Caso um pedido tenha sido efectuado em aplicação da alínea a) do presente número e a autoridade não for competente para dele conhecer, tal autoridade transmiti-lo-á à autoridade nacional competente e informará directamente a Parte requerente de tal facto.

d) Os pedidos ou as comunicações efectuados em aplicação do disposto no presente número, que não impliquem uma acção coerciva, poderão ser directamente transmitidos pelas autoridades competentes da Parte requerente às autoridades competentes da Parte requerida.

e) No momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, cada Parte poderá informar o Secretário-Geral do Conselho da Europa de que, por razões de eficácia, os pedidos feitos nos termos do presente número deverão ser dirigidos à sua autoridade central.

Artigo 28.º - Confidencialidade e restrição de utilização

1. Na falta de um tratado de auxúlio mútuo ou de um convénio com base nas legislações uniformes ou recíprocas vigentes entre a Parte requerente e a Parte requerida, será aplicável o disposto no presente artigo. Tais disposições não serão aplicáveis quando exista um tratado, um convénio ou legislação desse tipo, excepto se as Partes envolvidas decidirem aplicar, em sua substituição, o presente artigo, no todo ou em parte.

2. A Parte requerida poderá efectuar a comunicação de informações ou de material em resposta a um pedido sob condição de que:
   a) Tais informações e material permaneçam confidenciais, não podendo o pedido de auxílio mútuo ser satisfeito na ausência de tal condição, ou
   b) Tais informações e material não sejam utilizados para fins de investigações ou procedimentos diferentes dos indicados no pedido.

3. Se a Parte requerente não puder satisfazer uma das condições enunciadas no n.º 2 do presente artigo, informará, prontamente, a Parte requerida, a qual determinará se a

informação deve, ainda assim, ser transmitida. Se aceitar tal condição, a Parte requerente ficará vinculada pela mesma.

4. Qualquer Parte que forneça informações ou material sujeitos a uma das condições enunciadas no n.º 2 do presente artigo poderá exigir que a outra Parte lhe comunique elementos pormenorizados relativamente à utilização dada às informações ou ao material em causa.

Secção 2 – Disposições específicas

Título 1 – Auxílio mútuo em matéria de medidas provisórias

Artigo 29.º - Conservação expedita de dados informáticos armazenados

1. Uma Parte poderá solicitar a outra Parte que ordene ou, de outro modo, imponha a conservação rápida de dados armazenados através de um sistema informático que se encontre no território dessa outra Parte, e relativamente aos quais a Parte requerente pretenda efectuar um pedido de auxílio mútuo com vista à busca ou ao acesso por meio similar, à apreensão ou à obtenção por meio similar, ou à divulgação dos referidos dados.

2. Um pedido de conservação feito em aplicação do disposto no n.º 1 do presente artigo deverá especificar:
    a) A autoridade que solicita a conservação;
    b) A infracção que é objecto da investigação, bem como um resumo dos factos a ela conexos;
    c) Os dados informáticos armazenados a conservar e a natureza da sua relação com a infracção;
    d) todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;
    e) a necessidade da medida de conservação; e
    f) o facto de que a Parte pretende submeter um pedido de auxílio com vista à busca ou ao acesso através de um meio similar, à apreensão ou à obtenção por meio similar, ou á divulgação de dados informáticos armazenados.

3. Após ter recebido o pedido de outra Parte, a Parte requerida deverá tomar todas as medidas apropriadas de modo a proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para efeitos de resposta a um tal pedido, a dupla incriminação não será exigida como condição prévia à conservação.

4. Uma Parte que exiga a dupla incriminação como condição para responder a um pedido de auxílio mútuo visando a busca ou o acesso similar, a apreensão ou a obtenção por meio similar, ou a divulgação dos dados, poderá, relativamente a infracções diferentes das estabelecidas em conformidade com o disposto nos artigos 2º a 11º da presente Convenção, reservar-se o direito de recusar o pedido de conservação nos termos do presente artigo nos casos em que tenha motivos para crer que, no momento da divulgação, a condição de dupla incriminação não poderá ser observada.

5. Além disso, um pedido de conservação só poderá ser recusado se:
   a) o pedido respeitar a uma infracção que a Parte requerida entenda ser de natureza política ou com ela conexa;
   b) a Parte requerida considerar que a execução do pedido poderá atentar contra a sua soberania, a sua segurança, a ordem pública ou outros interesses essenciais.
6. Quando uma Parte requerida considerar que a conservação simples não será suficiente para garantir a futura disponibilidade dos dados ou que poderá comprometer a confidencialidade das investigações efectuadas pela Parte requerente ou prejudicá-la de outro modo, a Parte requerida informará rapidamente a Parte requerente, a qual decidirá se, não obstante, deverá executar o pedido.

7. Qualquer conservação efectuada em resposta a um pedido previsto no n.º 1 do presente artigo será válida por um período não inferior a 60 dias, de modo a permitir que a Parte requerente submeta um pedido com vista à busca ou ao acesso por meio similar, à apreensão ou à obtenção por meio similar, ou à divulgação dos dados. Após a recepção de um tal pedido, os dados deverão continuar a ser conservados aguardando a adopção de uma decisão relativa ao pedido.

Artigo 30.º - Divulgação expedita de dados de tráfego conservados

1. Sempre que, ao executar um pedido de conservação de dados relativos ao tráfego relacionado com uma comunicação específica formulada em aplicação do artigo 29.º, a Parte requerida descobrir que um fornecedor de serviços noutro Estado participou na transmissão dessa informação, a Parte requerida divulgará, de forma expedita, à Parte requerente uma quantidade suficiente de dados relativos ao tráfego, para fins de identificação de tal fornecedor de serviços e a via através da qual a comunicação foi transmitida.

2. A divulgação de dados relativos ao tráfego em aplicação do disposto no n.º 1 do presente artigo só poderá ser recusada se:
   a) o pedido respeitar uma infracção que a Parte requerida considerar de natureza política ou a uma infracção conexa; ou
   b) considerar que o cumprimento do pedido poderá atentar contra a sua soberania, segurança, ordem pública ou outros interesses essenciais.

Título 2 – Auxílio mútuo relativamente aos poderes de investigação

Artigo 31.º - Auxílio mútuo relativamente ao acesso a dados informáticos armazenados

1. Uma Parte poderá solicitar a outra Parte que proceda à buscas ou aceda de modo similar, que apreenda ou obtenha de modo similar, e que divulgue dados armazenados através de um sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29.º.

2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, os convénios e a legislação referidos no artigo 23º e nos termos das disposições pertinentes constantes do presente Capítulo.

3. O pedido deverá ser satisfeito tão rapidamente quanto possível nos casos em que:
   a) existam motivos para crer que os dados relevantes são particularmente susceptíveis de perda ou modificação;
   b) os instrumentos, os convénios e a legislação previstos no n.º 2 do presente artigo prevejam uma cooperação célere.

Artigo 32.º - Acesso transfronteiriço aos dados informáticos armazenados, mediante consentimento ou quando sejam acessíveis ao público

Uma Parte poderá, sem autorização de outra Parte:

a) aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), independentemente da localização geográfica desses dados;

b) aceder a, ou receber, através de um sistema informático localizado no seu território, dados informáticos armazenados localizados no território de outra Parte, caso a Parte obtenha o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar-lhe tais dados através de tal sistema informático.

Artigo 33.º - Auxílio mútuo relativo à recolha, em tempo real, de dados de tráfego

1. As Partes providenciarão, entre si, auxílio mútuo relativo à recolha, em tempo real, de dados de tráfego associados a comunicações específicas transmitidas no seu território por meio de um sistema informático . Sem prejuizo do disposto no n.º 2 do presente artigo, o auxílio mútuo regular-se-á pelas condições e pelos procedimentos previstos em direito interno.

2. Cada Parte providenciará o auxílio pelo menos no que diz respeito às infracções penais relativamente às quais a recolha, em tempo real, de dados relativos ao tráfegos estaria disponível em casos internos similares.

Artigo 34.º - Auxílio mútuo em matéria de intercepção de dados relativos ao conteúdo

As Partes providenciarão auxílio mútuo, na medida permitida pelos tratados e pela legislação interna aplicáveis, relativamente à recolha ou ao registo, em tempo real, de dados relativos ao conteúdo de comunicações específicas transmitidas através de um sistema informático.

Título 3 – Rede 24/7

Artigo 35.º - Rede 24/7

1. Cada Parte designará um ponto de contacto disponível 24 horas por dia, sete dias por semana, por forma a assegurar uma assistência imediata às investigações e procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou à recolha de provas, sob a forma electrónica, da prática de infracções penais. O auxílio mútuo incluirá a facilitação ou, se o direito e a prática internos o permitirem, a aplicação directa das seguintes medidas:
   a) A prestação de aconselhamento técnico;
   b) A conservação de dados em conformidade com os artigos 29.º e 30.º;
   c) A recolha de provas, prestação de informações de natureza jurídica e localização de suspeitos.

2.a) O ponto de contacto de uma Parte terá a capacidade para se corresponder com o ponto de contacto de outra Parte de forma rápida.

b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou das autoridades dessa Parte responsáveis pela cooperação internacional ou pela extradição, o ponto de contacto assegurará que pode agir em coordenação com tal autoridade ou tais autoridades de forma célere.

3. Cada Parte assegurará a existência de pessoal formado e equipado para facilitar o funcionamento da rede.

Capítulo IV – Disposições finais

Artigo 36.º - Assinatura e entrada em vigor

1. A presente Convenção estará aberta à assinatura dos Estados membros do Conselho da Europa e dos Estados não membros que tenham participado na sua elaboração.

2. A presente Convenção ficará sujeita a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário-Geral do Conselho da Europa.

3. A presente Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data em que cinco Estados, incluindo, pelo menos, três Estados Membros do Conselho da Europa, tenham manifestado o seu consentimento em

ficarem vinculados pela presente Convenção, de acordo com o disposto nos nºs 1 e 2 do presente artigo.

4. Relativamente a qualquer Estado signatário que exprima posteriormente o seu consentimento em ficar vinculado à presente Convenção, esta entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data em que o Estado em causa tenha expresso o seu consentimento em ficar vinculado pela Convenção, nos termos do disposto nos n.ºs 1 e 2 do presente Artigo.

Artigo 37.º - Adesão à Convenção

1. Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa poderá, depois de ter consultado os Estados contratantes da Convenção e tendo obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão será tomada pela maioria prevista na alínea d) do artigo 20.º do Estatuto do Conselho da Europa e por unanimidade de votos dos representantes dos Estados com direito a assento no Comité de Ministros.

2. Relativamente a qualquer Esatdo aderente à presente Convenção nos termos do n.º 1 do presente artigo, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data do depósito do instrumento de adesão junto do Secretário-Geral do Conselho da Europa.

Artigo 38.º - Aplicação territorial

1. Qualquer Estado poderá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, especificar o território ou os territórios a que a presente Convenção será aplicável.

2. Qualquer Estado poderá, em qualquer momento posterior, mediante uma declaração dirigida ao Secretário-Geral do Conselho da Europa, tornar extensível a aplicação da presente Convenção a qualquer outro território especificado na declaração. A Convenção entrará em vigor, relativamente a talterritório, no primeiro dia do mês seguinte ao termo

de um período de três meses a contar da data de recepção de tal declaração pelo Secretário-Geral.

3. Qualquer declaração formulada nos termos dos dois números anteriores, relativamente a qualquer território especificado nessa declaração, poderá ser retirada mediante notificação dirigida ao Secretário-Geral. A retirada produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data de recepção de tal notificação pelo Secretário-Geral.

Artigo 39.º - Efeitos da Convenção

1. O objectivo da presente Convenção é o de complementar os tratados ou acordos multilaterais ou bilaterais aplicáveis existentes entre as Partes, incluindo as disposições:
   a. Da Convenção Europeia de Extradição, aberta à assinatura a 13 de Dezembro de 1957, em Paris (STE n.º 24);
   b. Da Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, aberta à assinatura a 20 de Abril de 1959, em Estrasburgo (STE n.º 30);
   c. Do Protocolo Adicional à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal, aberto à assinatura a 17 de Março de 1978, em Estrasburgo (STE n.º 99).

2. Se duas ou mais Partes tiveram já celebrado um acordo ou um tratado relativo às matérias tratadas pela presente Convenção ou se, de outro modo, tiverem estabelecido relações sobre tais matérias, ou se procederem desse modo futuramente, terão igualmente a possibilidade de aplicar o referido acordo ou tratado ou estabelecer essas relações em substituição da presente Convenção. Contudo, sempre que as Partes estabeleçam relações respeitantes a matérias objecto da presente Convenção de modo diferente do previsto na presente Convenção, fa-lo-ão de uma forma que não seja incompatível com os objectivos e os princípios da Convenção.

3. Nada na presente Convenção afectará outros direitos, restrições, obrigações e responsabilidades de uma Parte.

Artigo 40.º - Declarações

Mediante declaração escrita dirigida ao Secretário-Geral do Conselho da Europa, qualquer Estado poderá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que se reserva o direito de exigir, se for caso disso, um ou mais elementos adicionais tal como vem previsto nos artigos 2.º, 3.º, alínea b) do n.º 1 do artigo 6.º, 7.º, n.º 3 do artigo 9.º e alínea e) do n.º 9 do artigo 27.º.

Artigo 41.º - Cláusula federal

1. Um Estado federal poderá reservar-se o direito de assumir as obrigações decorrentes do disposto no Capítulo II da presente Convenção na medida em que tais obrigações sejam compatíveis com os princípios fundamentais que governam as relações entre o seu governo central e os Estados federados ou outras entidades territoriais análogas, desde que se encontre em condições de cooperar com base no Capítulo III.

2. Sempre que efectuar a reserva prevista no n.º 1, um Estado federal não poderá utilizar os termos de tal reserva para excluir ou diminuir de forma substancial as suas obrigações nos termos do Capítulo II. Em qualquer caso, o Estado em causa dotar-se-á de meios amplos e eficazes que permitam a implementação das medidas previstas no referido capítulo.

3. Relativamente ao disposto na presente Convenção, cuja aplicação seja da competência legislativa de cada um dos Estados federados ou de outras entidades territoriais análogas que, por força do sistema constitucional da federação, não sejam obrigados a empreender medidas legislativas, o governo federal dará conhecimento, mediante parecer favorável, das referidas disposições às autoridades competentes dos Estados federados, encorajando-os a adoptar as medidas adequadas para a sua execução.

Artigo 42.º - Reservas

Mediante notificação escrita dirigida ao secretário-Geral do Conselho da Europa, qualquer Estado poderá, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que se fará prevalecer da reserva ou das reservas previstas no n.º2 do artigo 4.º, n.º 3 do artigo 6.º , n.º 4 do artigo 9.º, n.º 3 do artigo 10.º, n.º 3

do artigo 11.º, n.º 3 do artigo 14.º, n.º 2 do artigo 22.º, n.º 4 do artigo 29.º, e n.º 1 do artigo 41.º. Nenhuma outra reserva poderá ser formulada.

Artigo 43.º - Estatuto e retirada de reservas

1. Uma Parte que tenha formulado uma reserva nos termos do artigo 42º da presente Convenção, poderá retirar tal reserva, no todo ou em parte, mediante notificação dirigida ao Secretário-Geral do Conselho da Europa. Tal retirada produzirá efeitos à data da recepção da referida notificação pelo SecretárioGeral. Se a notificação mencionar que a retirada de uma reserva deverá produzir efeitos numa determinada data, e se tal data for posterior àquela em que o Secretário-Geral receber a notificação, a retirada produzirá efeitos nessa data posterior.

2. Uma Parte que tenha feito uma reserva prevista no artigo 42.º, retirará tal reserva, no todo ou em parte, desde que as circunstâncias o permitam.

3. O Secretário-Geral do Conselho da Europa poderá, periodicamente, solicitar às Partes que tenham feito uma ou mais reservas previstas no artigo 42.º informação sobre as perspectivas da respectiva retirada.

Artigo 44º - Emendas

1. Qualquer Parte poderá propor emendas à presente Convenção, que serão comunicadas pelo Secretário-Geral do Conselho da Europa aos Estados membros do Conselho da Europa, aos Estados não membros que tenham participado na elaboração da presente Convenção, bem como a qualquer Estado que a ela tenha aderido ou tenha sido convidado a aderir nos termos do seu artigo 37º.

2. Qualquer emenda proposta por uma Parte será comunicada ao Comité Europeu para os Problemas Criminais (‘CDPC’), o qual submeterá o seu parecer sobre a referida alteração ao Comité de Ministros.

3. O Comité de Ministros examinará a emenda proposta e o parecer submetido pelo Comité Europeu para os Problemas Criminais (‘CDPC’) e, após consulta com os Estados não membros Partes na presente Convenção, poderá adoptar a referida alteração.

4. O texto de qualquer emenda adoptada pelo Comité de Ministros em conformidade com o n.º 3 do presente artigo será comunicado às Partes após aceitação.

5. Qualquer emenda adoptada em conformidade com o n.º 3 do presente artigo entrará em vigor no trigésimo dia a contar da data em que todas as Partes tenham informado o Secretário-Geral da sua aceitação.

Artigo 45.º - Resolução de litígios

1. O Comité Europeu para os Problemas Criminais do Conselho da Europa será mantido informado sobre a interpretação e a aplicação da presente Convenção.

2. Em caso de litígio entre as Partes sobre a interpretação ou a aplicação da presente Convenção, aquelas esforçar-se-ão por resolver o litígio por meio de negociação ou qualquer outro meio pacífico à sua escolha, incluindo a submissão do litígio ao Comité Europeu para os Problemas Criminais, a um tribunal arbitral cujas decisões vinculem as Partes no litígio, ou ao Tribunal Internacional de Justiça, segundo acordo comum entre as Partes interessadas.

Artigo 46.º - Consultas entre as Partes

1. As Partes consultar-se-ão periodicamente, se necessário, a fim de facilitar:
   a) o uso e a implementação efectivos da presente Convenção, incluindo a identificação de qualquer problema na matéria, bem como os efeitos de qualquer declaração ou reserva formulada nos termos da presente Convenção;
   b) a troca de informações sobre os desenvolvimentos jurídicos, políticos ou técnicos significativos verificados no domínio da criminalidade informática e da recolha de provas sob a forma electrónica;
   c) a apreciação sobre eventuais complementos ou emendas à presente Convenção.

2. O Comité Europeu para os Problemas Criminais (CDPC) será periodicamente informado do resultado das consultas referidas no n.º 1 do presente artigo.

3. O Comité Europeu para os Problemas Criminais (CDPC) facilitará, se necessário, as consultas referidas no n.º 1 do presente artigo e adoptará as medidas necessárias para auxiliar as Partes no seu esforço de complementar ou alterar a presente Convenção. O mais tardar findo um prazo de três anos a contar da entrada em vigor da presente Convenção, o Comité Europeu para os Problemas Criminais (CDPC) procederá, em cooperação com as partes, a uma reapreciação das disposições da presente Convenção e proporá, se for caso disso, as emendas adequadas.

4. Salvo se o Conselho da Europa as tomar a seu cargo, as despesas ocasionadas pela aplicação do disposto no n.º 1 do presente artigo serão suportadas pelas Partes segundo a forma que entendam adequada.

5. As Partes serão assistidas pelo Secretariado do Conselho da Europa no exercício das suas funções decorrentes do presente artigo.

Artigo 47.º - Denúncia

1. Qualquer Parte poderá, a todo o momento, denunciar a presente Convenção mediante notificação dirigida ao Secretário-Geral do Conselho da Europa.

2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data de recepção da notificação pelo Secretário-Geral. 37

Artigo 48º - Notificação

O Secretário-Geral do Conselho da Europa notificará os Estados membros do Conselho da Europa, os Estados não membros que tenham participado na elaboração da presente Convenção e qualquer Estado que a ela tenha aderido ou tenha sido convidado a aderir de:

a) Qualquer assinatura;
b) Do depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;

c) De qualquer data de entrada em vigor da presente Convenção em conformidade com os seus artigos 36.º e 37.º;
d) De qualquer declaração feita em aplicação do disposto no artigo 40.º, ou de qualquer reserva feita em aplicação do artigo 42.º;
e) De qualquer outro acto, notificação ou comunicação relacionados com a presente Convenção.

Em fé do que, os abaixo assinados, devidamente autorizados para o efeito, assinaram a presente Convenção.

Feito em Budapeste, a 23 de Novembro de 2001, em francês e inglês, fazendo ambos os textos igualmente fé, num único exemplar que será depositado nos arquivos do Conselho da Europa. O Secretário-Geral do Conselho da Europa transmitirá cópias autenticadas a cada um dos Estados Membros do Conselho da Europa, aos Estados não Membros que tenham participado na elaboração da presente Convenção e a qualquer Estado convidado a ela aderir.

Fonte: UNIÃO EUROPEIA, Convenção sobre o cibercrime, 2013.