ORDEM DOS ADVOGADOS DO BRASIL
Comitê sobre Crimes Eletrônicos

CORIOLANO AURÉLIO DE ALMEIDA CAMARGO SANTOS

Presidente do Comitê sobre Crimes Eletrônicos da OAB SP.

As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico

"A CULTURA
É UM DIREITO"

São Paulo
2009

HOMENAGEM

Este primeiro Livro no ambiente virtual sobre Crimes Eletrônicos está à disposição de todos os Advogados, estudantes e pesquisadores e da sociedade no Portal da Ordem dos Advogados do Brasil Secção de São Paulo. O objetivo é baratear e simplificar os estudos dos Colegas e pesquisadores do tema.

Este espírito de solidariedade e de vanguarda é a espinha dorsal e marca da Gestão do **Presidente Luis Flávio Borges D´Urso** frente a Ordem dos Advogados do Brasil Secção de São Paulo. Ao nosso querido Presidente rendo as minhas homenagens e expresso meus cumprimentos pelos inúmeros trabalhos realizados na era do Direito na Sociedade da Informação. Nesta luta face às ameaças no ambiente virtual, peço licença para reproduzir a palavras de nosso Presidente. É o que segue:

- ✓ **"A internet tem servido aos criminosos para alcançar suas vítimas. Precisamos alertar os pais para que monitorem seus filhos, verifiquem como eles usam a rede, e os protejam. A informação é um importante instrumento de combate à pedofilia"**

- ✓ **"É preciso investir fortemente no desenvolvimento de novas tecnologias capazes de localizar as pessoas que produzem e consomem material pornográfico, assim como é preciso investir no treinamento de equipes policiais especializadas no combate à pedofilia", avalia Luiz Flávio Borges D'Urso, presidente da OAB SP.**

Agradeço a Deus, por iluminar o meu caminho com sua presença em todos os momentos. Agradeço a Deus pela oportunidade de ser Pai e por ter me agraciado em 2008 com a vinda de meus filhos gêmeos: Marco Aurélio e Cesar Augusto.

Agradeço a minha esposa Ana Paula por seu apoio e compreensão durante o tempo que estive ausente estudando.

Agradeço a minha Avó Vera Almeida Bueno de Camargo, quarenta anos dedicados à Educação, pelo carinho e apoio durante toda a minha vida.

Agradeço e rendo homenagens a meu orientador no Mestrado o Desembargador e Diretor da Escola Paulista da Magistratura, sua Excelência Dr. Antônio Rulli Júnior pelos ensinamentos e pela honra de ser seu aluno e orientando.

Resumo

Este trabalho tem por objetivo mostrar algumas questões que os novos adventos tecnológicos suscitam ao Direito ao ponto de inaugurar uma nova vertente de estudos, o Direito da Sociedade de Informação. Dentre as novidades que a era digital traz para a sociedade estão os crimes eletrônicos, ou crimes tecnológicos, que lesam cidadãos e governos e que não estão ainda suficientemente estudados ou têm punições adequadas previstas pelas leis. Discutem-se fatos ilícitos ocorridos nas duas últimas décadas (1990/2000) por conta da nova organização da sociedade em torno da tecnologia da informação. Abordam-se pontos polêmicos do Direito da Sociedade da Informação a partir do conceito de Segurança da Informação, associando-o a toda uma logística operacional que envolve custos que vão desde a previsão de contingências até o desenvolvimento de mecanismos preventivos e até mesmo à elaboração de métodos para impressão de elementos de prova em papel. Em relação aos cibercrimes, aponta-se uma preocupação que os governos devem ter ao implementar novas ferramentas de automação de controles fiscais como a nota fiscal eletrônica e o sistema público de escrituração digital. Pretende-se mostrar algumas fragilidades produzidas na sociedade por causa de tais avanços digitais e sugerir como a segurança da informação, bastante investigada por empresas e governos estrangeiros, precisa estar na pauta principal da implantação desses novos controles da conjunção de projetos públicos e privados em meio a redes de crime cibernético organizado.

PALAVRA-CHAVE: Direito; Direito Digital; Direito da Sociedade da Informação; Cibercrimes; Nota Fiscal Eletrônica.

Abstract

The aim of this work is to bring to light some questions that the new technological happenings have brought to the studies of Law, to the point of establishing inside it a new discipline, the Information Society Law. Among the new facts that this new era brings along are cybercrimes, or technological crimes, that cause harm to the society and its citizens and that are not yet sufficiently studied or have penalties established by law. This work brings to discussion illicit facts that take place in the last two decades (1990/2000) due to the new organization of society around Information Technology. It broaches polemic points inside Information Society from the concept of Information Security linking it to the logistics of operations that involves costs of preventing and developing contingencies and the elaboration of methods of printing documents in safe paper. Regarding cybercrimes, it intends to point out some concerns that governments should have related to electronic coupons and the public system of digital entries. It also intends to point out some fragilities produced due to such digital happenings and suggest how Information Security, as already investigated by business companies and foreign governments, has to be in the main list of concerns and discussions of implementing these new controlling systems that are taking place inside a society where organized crime is present.

Keywords: Law; Digital Law; Information Society Law; Cybercrimes; Electronic Coupons.

Sumário

0. Introdução

Com a globalização e a evolução tecnológica, a troca de informações passa a ser feita em tempo real, fundando a Era Digital e gerando novos tipos de preocupações. Com o advento da Internet e a realidade da era digital e on-line, indispensável é a adequação do Direito, que necessita afiar seus instrumentos e lançar luzes sobre as novas relações sociais que se delineiam, pois, juntamente com a evolução tecnológica, inaugura-se a era de crimes virtuais. O Direito da Sociedade da Informação, nova vertente do Direito que se relaciona intimamente com a era de evolução tecnológica que ora se apresenta, tem relação estreita com os fenômenos e processos de pesquisas tecnológicas. Nesse patamar estão os crimes praticados por meio do uso de sofisticadas tecnologias. Estamos todos conectados e a informação se propaga em alta velocidade. Atualmente, tal é a evolução do uso da Internet que recentemente índios brasileiros usam-na preferencialmente ao arco e flecha para se defenderem. Grupos indígenas fizeram denúncias à Presidência da República sobre a invasão de madeireiros do Peru interessados no mogno das reservas indígenas via mensagem eletrônica em maio de 2008[1].

Crimes virtuais acontecem com grande freqüência. Portanto, a segurança da Informação é hoje um problema sério e contínuo enfrentado por centenas de países. Atualmente, criminosos utilizam ferramentas dotadas de alta tecnologia com poder imensurável de ação, seja para destruir dados, seja para capturar

[1] Conforme notícia veiculada no Jornal Nacional (Rede Globo de Televisão) em 26/05/2008, disponível no sítio http://jornalnacional.globo.com/Telejornais/JN/0,,MUL537286-10406,00-EMAIL+EVITA+GUERRA+NA+FRONTEIRA+DO+BRASIL+COM+PERU.html

informações sigilosas, extorquindo autoridades e governos. Na primeira parte deste trabalho de pesquisa pretende-se situar como o Direito da Sociedade da Informação procura compreender a nova realidade que se apresenta e como a Sociedade da Informação procura organizar-se e proteger-se por meio de normas de segurança estabelecidas em âmbito nacional e internacional.

A segunda parte deste trabalho de pesquisa procura examinar algumas condutas da rede de cibercriminosos em diversos países. São analisados os riscos envolvendo projetos de governo no Brasil com grande grau de dependência da utilização da internet e seu convívio presente e futuro como estas ameaças. Para tanto, foram analisadas as atuações de diversos grupos de inteligência no combate aos crimes de alta tecnologia e propagados por meio de sistemas de comunicação eletromecânicos. Trata-se do surgimento dos novos avanços tecnológicos e sociais, e o surgimento de novos núcleos criminosos que se utilizam como espinha dorsal de sofisticada tecnologia para maximizar resultados terroristas em diversos modelos. Relata-se a migração de facções criminosas brasileiras que atualmente enviam seus soldados para programas de treinamento em outros países, objetivando modernizar arsenal de crimes cibernéticos a patamares até hoje desconhecidos.

O comportamento das agremiações criminosas atualmente adota a estratégia de qualquer outra organização econômica. Ou seja, são organizados novos núcleos de atividade tecnológica para cometer ilícitos, objetivando minimizar suas perdas em outros setores da facção. Colheu-se o depoimento de diversas autoridades as quais informaram que no ano de 2008 a sofisticação dos crimes cibernéticos cresceu de modo exponencial.

Nesse cenário, foi a analisado o perfil do criminoso da era moderna, dotado de elevado grau de instrução, capaz de utilizar a Engenharia Social para levar usuários avançados a instalar programas espiões dentro de seus computadores. Analisam-se ainda nesta pesquisa alguns programas invasores, que estão cada vez mais inteligentes. Programas maliciosos são capazes de se auto-atualizar e executar varreduras inteligentes a procura somente de dados

sigilosos dotados de valor e também em busca de dados de cartões de crédito e contas bancárias.

As autoridades e pesquisadores brasileiros e de outros países mostram que os criminosos cibernéticos são dotados de alto grau de conhecimento. Para alguns usuários da internet entrevistados, a certificação digital e outros métodos de segurança não implicam atualmente em diferencial capaz de garantir a validade jurídica de identificação e a privacidade e inviolabilidade de dados, seja o usuário treinado ou não. Os ataques de programas “iscas” e arquivos “espiões” se sofisticam a tal ponto que mesmo usuários avançados têm dificuldade em reconhecer uma mensagem falsa ou verdadeira.

Na segunda parte deste trabalho abordam-se ainda os cibercrimes e as muitas proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, bem como na rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A informação e a disponibilidade da informação passam a ter um grande valor para empresas e governos. Cresce a cada dia a necessidade de proteção do capital intelectual e proteção da capacidade de gerar e receber informações. Nas empresas, nasce o conceito de que o capital humano deve ser mais protegido que outrora, uma vez que uma mensagem eletrônica mal intencionada pode comprometer a reputação de governos, Estados, empresas ou mercados. Nessa nova realidade, nasce uma nova cultura, a de que as políticas de segurança da informação cada vez mais são objeto de projetos críticos de sucesso de empresas privadas e de entidades públicas.

A presente pesquisa científica pretende investigar algumas das múltiplas faces dos crimes cibernéticos e por sua vez os crimes praticados por meio de avançadas ferramentas tecnológicas e seus reflexos no mundo Jurídico com o objetivo de demonstrar que os crimes cometidos com o uso da internet são uma

fonte de preocupação para a implantação de novas ferramentas de controle eletrônico do governo no Brasil. Na terceira parte deste trabalho, pretende-se remeter o leitor a uma reflexão científica e sistêmica da convivência de projetos empresariais e governamentais como a Nota Fiscal Eletrônica em meio a códigos sofisticados e maliciosos, que podem acarretar graves problemas legais, muitas vezes camuflados em meio ao arsenal de produtos e materiais ilegais oferecidos na Internet. Em tese, discute-se e reprova-se a idéia do surgimento de projetos de controle eletrônico como o Emissor de Cupom Fiscal e da Nota Fiscal Eletrônica como panacéia fiscal do Século XXI e frisa-se que o ataque de *botnets*[2] em larga escala tornará frágil o sistema de alimentação da base de dados do fisco e de contribuintes. Aspira-se sustentar que o desenvolvimento tecnológico sustentável requer investimento contínuo em segurança, que a eficácia de qualquer projeto de controle fiscal eletrônico representa grande avanço, contudo um dos grandes desafios será a criação de mecanismos ainda mais inteligentes para mitigar a ação de criminosos. Novos conceitos são propostos e trata-se de ponderar sobre a capacidade da Administração Fazendária Nacional e Regional e de empresas para superar e prever a sagacidade e disfarce de facções e organizações criminosas, cada vez mais perigosas e altamente especializadas no seqüestro, furto, adulteração, danificação, controle ou geração da perda proposital de informações confidenciais de empresas e governos.

[2] Botnet é um "exército" de Bots (uma rede de computadores infectados que podem ser controlados remotamente). Eles são controlados por piratas informáticos através de instruções em linha de comando ou, mais recentemente, programas com interfaces gráficas. Segundo a Trend Micro, estima-se que 10.000 computadores sejam diariamente transformados em "zombies" e recrutados para fazerem parte de BotNets. Disponível em: http://www.miudossegurosna.net/artigos/2006-02-17-bits&bytes.htm. Acesso em 17 fev.2006.

1. A Sociedade da Informação: Direito e Tecnologia.

Para o Dicionário Houaiss da Língua Portuguesa, Direito, no sentido de termo jurídico, pode ser entendido como o

> conjunto de normas da vida em sociedade que buscam expressar e também alcançar um ideal de justiça, traçando as fronteiras do ilegal e do obrigatório; ciência que estuda as regras de convivência na sociedade humana; jurisprudência

Sendo assim, ao se compreender o Direito como a ciência que rege e normaliza a vida no seio social, entende-se que com o advento da Tecnologia e todas as mudanças que ela tem trazido para o mundo, necessário seja estudar melhor a relação entre as duas ciências e os efeitos que a segunda tem sobre a primeira, com o intuito de alcançar o "ideal de justiça" e, se possível, de traçar as fronteiras do "ilegal e do obrigatório".

Sobre o conjunto de mutações sociais que ocorrem na era da revolução digital, afirma Aires José Rover (2004, p. 236):

> Transformações sociais levam a transformações no mundo do Direito. Estão na ordem do dia temas como contratos eletrônicos, assinatura digital, direitos autorais, tributação dos meios eletrônicos, informática jurídica, urna eletrônica, direito de acesso, governo eletrônico... uma infinidade de novos conceitos e neologismos é incorporada ao cotidiano das relações sociais, comerciais e jurídicas: e-mail, e-business, e-gov, ciberespaço, portal, chats ou download.

Uma das transformações relevantes ocorridas ultimamente foi a criação da Nota Fiscal Eletrônica – NF-e – em vigor desde setembro de 2006 nos Estados de Goiás, Rio Grande do Sul, São Paulo, Bahia, Maranhão e Santa Catarina e que substitui notas fiscais impressas modelos 1 e 1A. Trata-se de um instituto

oficial de fiscalização tributária originária de uma parceria entre o ENCAT (Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais) e a Receita Federal do Brasil e que tem por objetivo facilitar a arrecadação fiscal.

Um outro produto da combinação entre tecnologia e Direito é o Sistema Público de Escrituração Digital – SPED[3], um sistema em desenvolvimento pela empresa pública SERPRO - Serviço Federal de Processamento de Dados – composto por três módulos, Escrituração Contábil Digital, Escrituração Fiscal Digital e Nota Fiscal Eletrônica, que visa a promover a atuação integrada dos fiscos nas três esferas de governo (federal, estadual e municipal) e a uniformizar o processo de coleta de dados contábeis e fiscais, bem como tornar mais célere a identificação de ilícitos tributários, reduzindo assim custos e simplificando e agilizando processos.

Tais inovações trazem para o Direito da Sociedade da Informação um novo campo de análise, em que há muito a ser descoberto e pesquisado. Cada vez mais o Estado pretende obter informações fiscais integrais dos contribuintes em tempo real. Diante dessa nova realidade, o Direito da Sociedade da Informação é o ramo do Direito que tem maior relevância para seu estudo multidisciplinar e científico. A internet torna-se uma apreensão, para muitos, um objeto que inexiste, ou está dentro do mundo de percepções ligadas a esfera íntima e valorativa. Ela é captada pela sensibilidade pelas meditações da consciência imediata. De toda sorte pela multiplicidade de conceitos, novos fenômenos comportamentais que surgem com a mistura de internet e novas tecnologias, percebe-se que as percepções humanas são as mais variadas, buscando conceituar de uma forma esta nova realidade, ou nova era informacional.

O Direito da Sociedade da Informação reúne conceitos interdisciplinares capazes de se resvalarem por lógicas diferentes, com estudos diferentes, não ousando desejar obter todas as respostas, mas com a pretensão de talvez poder remeter o leitor a ampliar o número de indagações possíveis. Durante a pesquisa

---

[3] Tanto o SPED quanto a NF-e serão discutidos no decorrer deste trabalho.

procurar-se-a deixar claro o conceito de que a rapidez e a grandeza de movimentos processados pela internet muitas vezes tornam cidadãos e governos incapazes de conceber intelectualmente a magnitude dos danos que possa ser causados pelo uso criminoso da rede ou a potencialidade de seus benefícios.

1.1 - Segurança da Informação

A Segurança da Informação propõe discussão dentro do Direito em vários dos seus ramos. Para Dawel (2005, p. 16) um grande problema para o cumprimento da Política de Segurança da Informação está nas pessoas, uma vez que elas cumprem papel fundamental, ativo e central e nem sempre estão cientes disso. Em suas palavras:

> (...) as pessoas estão sempre esperando que alguém esteja fazendo alguma coisa de bom pela segurança da empresa. Entendem sua responsabilidade como limitada e de pequena relevância perante o todo. Se todos estiverem pensando assim, ninguém fará nada e quando acontecer um incidente, o espanto será geral.

Toda informação contida nos computadores ou em qualquer outro ambiente é de fundamental importância para uma empresa e por isso os profissionais devem se preocupar constantemente com a segurança da informação. Esta pode ser considerada muitas vezes como o elemento de maior importância para a sobrevivência de empresas públicas e privadas.

A sociedade carrega uma gama infinita de informações. Nesse sentido, ondas evolutivas trazidas pela tecnologia e baseada em redes de informação, possibilitaram a universalização do conhecimento gerido de forma instantânea. A dinamização do acesso a centros de pesquisa e a outros órgãos provocou mudanças das instituições públicas e privadas, levou diferentes campos da vida social e política a ganhar autonomia e racionalidades próprias, nem sempre congruentes entre si, abrindo para criminosos diversas possibilidades.

O pensamento social, inclusive o jurídico, está por seu lado atravessando uma fase de críticas, vendo-se os estudiosos de diversos campos científicos

obrigados a enfrentar o desafio de novos momentos de reflexão que até então não haviam imaginado. Não são os mais poderosos economicamente que vão sobreviver às inovações tecnológicas, mas aqueles que mais rapidamente se adaptarem às mudanças ou que forem capazes de enfrentar a realidade de que o manuseio das novas tecnologias deve caminhar de mãos dadas com a segurança da informação e os meios de prova mais sustentáveis.

A manutenção da segurança da informação requer investimentos contínuos, ou seja, é um projeto sem prazo para terminar. As ameaças evoluem e a segurança deve evoluir no mesmo passo dessas ameaças. Contudo, em muitas comunidades e governos, os investimentos nesse segmento são tratados como despesa supérflua e não prioritária.

Por seu papel fundamental na nova sociedade digital que se forma, a segurança da informação deve ser tratada com uma visão de investimento relevante e urgente, a fim de que se possa resguardar a informação de possíveis ameaças. Vis-à-vis, as vulnerabilidades, ameaças e riscos são constantes e podem ocorrer a qualquer momento. As empresas e os governos são alvos constantes de criminosos. Assim, caso algum ataque venha a ocorrer, dependendo da sua natureza ele poderá gerar um sério impacto na reputação da organização e em suas operações, gerando dispêndios e até paralisação dos negócios.

Vive-se hoje o que se convencionou chamar de era informacional, ou a sociedade da informação. Nesse meio, a informação é um ativo de grande valia, movendo mercados e mobilizando consciências e processos legislativos políticos e jurídicos. Aquele que mais rapidamente concentra uma gama de informações qualitativas diminui seus custos e tempo de transação, ganha vantagem competitiva, evitando gargalos na cadeia logística de operação sistêmica. Através de programas específicos, criminosos são capazes de ler a senha da assinatura eletrônica[4] dos juízes para os fins do processo judicial. Determinadas informações

[4] Assinatura eletrônica, para os objetivos colimados pelo processo judicial, abrange os seguintes elementos de identificação do usuário: a) assinatura digital, calcada em certificado digital emitido por autoridade certificadora credenciada na forma da lei; b) mediante cadastro do

podem ser tão importantes que o custo para manter sua integridade será menor que o custo de não dispor dela adequadamente. Ou seja, o investimento em segurança para nossos Tribunais é de alta relevância já que as ameaças e ataques estão ditando a política das instituições ao redor do globo.

A experiência das empresas é relevante ao Poder Judiciário. Para elas são concebidas diferentes análises de riscos, projetadas com base em estudos de profissionais de diversos setores para que seja possível fazer um planejamento ideal. Ou seja, a melhor estratégia é baseada nos resultados de todos os fatos conhecidos, assim determinando a melhor solução. A grande preocupação não está na construção dos melhores equipamentos e sistemas, mas sim o uso apropriado das informações de quem a detenha.

Tome-se como exemplo o caso da polícia japonesa que teve dados sigilosos de uma investigação divulgados porque um vírus atacou o computador pessoal de um de seus investigadores, que mantinha em seu poder informações confidenciais. Entre as informações divulgadas havia evidências coletadas em cenas de crimes e relatórios sobre investigações, além do nome de policiais envolvidos nos casos. Para um consultor de empresa de segurança citado na reportagem, chamado Graham Cluley

> Este incidente deve lembrar às empresas que elas precisam levar a questão da segurança a sério. Arquivar dados em computadores pessoais deixa as organizações bastante vulneráveis[5]

Trata-se de uma equação de pesos e medidas, onde surge o ROI (Retorno sobre o Investimento) que, segundo Marcos Sêmola (*apud* Darwel, 2005, p. 23-25):

> [...] é uma ferramenta antiga e velha conhecida dos empreendedores, investidores e executivos atentos ao mercado e às oportunidades. Construída através do cruzamento de dados reais relacionados a custos diretos, indiretos e intangíveis, com a projeção de investimentos obtêm-

---

usuário nas Páginas na Internet no Poder Judiciário, ou por outra forma que venha a ser disciplinada pelo Tribunal por ato administrativo de sua Presidência na conformidade do Regimento Interno. Definição cf.inc.II do par.2.°do art.1° da Lei 11.419/2006.

[5] disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u19727.shtml>, acesso em março de 2006.

> se um ótimo instrumento para nortear as ações desses executivos. [...]O ROI da segurança tem especialmente muitas respostas elucidativas que nos ajudam a reverter a velha imagem de despesa, convertendo-a em investimento e, diga-se de passagem, um ótimo investimento!

Por sua vez, Dawel (2005, p. 41), ao comentar sobre risco, define-o como sendo "[...] apenas uma forma de representar a probabilidade de algo acontecer. Trata-se de uma possibilidade. Portanto, pode ocorrer ou não".

Leis, decretos, medidas provisórias, normas, estão sendo criados pela justiça brasileira com o intuito de coibir os ataques às informações, dentro os quais podemos citar:

- Decreto n.º 3.505, de 13 de junho de 2000 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Decreto n.º 3.587, de 5 de setembro de 2000 que estabelece normas para a Infra-Estrutura e Chaves Públicas do Poder Executivo Federal – ICP-Gv.
- Lei n.º 8.159, de 8 de janeiro de 1991 que dispõe sobre a Política Nacional de Arquivos Públicos e Privados.
- Decreto n.º 3.865, de 13 de julho de 2001 que estabelece requisito para Contratação de Serviços de Certificação Digital pelos Órgãos Públicos Federais.
- Medida Provisória n. º2.200-2, de 24 de agosto de 2001, institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia.

A Internet não pode ser vista e propagada como um ambiente sem lei. É preciso existir muito mais do que um mínimo de controle legal sobre o tráfego de informações aliado à tecnologia para que ela seja segura. Entre os meios de segurança de tráfego de informações encontra-se a criptografia de mensagens. Trata-se de um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação por meio da cifragem de um texto a ser enviado. Enquanto em trânsito pela rede, a mensagem trafega em código desconhecido, que será

decifrado assim que chegar ao seu destinatário final. A criptografia assegura, por meio da utilização de uma chave pública e outra privada[6], a privacidade da informação, mantendo o conteúdo da mensagem oculto de qualquer um que não seja seu destinatário. Quando não é feita a criptografia do conteúdo de uma mensagem, qualquer pessoa pode ter acesso a ela porque o fundamental protocolo que transmite a informação que trafega pela rede chamado de TCP/IP. O TCP/IP - Protocolo de Controle de Transmissão/Protocolo Internet (Transmission Control Protocol/Internet Protocol) - encapsula as informações a serem transmitidas pela Internet. Acrescenta cabeçalhos utilizados para especificar os endereços dos computadores destinatários e remetentes, para dividir e remontar as informações em pequenos pacotes, para aumentar ou diminuir a velocidade de transmissão conforme a confirmação ou não dos pacotes recebidos. Para alguns pesquisadores que viveram o nascedouro da internet no Brasil e nos Estados Unidos, o protocolo não sofreu alterações substanciais em sua infra- estrutura básica e não foi gerado para prover alta performance em transações de dados sigilosos, sendo assim um meio vulnerável a transição de dados[7].

Dessa maneira, quando enviamos uma mensagem não encriptada[8] ela pode ser interceptada durante seu percursos por um terceiro que não seja seu

---

[6] O que é criptografia de chaves pública e privada? A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente. Disponível em: <http://www.htmlstaff.org/cartilhaseguranca/cartilha-03-privacidade.html#subsec1.2> Acesso em 31 maio 2008.

[7] Informação dada por Giovanni Casagrande, sócio-diretor da empresa Central de Domínio http://www.centraldedominio.com.br - fundador do primeiro provedor de acesso a internet no Estado de São Paulo a *Assat Net* e *Net Point*. Essa informação foi também confirmada peço professor Doutor Mauro Cansian da UNESP, no dia 8 de novembro de 2008 no encontro dos Grupos de Estudo do Comitê Gestor da Internet.

[8] O que é a encriptação? A encriptação é um meio para melhorar a segurança de uma mensagem ou arquivo através da codificação dos conteúdos, de modo a que só possam ser lidos por quem tenha a chave de encriptação adequada para os descodificar. Por exemplo, se comprar algo na Internet, as informações da transacção (tais como endereço, número de telefone e número de cartão de crédito) são geralmente encriptadas para que se mantenham seguras. Utilize a encriptação quando pretender um nível de protecção elevado para as informações. Disponível:

destinatário, que pode lê-la ou alterá-la. A idéia é que se encontre um sistema no qual as mensagens possam percorrer a rede de um modo seguro. Segundo o professor da Universidade de Brasília Pedro Rezende[9] em 70% dos casos de escolha de senha, esta cifragem pode ser quebrada por *crackers* (*hackers* criminosos), usando programas que aplicam ataques de dicionário em tais cifragens. E quando a senha for robusta, o atacante pode ser valer de programas chamados cavalos-de-tróia, amplamente difundidos no mundo do cibercrime e facilmente programáveis na linguagem da comunicação de processos do *Windows* (Vbscript), em uma linguagem de programação ativo no *Internet Explorer* ou no *Outlook*, para interceptarem do teclado a digitação da senha transmitindo-as ao atacante, até através de carona em conexões a sites suspeitos.

Os algoritmos[10] que executam a criptografia podem ser simétricos ou assimétricos. O primeiro é um tipo de chave mais simples onde o emissor e o receptor usam a mesma chave. O segundo já é mais complexo, pois se trabalha com duas chaves: pública e privada. Segundo Fleury (1998)

> se hoje temos computadores para criptografar dados e processar informações que antes eram impossíveis, os mesmos computadores são usados para quebrar algoritmos e descobrir a chave que foi usada. Uma chave com poucos caracteres é fácil de ser adivinhada, pode-se tentar algumas possibilidades até que se consegue chegar na chave certa. Portanto, quanto maior o número de caracteres (ou bytes - 1 byte = 8 bits) mais segura será uma chave.

É preciso que os Tribunais e o Governo brasileiro estejam atentos. Para alguns, fala-se na possível quebra da criptografia, mas muito se tem a estudar a respeito da matéria. Para o primeiro bloco de pesquisadores, o rompimento das chaves é tarefa quase impossível diante das diversas combinações a serem feitas

---

<http://windowshelp.microsoft.com/Windows/pt-PT/Help/f219e5c8-b97b-469a-8dc3-d1791fa6386c2070.mspx> Acesso 31 maio 2008.

[9] Disponível: <http://www.cic.unb.br/docentes/pedro/trabs/SBC.htm> Tipos mais simples de Fraude e Ofuscação do seu Risco

[10] seqüência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas (p.ex.: algoritmo para a extração de uma raiz cúbica) segundo o Dicionário Houaiss da Língua Portuguesa.

para se conseguir êxito. Outros pesquisadores se mostram mais céticos e acreditam que a criptografia pode ser quebrada com relativa facilidade.

Há uma modalidade usada de encriptação conhecida como assinatura digital, um código destinado a garantir que o remetente de uma mensagem é quem ele realmente diz ser ou que a mensagem original não foi alterada. Ou seja, trata-se de um código que confere validade à operação. As mensagens enviadas por e-mail passarão a ser enviadas com a assinatura do remetente e caso ocorra alguma alteração na mensagem original a assinatura será deformada.

A autoridade certificadora atualmente no Brasil é a ICP-Brasil, regulada pela medida provisória nº 2.200-2 de 24 de agosto de 2001, mencionada anteriormente, enuncia em seu Artigo 1º:

> Art. 1º - Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira[11] - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Trata-se de um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais. A ICP-Brasil foi criada pelo Governo Federal com a intenção de regulamentar as atividades de certificação digital no País, fornecer maior segurança nas transações eletrônicas e incentivar a utilização da Internet como meio para a realização de negócios.

Dadas as inovações tecnológicas que têm sido propostas e incorporadas pelo governo brasileiro, cabe ao Direito acompanhar essas mudanças tecnológicas e atentar-se às novas ameaças e realidades. Existem hoje no Direito conflitos que se colocam em função da tecnologia e para os quais a lei nem sempre está preparada para resolver. O Judiciário possui um papel fundamental para se lidar com essa nova realidade.

---

[11] Informações sobre a ICP-Brasil podem ser encontrada em um site do governo brasileiro: <https://www.icpbrasil.gov.br/> Acesso em novembro de 2008.

1.2 - Normas brasileiras de Segurança da Informação - NBR ISO/IEC 17799

A questão da segurança da informação está recebendo um tratamento destacado por parte das empresas, bem como no âmbito do Governo Federal. A Secretaria Executiva do Conselho de Defesa Nacional, órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República, instituiu pela Portaria nº. 31, de 22 de novembro de 2005 um Grupo de Trabalho, e pela Portaria nº. 5, de 20 de janeiro de 2006 designou seus membros, com o objetivo de definir e desenvolver Metodologia de Gerenciamento de Segurança de Sistemas de Informação para a Administração Pública Federal - APF e criar Normas, Padrões e Procedimentos a serem utilizados no âmbito da APF com relação ao Gerenciamento da Segurança dos Sistemas de Informação que servirão de parametrização para o Sistema de Controle Interno do Poder Executivo Federal quando da realização dos processos de auditoria e verificação. As empresas e o governo têm seguido a norma de segurança NBR ISO IEC 17799[12] que diz respeito à principal norma de implementação da Gestão em Segurança da Informação. Ela pode ser utilizada por empresas e órgãos públicos na geração de programas voltados a promover a segurança da informação.

A norma preconiza treinamento e adequação dos funcionários e servidores em relação à Política de Segurança para atingir plenamente o propósito que é a segurança dos ativos, ou seja, da informação, excluindo as possibilidades de risco e ameaças quanto às vulnerabilidades, quais sejam: Confidencialidade, Integridade e Disponibilidade das informações, a invasão acontece justamente quando a segurança falha. Prega também a conquista do comprometimento da

[12] A ISO/IEC17799 É uma norma de Segurança da Informação revisado em 2005 pela ISO e pela IEC. A versão original foi publicada em 2000, que por sua vez era uma cópia fiel do padrão britânico (BS) 7799-1:1999. O padrão é um conjunto, de recomendações para práticas na gestão de Segurança da Informação. Ideal para aqueles que querem criar, implementar e manter um sistema. A ISO/IEC-17799 Tem como objetivo confidencialidade, integridade e disponibilidade das informações são fatores muito importantes para segurança e integridade das informações. Disponível: <http://pt.wikipedia.org/wiki/ISO/IEC_17799 >- Acesso 30 maio 2008.

diretoria da empresa e da cúpula dos Tribunais para custear o aprimoramento dos recursos para implementação da Segurança da Informação. Segundo a norma, é preciso compreender que para o sucesso da segurança é necessário o controle e não proibição, sendo recomendável a apresentação de uma cartilha de atividades permitidas ao usuário para o perfeito manuseio das informações, destacando que a informação é da empresa e não de quem a manipula.

O que vem a ser informação? Qual é o papel que ela representa para os negócios? Marcos Sêmola (2003, p. 39) diz que "A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa."

No papel de "ativo crítico" para uma empresa, a informação se coloca como um ativo de valor, um "elemento essencial" para a saúde de uma organização. Nas palavras de André Campos (2006, p. 4)

> Os aspectos da geração de conhecimento a partir da informação são de especial interesse para as organizações, que, pela exposição de seus colaboradores à informação, poderão gerar verdadeiro valor para seus negócios. A utilização da informação alinhada à estratégia da organização representa benefícios à imagem da organização, facilitação para a inovação, diferenciação do produto e redução do custo e do risco do negócio, minimamente.
> Entendemos, assim, que a informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões e representa efetivamente valor ao negócio, dentro de cada um dos seus processos.

Deve-se ter em mente que a Segurança da Informação existe como meio e como fim, quer para garantir a confidencialidade, integridade e disponibilidade das informações, que para o alcance da segurança por meio de políticas adequadas em conformidade com normas, leis e políticas existentes. Visto a importância que tem a informação para uma empresa, pode-se imaginar o quanto é necessário observarem-se normas de segurança a ela relacionadas.

Há uma norma da Segurança da Informação que foi criada para ter como base a Gestão de Segurança da Informação conhecida como BS7799: parte 1

que é uma norma britânica e que possui uma versão brasileira – NBR ISO/IEC[13] 17799, que após ajustes foi traduzida e disponibilizada pela ABNT (Associação Brasileira de Normas Técnicas).

Aderir a uma norma, como exemplo a ISO 9001 ou 9002, pode significar um importante diferencial para a segurança dos tribunais, Estados e empresas. A mesma coisa ocorre com a ISO/IEC 17799, que traz uma Política de Segurança da Informação em seu cerne, o que dá maior garantia no compartilhamento das informações.

O objetivo da norma é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Seu principal requisito é definir a segurança a informação como um ativo importante para os negócios e fornecer o caminho para que a organização proceda. Com esse objetivo, a norma brasileira NBR ISO/IEC 17799 define que as organizações devem proceder:

I. À avaliação de risco dos ativos, pela identificação das ameaças, das vulnerabilidades e sua probabilidade de ocorrência;

II. À análise da legislação vigente, estatutos, regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviços precisam atender;

III. Aos conjuntos particulares de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Toda Política de Segurança deve estar alinhada ao negócio e os usuários devem estar totalmente envolvidos no processo de adequação e implementação

[13] A ISO (*Internacional Organization for Standardization* – Organização internacional para Padronização) e IEC (*International Electrotechnical Comission* – Comissão Internacional Eletrotécnica) formam um sistema especializado para padronização mundial.

dos procedimentos corretos. Os controles para Segurança das Informações terão seus preços mais reduzidos e mais eficazes se incorporados a uma operação quando esta encontra-se ainda em estágio de projeto.

Em 2005, surgiu a Norma 27001:2005 com o objetivo de programar as organizações para adequação do Sistema de Gestão da Segurança da Informação (SGCI). A Norma 27001 adota o modelo conhecido como "*Plan-Do-Check-Act*"[14] que é aplicado para estruturar todos os processos do SGCI além da adoção da Norma ISO 17799. Dessa forma, pode-se dizer que a Norma ISO 17799 está contida na Norma 27001.

1.3.1 – Norma internacional de segurança da informação - SARBANES OXLEY

Criada pelos Senadores *Michael Oxley* e *Paul Sarbanes*, a norma internacional *Sarbanes Oxley* foi aprovada em 2002 pelo governo americano para acabar com as fraudes contábeis, contém 11 títulos ou seções e é focalizada principalmente na responsabilidade penal da diretoria. Claramente os controles necessários envolvem muito mais que as próprias contabilidades, entre eles: fraude financeira interna, furto qualificado mediante fraude da propriedade intelectual e ampla apropriação indébita de informações de clientes, conforme pregam algumas previsões. O ato de *Sarbanes Oxley* é a mais importante legislação que afeta as corporações com leis de segurança norte-americanas.

A *Sox*, como também é conhecida, foi ordenada para proteger os investidores por meio do combate ao crime incorporado. Exige para as companhias programar políticas de controles amplos para prevenir e responder pontualmente às atividades fraudulentas dentro da empresa.

---

[14] Plan (Planejar)- Do(Fazer) – Check (Checar)- Act (Agir).

O principal objetivo é restabelecer e aumentar a confiança do investidor e a sustentabilidade das organizações, com isso há imposição de uma sucessão de boas práticas, além de requisitos técnicos operacionais.

As seções 301, 302 e 404 são as mais comentadas. A 301 é destinada a denúncias anônimas por empregados, a 302 é sobre a responsabilidade pessoal dos diretores executivos e diretores financeiros. Já a 404 determina avaliação anual dos controles e procedimentos internos para fins de emissão do relatório financeiro. Esta requer que os executivos se certifiquem de que as demonstrações financeiras sejam precisas, destaca o fato de a lei não tolerar demora com respeito a investigações, além de requerer revelação ao público. Deve ser dada uma particular atenção às seções 301, 302 e 404 porque nelas é exigida a atuação de um advogado especializado.

Uma companhia deve efetivamente e rapidamente responder a incidentes internos (como fraude financeira) e ataques externos que podem ter efeitos materiais na empresa. Quando falamos em *Sarbanes Oxley* isso significa que o mercado está querendo maior confiança. A *Sarbanes Oxley* também é conhecida como a Lei de Responsabilidade Fiscal e, segundo a seção 302, em caso de violação, os diretores, auditores e consultores dessas empresas estarão sujeitos à pena dessa Lei (que vão de 10 a 20 anos de prisão e multa de até 5 milhões de dólares, dependendo do caso).

Outro dos destaques da nova lei é a sua aplicabilidade às empresas estrangeiras que possuem valores mobiliários registrados na SEC (*Securities and Exchange Commisio*), o que estende de forma considerável a intenção de aplicação da legislação norte-americana de mercado de capitais. Ou seja, aplica-se a norma à elite das companhias brasileiras (atualmente mais de 38 empresas) que possuem ações na bolsa de valores norte-americanas, passando conseqüentemente, a estarem sujeitas à nova Lei, regulamentação que se estende a todas as filiais da empresa. As empresas multinacionais com sede no Brasil e cotação na Bolsa de Nova Iorque passaram por rigorosas adequações no sentido a imprimir um maior rigor em seus procedimentos internos. *Mutatis*

mutandis, os Poderes Públicos brasileiros podem aproveitar essa experiência das companhias privadas para criarem manuais de procedimentos técnicos e políticas de segurança e tratamento de documentos sigilosos, bem como disciplinar o uso dos equipamentos informáticos durante o expediente de trabalho. Recomenda-se que as empresas criem áreas de convivência para que funcionários possam se utilizar a internet para uso particular durante o expediente de trabalho. Deve-se criar um compromisso de uso cientificando os funcionários das empresas das regras como por exemplo, a vedação do uso do MSN e Skype, vedação quanto ao envio de arquivos da empresa para a conta de e-mail particular do funcionário, a vedação para o uso de conta de e-mail particular para tratar de assuntos oficiais das empresas e governos.

Em relação às tendências relacionadas ao tratamento das comunicações oficiais vimos a imprensa Nacional e Internacional noticiar que o FBI investiga e-mails da Governadora do Alaska e candidata republicana a vice-presidência dos EUA que supostamente teria usado o e-mail do Yahoo para tratar de assuntos oficiais. Vimos que nos EUA a discussão ganhou relevo após a descoberta de que o Governo Bush se utilizou de contas particulares de e-mail para conduzir assuntos da Casa Branca.

Os Tribunais Brasileiros têm proibido a utilização de arquivos e documentos eletrônicos sigilosos de propriedade da empresa que haviam sido remetidos do e-mail corporativo do empregado para uma conta de e-mail pessoal. Em um caso recente a AMBEV – Companhia de Bebidas das Américas, ajuizou ação de obrigação de não fazer em face de R. P. Diz a empresa que o réu burlou o regulamento da empresa e o sistema de segurança e remeteu correspondências eletrônicas para o seu email pessoal, a elas anexando diversos documentos contendo informações confidenciais relacionadas aos negócios dela autora.Pediu a antecipação dos efeitos da tutela de mérito, para que fosse determinado ao réu se abster de utilizar a documentação suprimida dos seus arquivos. Requereu a AMBEV que o processo tramitasse em segredo de justiça. Empregado exercia a função de “Staff de Qualidade”, sendo responsável por todo

o seu sistema de qualidade, inclusive liberação de insumos e produtos. Funcionário ele livre trânsito nos seus arquivos digitais, inclusive os de acesso restrito, como também participava de reuniões gerenciais. Após o desate contratual com a AMBEV foi admitido por uma de suas maiores concorrentes a Coca-cola, circunstância que lhe causa maior apreensão com o uso indevido dos documentos retirados do seu sistema. O Funcionário tinha plena ciência das restrições impostas pela empresa para a utilização dos documentos digitais de sua propriedade, recebeu uma cópia do Código de Conduta de Negócios e se comprometeu a cumprir as suas diretrizes, conforme tendo assinado recibo.[15]

Estar em conformidade com a *Sarbanes Oxley* justifica-se para empresas que participam ativamente nas bolsas de valores ou que têm um investimento alto na economia externa, a qual está atualmente em US$ 75 milhões. Podemos citar dentre as empresas brasileiras a Petrobrás e a empresa de energia elétrica CPFL.

Ressalta-se que a *Sarbanes Oxley* exige conformidade contínua e avaliação permanente com testes freqüentes e validações dos controles internos (seção 302), assim como um histórico de banco de dados e de fluxo de informações ampliado e adequado que permita a tomada de melhores decisões empresariais e também a guarda de provas legais. Estar em conformidade com a *Sarbanes Oxley* não é uma opção. As companhias que se negam a instituir os controles exigidos com toda certeza geram desconfiança e impacto no valor da ação para o acionista. O aumento da credibilidade nas empresas que cumprem seu papel em relação a *Sarbanes* é com certeza o resultado mais louvável e um ponto a mais na reputação de seus gestores.

A *Sarbanes Oxley* trouxe um novo padrão mundial de proteção corporativa ao enfatizar a responsabilidade gerencial do PSI – Profissional de Segurança da Informação - para estabelecer e manter uma infra-estrutura adequada de Segurança da Informação. Complementarmente, a *Sarbanes Oxley*

---

15 Esta decisão está disponível em PDF http://www.leonardi.adv.br/blog/wp-content/uploads/2008/09/sentenca00840200700413 00-1.pdf . Referências: 4ª VARA DO TRABALHO DE JOÃO PESSOA/PB. AÇÃO DE OBRIGAÇÃO DE NÃO FAZER. PROC. Nº 00840.2007.004.13.00-1.AUTORA: AMBEV – COMPANHIA DE BEBIDAS DAS AMÉRICAS RÉU: R. P. L.

tornou obrigatória a avaliação e a certificação por autoridade governamental das condições de segurança dos processos de negócios da organização.

Para demonstrar que seus sistemas estão seguros, a empresa necessita implementar controles físicos e controles lógicos que previnam acessos sem autorização, tais como o uso de f*irewalls*[16] ; proteção contra intrusão; avaliação contínua de vulnerabilidade. A administração também pode demonstrar que instrui adequadamente e treina os usuários provendo educação contínua que inclui ética, segurança de sistema; confidência e padrões de integridade. Aos auditores caberá avaliar esses itens e assegurar que a segurança é monitorada ativamente.

[16] Parede de Fogo: são programas que bloqueiam o acesso não autorizado de potenciais invasores.

2. Crimes de Informática

A era digital, que traz com ela a evolução dos meios eletrônicos, a facilidade e acessibilidade ao universo da internet e aos novos equipamentos eletrônicos disponíveis no mercado consumerista, tem gerado grandes impactos na sociedade. Ocorre que a ciências jurídicas também têm sido impactadas sensivelmente por tais evoluções, principalmente na seara criminal, pois o crescimento contínuo do uso da Internet vem possibilitando a prática de crimes complexos.

O número de denúncias cresce na mesma proporção que o número de acessos à Rede Mundial de Computadores. Com efeito, surgiu uma nova modalidade de crimes, os chamados crimes virtuais. Utilizamos para eles a definição do Professor Irineu Francisco Barreto Junior (2007, p. 71):

> Com o advento da Internet e da Sociedade da Informação, surgiu uma nova modalidade de crimes cometidos no espaço virtual da rede através de *e-mails* (correio eletrônico), *web sites* (sítios pessoais, institucionais ou apócrifos) ou mesmo ocorridos em comunidades de relacionamento na *Internet,*entre as quais a mais conhecida é o Orkut, propriedade do provedor de conteúdo americano Google. As transações comerciais eletrônicas, envolvendo compras que exigem a identificação do número de cartão de crédito, as transações bancárias, que solicitam registro de dados referentes às contas correntes bancárias, além do uso de senhas e demais mecanismos de segurança, assim como a profusão de novas modalidades relacionais mantidas em sociedade, através da *Internet,* propiciaram o surgimento de novas modalidades de crimes na *web*, batizados de *crimes virtuais.*

Para se tratar dos crimes virtuais, Fabrízio Rosa prescreve o uso do Direito Penal da Informática, que lado a lado com o Direito Civil da Informática

formam o Direito da Informática. Rosa diferencia as áreas de pertinência dos dois ramos do Direito da Informática da seguinte maneira (2005, p. 26):

> [...] pode-se definir o chamado Direito de Informática em dois ramos principais: o Direito Civil da Informática e o Direito Penal da Informática. No âmbito concernente ao Direito Civil da Informática, este passaria a concentrar seus estudos no conjunto de normas que regulariam as relações privadas que envolvem a aplicação da Informática, quais sejam: computadores, sistemas, programas, cursos, direitos autorais, documentos eletrônicos, assinaturas digitais etc. Já no que se refere ao Direito Penal da Informática, este seria o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos que atentem contra o acesso, uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos, os computadores.

Desse modo, diante da transformação dos acontecimentos provocados pela era digital, os conceitos legais antes utilizados para definir crimes têm sofrido grandes reformulações. Se o Direito sempre teve necessidade de acompanhar as mudanças que ocorrem na sociedade, isso se acelera sobremaneira nos dias atuais. Assim**,** não se pode entender o Direito como uma ciência estática e efêmera. Ao contrário, o Direito é o reflexo daquilo a que a sociedade aspira e de que necessita. Novas situações jurídicas exigem modificações da lei, e principalmente, tratamento diversificado e específico do caso concreto pelos profissionais das ciências jurídicas.

Igualmente, a própria Sociedade que se utiliza desses meios eletrônicos diariamente para atender às necessidades demandadas pela vida moderna, sobretudo a Internet, têm sido vítima dos ilícitos praticados pelos criminosos que se utilizam desse meio tecnológico em busca do anonimato.

Não podemos olvidar que muitas ações dessa espécie lesam diretamente direitos protegidos pelo ordenamento jurídico. Também é importante ressaltar que a legislação vigente tem sofrido modificações para que os novos tipos penais que trazem inserida em seu bojo a tecnologia tenham de ser resolvidos com maior celeridade processual para que sofram repressão verdadeira, uma vez que no momento não existe uma lei específica para esses tipos de delitos, correndo o risco de o criminoso ficar impune.

Dentre os novos delitos penais cometidos no mundo virtual, os chamados *cibercrimes*, destacam-se e nomeiam-se alguns a seguir. O "*cracking*" ou quebra de um sistema de segurança, de forma ilegal e sem ética, por um *cracker.* O "*phishing scam*", técnica que permite que piratas virtuais roubem informações de uma máquina com o objetivo principal de burlar transações financeiras. Os atos de "*gray hat*" e de "*black hat*". A cor do chapéu define que tipo de ações o *hacker* pratica. Aquele de "chapéu branco" é um *hacker* ético. O "*black hat"* (chapéu preto) é o *hacker* anti-ético, também denominado *cracker*. O *hacker* "*gray hat*" (chapéu cinza) é aquele penetra um sistema sem, no entanto, lesá-lo, ferir sua confidencialidade ou praticar vandalismo. Vale a observação de que, na ética *hacker*, apenas o ato de quebrar um sistema já configura em si um ato de infração. Nomeiam-se também o pichamento digital – inserção de textos ou figuras de terceiros em sites sem a autorização destes – e a espionagem eletrônica, definida por Fabrízio Rosa (2005, p. 67) como

> obtenção por meios ilegítimos ou divulgação,transferência, sem autorização nem outra justificação legal, de um segredo comercial ou industrial, no intuito de causar prejuízo econômico à pessoa a quem, por direito, pertence o segredo ou de obter para si ou para outrem uma vantagem econômica ilícita.

Por fim, destacam-se as difusões de códigos eletrônicos maliciosos danosos e não-danosos, tais como s*pywares*, a*dwares* ou a fraude eletrônica. O *spyware* é um programa que transmite informações pessoais de um computador conectado à internet sem que o usuário seja avisado. O *adware* é um tipo de *spyware*, um pouco menos ofensivo, que transmite apenas informações a respeito da utilização do sistema (em vez de informações pessoais).

Para exemplificar esses crimes cibernéticos destacamos delito penal cometido recentemente por uma quadrilha especializada em fraudes pela Internet e descoberto pela Polícia Federal numa operação que foi divulgada sob o nome de "Carranca de Tróia". Segundo informações da polícia, um dos envolvidos na

quadrilha confessou ter conseguido entre 700 mil e um milhão de reais capturando informações bancárias por meio de sites na internet[17]

O cometimento de crimes através de meios eletrônicos vem crescendo assustadoramente. As autoridades têm trabalhado de forma conjunta para apuração das mais diversas modalidades ilícitas, não medindo esforços para afastar a impunidade, inclusive a modalidade de prisão para esses casos quase sempre tem acontecido na modalidade de flagrante, o que comprova certamente a eficiência das autoridades que os investigam.

Segundo Dr. Paulo Quintiliano[18], crimes informáticos são todos aqueles praticados com a utilização do meio da tecnologia. Ou seja, definimos crimes de alta tecnologia como todos aqueles que se utilizam de ferramentas e instrumentos tecnológicos sofisticados para a práticas de delitos. Por exemplo, os criminosos se utilizam de um sistema de captação de sinais de rádio para captar informações a distância os dados e informações a respeito das operações que estão sendo realizadas naquele momento por caixas eletrônicos com o objetivo de posteriormente promover saques nessas contas. Por outro lado, em um método menos sofisticado, o criminoso pode implantar dentro do terminal bancário uma pequena máquina leitora de dados. Essa máquina pode enviar informações por meio de sinais de radiofreqüência, na versão mais avançada, ou mesmo, deve ser retirada pelo criminoso ao final de um determinado período, para que ele possa colher os dados de que precisa para a prática do ilícito.

Portanto, o crime cibernético é uma modalidade do crime informático, praticado com emprego de sofisticada tecnologia. Quintiliano esclarece que crimes cibernéticos s*tricto sensu* (próprios), são aqueles que não poderiam ser

---

[17] notícia disponível integralmente no endereço <http://www.antifraudes.com.br/portal/noticia.php?id=334411> acesso em outubro de 2008.

[18] Dr. Paulo Quintiliano é perito criminal Federal da Polícia Federal, onde atua na área de combate aos crimes cibernéticos. É graduado em Ciência da Computação e em Direito, mestre em Ciência da Computação e doutor em Processamento de Imagens e Reconhecimento de Padrões. Em 2005, foi eleito o conselheiro representante da América Latina no "International Botnet Task Force Counsel". É o editor-chefe do "The International Journal of Forensic Computer Science (IJoFCS)" e coordenador-geral das conferências "ICCyber - The International Conference on Computer Science" e "ICoFCS - The International Conference of Forensic Computer Science". É o presidente da HTCIA Brasília Chapter.

praticados sem a utilização do espaço cibernético. Por outro lado, os crimes informáticos *lato sensu* ou impróprios podem ser praticados sem a utilização do espaço cibernético apenas com o emprego de tecnologia.

Os estudiosos da área afirmam que tais ilícitos com uso da Internet podem ser enquadrados na atual legislação penal extravagante, bem como em nosso Código Penal. Tal assertiva se dá pelo argumento que a Internet é o meio pelo qual se executam esses crimes, tais crimes são conhecidos como crimes digitais, cibernéticos ou cibercrimes.

Na opinião do Dr. Marco Antônio de Barros (*in* PAESANI, 2007, p. 290-291):

> Sem existir a correspondente tipificação penal, os crimes praticados mediante a utilização de *sites* de relacionamento (como, por exemplo, aqueles que têm sido identificados no Orkut), invasões de PC´s, ataques a redes e a outros meios de comunicação eletrônica têm sido denunciados à Justiça como sendo crimes previstos na legislação penal tradicional, tais praticados contra a honra, furto mediante fraude, estelionato, formação de quadrilha, tráfico de drogas etc.
> A questão que estaciona no campo da dúvida é saber se o direito penal clássico pode abranger algumas dessas novas realidades ilícitas, ante a vedação de se proceder a analogia *in mallam partem.* Contra a elasticidade do Código Penal são apresentados argumentos substanciosos, fundados em princípios fundamentais, tais como o de não haver crime sem lei anterior que o defina, nem pena sem prévia cominação legal (art. 5º, XXXIX, CF), ou o princípio da reserva legal, que estabelece que só pode haver punição se existir uma lei formal que defina determina conduta como criminosa.
> No Senado Federal brasileiro, a discussão sobre a necessidade ou não de se elaborar uma lei específica para tipificar e punir os crimes eletrônicos ainda não terminou. Renan Calheiros nos informa sobre a existência de três projetos em tramitação, que foram reunidos e estão sendo relatados pelo senador Eduardo Azeredo. A tendência, segundo o parlamentar, é a de que se aprove uma atualização pontual das leis penais existentes, acrescentando aos crimes já tipificados novos artigos e dispositivos sobre o uso da informática na ação criminosa, considerando as condutas como agravantes e atribuindo penas mais severas.

Virgínia Soprana Dias, em seu artigo "Aspectos da Segurança Jurídica no Âmbito dos Crimes Cibernéticos" (DIAS, 2007), comenta sobre a situação da regulamentação legislativa citando Demócrito Reinaldo Filho: “(...) a indiferença legislativa levaria necessariamente ao obsoletismo de institutos jurídicos”.

Ainda segundo a autora (idem, p. 87-88):

> Objetivando, então, estabelecer se há possibilidade ou não de enquadramento das condutas virtualmente realizadas no ordenamento jurídico, formas distintas de classificação dos cibercrimes são apontadas pela doutrina: forma de atuação do agente, bem jurídico visado, tipo de conduta lesiva, dentre outras. Há autores que de certa forma relativizam o assunto quando classificam os crimes cibernéticos quanto ao seu objetivo: para Maria Helena Junqueira Reis, poder-se-iam separar dois temas, em que constariam do primeiro os crimes regulados pelo instituto do Código Penal e das leis especiais e, do segundo, os demais, decorrentes da tecnologia dos computadores. Isso quer significar que existiriam os crimes em que o sujeito que os pratica visa a um bem juridicamente protegido, mas interno ao universo virtual ou dele dependente – necessariamente ou não - , em que a rede, no caso, seria mera ferramenta para a prática de algum tipo penal; e, diametralmente, existiriam também os crimes em que o agente visa à prática de atos exatamente referentes à rede de computadores, em que o sistema da rede é em si o objetivo material da conduta(...)
> (...) Convém, outrossim, apontar as especificidades em que os crimes cibernéticos estão envoltos, a fim de que possa vislumbrar a real amplitude desse universo e, por decorrência, a necessária regulamentação legislativa. As condutas em que o agente visa a um bem jurídico relativo ao próprio sistema informático – aquelas em que o objeto da ação causa lesão a bens ou a dados de informática – fogem à esfera protetiva do Estado, uma vez que as particularidades dessas ações as impedem de se subsumir a qualquer tipo penal: o conceito de “dado” ou “informação eletrônica” não se equipara à “coisa” no Código Penal, o que inviabiliza a aplicação nos crimes contra o patrimônio. Também não há previsão legal pra alteração de senha ou de meio de acesso a programa de computador ou dados ou mesmo à criação e disseminação de programas ou dados com fins nocivos.
> Logo, a solução não poderia fugir à criação de leis específicas, que possibilitem trazer tipicidade às condutas realizadas em função das novas tecnologias, e que, em virtude das sanções penais que impliquem, coíbam a prática dos cibercrimes.

O Professor Fabrízio Rosa também faz considerações sobre a legislação penal (2005, p. 73)

> Não resta dúvida de que a criminalidade informática, infelizmente, é uma manifestação da atualidade, que deve ser combatida. A discussão centra-se em torno das modalidades técnicas de previsão, em referência à dúvida de se abrir caminho a uma legislação especial e autônoma ou então a medidas que inserissem as disposições incriminadoras no corpo do velho Código Penal de 1940, ora vigente. Não resta dúvida de que a *Internet* é um meio novo de execuções de crimes “velhos”, contidos no Código Penal; entretanto, esses crimes não são considerados “crimes de Informática”. Estelionato é sempre estelionato, praticado com assistência do computador ou sem ela; afirmar que alguém cometeu um fato definido como crime, sem que tal seja verdade, configura delito de calúnia (Código Penal, art. 138), tanto quando a difusão é feita oralmente ou pelos caminhos da *Internet.* No entanto, como já salientado, não se deve confundir um crime comum praticado pelo uso ou contra o computador

> com um “crime de Informática” propriamente dito. Assim, ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si que, então, se torna objeto de aprofundamentos novos, os “crimes de Informática”, até então desconhecidos pelo legislador penal pátrio de 1940, surgidos com o advento do computador e da *Internet.*

2.1 - Governos e segurança digital

Conforme Christopher Painter[19], Chefe do Departamento de Tecnologia da Informação e Propriedade Intelectual da Divisão Criminal do Departamento de Justiça dos EUA, a revolução digital traz presente em seu arcabouço o conceito de duas leis. Essas leis podem vir a regulamentar os novos fatos jurídicos eletrônicos. No entanto, em função da velocidade e da perfeição dos novos ataques tecnológicos ao governo e a empresas, estas leis poderiam nascer já obsoletas [20].

Neste cenário, segundo ele, para os órgãos de combate aos crimes cibernéticos dos Estados Unidos, fica evidente que o crime cibernético se divide em três partes, a saber:

---

[19] PAINTER,Christopher. Crimes Digitais e Segurança Cibernética. *In* : Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008. Painter é chefe do Sub-Grupo de Crimes de Alta Tecnologia do G8 / Chefe do Departamento de Tecnologia da Informação e Propriedade Intelectual - Divisão Criminal, do Departamento de Justiça dos Estados Unidos da América.

[20] Informações deste capítulo junto às autoridades aqui relatadas foram colhidas através de entrevista do pesquisador durante o Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais', realizado na Câmara dos Deputados no dia 28 de maio – Auditório Nereu Ramos, Brasília. O Conselho de Altos Estudos e Avaliação Tecnológica, sensível à questão, promove, por iniciativa do Dep. Colbert Martins, o Seminário Crimes Cibernéticos e Investigações Digitais, com o objetivo de incorporar contribuições que possam aprimorar o substitutivo do Senador Eduardo Azeredo, com vistas a uma adequação do ordenamento jurídico brasileiro na reformulação da legislação relacionada à temática. O evento tem o apoio da Embaixada Americana, do Conselho da Europa e da Interpol. Outras autoridades foram entrevistadas nos dias 26 e 27 de maio no Congresso Nacional, uma vez que diversas autoridades estavam no Brasil em função deste evento e também em função de terem sido convocadas para auxiliar nos trabalhos da Comissão Parlamentar de Inquérito de Combate a Pedofilia que promove uma ação de mútua cooperação com diversas autoridades do mundo.

Na primeira, o computador é objeto, a arma, a ferramenta para realização do crime e ao mesmo tempo é o alvo dos crimes. Painter cita o ataque a banco de dados que o abastece. Esses ataques e intrusões, ainda que arquivos não sejam subtraídos ou apagados, nos Estados Unidos já são tipificados como crime. Não no Brasil. Menciona o pesquisador que, no Brasil, uma vez que o criminoso retire uma cópia dos arquivos da vítima sem ser notado, em tese não se estaria cometendo nenhum ilícito penal. Christopher Painter menciona que os Estados Unidos, em 2007 e 2008, tiveram perdas financeiras enormes em função do ataque de criminosos virtuais.

A segunda etapa versa sobre o comércio de identidade de cidadãos americanos, que tem crescido em ritmo alarmante. O Departamento de Justiça Americano identificou diversos sítios onde atualmente se oferecem cartões de crédito falsos de cidadãos americanos de todas as principais operadoras de cartões de crédito do mundo.

Na terceira parte o autor relata que as quadrilhas se aperfeiçoaram a tal ponto que antes mesmo de serem identificados os servidores que abastecem essas informações na rede, os sítios somem deixando muitas vezes vestígios cibernéticos difíceis de serem rastreados.

Nos últimos três anos cresceu o número de *hackers* dedicados especializados em chantagear pessoas físicas, jurídicas, autoridades do governo e até mesmo agências governamentais. O *modus operandi* do criminoso está relacionado à sua imensa habilidade individual de acessar informações altamente sigilosas que geralmente podem comprometer a reputação de empresas públicas e privadas e também de pessoas que gozam de notória reputação na sociedade. Em muitos casos, após o acesso às informações, essas são capturadas e posteriormente o criminoso entra em contato com sua vítima ameaçando divulgar a informação secreta a concorrentes ou mesmo vendê-las para algum governo estrangeiro que esteja disposto a pagar seu preço. Ou seja, muitas vezes a vitima passa a ser monitorada antes mesmo que a informação venha a cair nas mãos do criminoso. O *hacker* moderno estuda sua vítima verificando quais informações lhe

são verdadeiramente preciosas e capazes de lhe atingir com maior grau de impacto.

Outro ataque que vem evoluindo e sofisticando-se paulatinamente é aquele perpetrado pela chamada "bomba lógica[21]". Ela é instalada pelo criminoso diretamente na rede de sistema do governo ou de empresas e objetiva com a sua detonação a destruição de um grande número de dados e informações preciosas. Tais bombas ainda objetivam danificar equipamentos e infra-estrutura, de modo a gerar um congestionamento de informações. Relatou Christopher Painter que o Brasil não está livre do ataque de criminosos que possam vir a desencadear uma série de ataques com o intuito de espalhar o terror e desmoralizar instituições como o Poder Judiciário Brasileiro. Esses ataques certamente, segundo ele, terão o objetivo de tornar indisponíveis os seus sistemas ou mesmo virão a capturar informações sigilosas de processos em andamento e ainda capturar informações que possam ferir a honra de magistrados, promotores e advogados.

As facções criminosas que atuam nos Estados Unidos são altamente organizadas, informou Christopher Painter. Ele descreve que os criminosos se comunicam em uma linguagem própria e muitas vezes nem mesmo se conhecem pessoalmente. Essas organizações agem em grupo, diferente do *hacker* dedicado que atua sozinho, e procuram atuar em grupo e de forma sigilosa e anônima. Na maioria das vezes, a comunicação para o ataque vai passar por diversos países. Como alerta ao Poder Judiciário Brasileiro, Painter informou que em 2007 *hackers* criminosos dispararam um forte ataque contra a Suprema Corte Argentina. Esse ataque teve como objetivo congestionar os servidores da Suprema Corte, de modo que todos os operadores do Direito em determinado período não tivessem acesso a inúmeras informações vitais para o desenvolvimento de seu trabalho. É de se concluir, portanto, que o Brasil, por sua expressão internacional, pode ser

---

[21] A Bomba Lógica explode tudo a seu redor, só que ela só existe dentro dos computadores. Uma bomba lógica é um programa que tem como único objetivo destruir dados ou hardware, quando tal coisa é possível. Segundo artigo do sítio *howstuffworks,* uma bomba destas normalmente é planejada por empregados insatisfeitos ou por espiões corporativos. Sendo um programa especifico e não classificado como vírus, fica difícil a proteção de redes de computadores contra a bomba. Disponível:< http://www.bernabauer.com/bomba-logica/ > Acesso em 30 maio 2008.

alvo destes criminosos que, segundo ele, têm como objetivo muitas vezes retirar a credibilidade de instituições fazendo-as parecer frágeis frente à população. Atualmente os Estados Unidos lutam para aumentar a privacidade dos americanos do mesmo modo que trabalham em Leis que possibilitam incluir de forma cada vez mais célere a possibilidade de realizar interceptação de ligações telefônicas de redes criminosas.

Um outro ataque recente contra Governos foi o ataque aos meios de comunicação sofrido pela Estônia, onde os atacantes, através de técnicas de negação de serviço, tiraram do ar os principais sítios do governo, afetando também o acesso à internet do país, gerando milionários prejuízos financeiros além de uma crise diplomática com a Rússia (PEOTTA, 2007).

Um outro desafio que se apresenta, relata Christopher Painter, é a inclusão de toda tecnologia dentro de um único arcabouço legal, capaz de prever em sua redação a possibilidade de o governo e autoridades agirem de forma ativa frente a uma série de novas tecnologias. Ele cita como exemplo a incapacidade do Estado americano em conceder uma determinada ordem judicial ou cumprir esta ordem judicial de modo a agir especificamente em relação a um determinado tipo de comunicador voltado ao crime. Ou seja, a autoridade judicial poderá encontrar dificuldades de entender a forma como deve ser concedida determinada ordem judicial se não tiver conhecimento profundo de como funciona essa tecnologia, qual foi o raio de ação do crime, evitando assim que em uma ordem judicial não sejam respeitados os direitos constitucionais dos cidadãos americanos. Ele cita como exemplo o caso de criminosos versados em tecnologia terem instalado aparelhos em uma determinada rede interna e externa de telefonia utilizada por pessoas físicas e jurídicas. Após algum tempo, esses números de telefones passaram a ser controlados por facções criminosas que começam a utilizar esses aparelhos de comunicação como espinha dorsal de uma nova teia de comunicação dirigida a favor do crime. Menciona o pesquisador que atualmente são vários equipamentos que possibilitam ao criminoso moderno a interatividade e o alcance com estes equipamentos e muitas vezes ainda a forma

de sua utilização pode ser otimizada de modo a ter um maior ou menor grau de alcance. Pois bem, explica, se o promotor, o magistrado ou mesmo o advogado de defesa não for capaz de identificar o alcance do raio de ação destes equipamentos, não serão capazes de oferecer à sociedade uma resposta efetiva contra tais incidentes e criminosos. O governo americano acredita firmemente que não basta o policial, o serviço secreto e os oficiais especializados das agencias de inteligências reterem o conhecimento das novas tecnologias. O governo americano acredita que é necessário que os promotores e juízes sejam constantemente treinados para entenderem como funciona o equipamento da alta tecnologia voltado à pratica de ilícitos da órbita civil e criminal. Em um primeiro momento, o governo Americano enfrentou uma resistência inicial muito grande por parte dos juízes que não gostavam de serem treinados para compreender esse universo informacional tecnológico da era da Sociedade da Informação. Atualmente o Departamento de Justiça treina cerca de 50 promotores e juízes todos os meses. O treinamento é rigoroso e obrigatório, uma vez que para as autoridades do Governo Americano o momento é critico e requer atenção não só dos Estados Unidos, mas de todo o mundo. O alerta é geral e indica que os EUA estão em constante prontidão para esta nova realidade de delitos praticados por meio de alta tecnologia. Para que esse combate seja ainda mais efetivo, o Departamento de Justiça dos Estados Unidos criou uma divisão de combate, investigação e repressão aos chamados crimes praticados por alta tecnologia.

Ainda em relação à dificuldade de se identificar o criminoso, o chefe do Departamento de Justiça dos Estados Unidos relata que as redes sem fio de comunicação pela Internet, comumente denominadas redes *wireless*[22], são muito usadas pelas facções criminosas nos Estados Unidos e que tornam muito difícil a

[22] As redes sem fio (wireless), também conhecidas como IEEE 802.11, Wi-Fi ou WLANs, são redes que utilizam sinais de rádio para a sua comunicação. Este tipo de rede define duas formas de comunicação: modo infraestrutura: normalmente o mais encontrado, utiliza um concentrador de acesso (Access Point ou AP); modo ponto a ponto (ad-hoc): permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP. Estas redes ganharam grande popularidade pela mobilidade que provêem aos seus usuários e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos, etc. Disponível: <http://cartilha.cert.br/bandalarga/sec2.html > Acesso 30 maio 2008.

identificação dos criminosos. Nos Estados Unidos os provedores não estão obrigados a fornecer os dados de seus usuários às autoridades a não ser por ordem judicial. Contudo, as autoridades competentes, antes da obtenção da ordem judicial podem solicitar que determinadas informações sob potenciais criminosos sejam preservadas até que seja obtida a ordem judicial.

Para o Departamento de Justiça Americano, tem crescido a consciência de que é preciso existir uma cooperação muito forte entre a iniciativa privada e as agências de inteligência. Por outro lado, segundo estudos dessa organização, somente com a máxima integração as autoridades Americanas podem fazer frente à criminalidade cibernética. Ou seja, o Departamento de Justiça classifica que a cooperação em todos os níveis e o investimento constante em tecnologia são fundamentais a qualquer governo. O governo americano vê como fundamental o constante aprimoramento das autoridades nos estudos científicos em campos de pesquisas diversos. O Departamento de Justiça dos Estados Unidos entende que estes são novos delitos, os delitos de uma nova era, a era cibernética. São os chamados delitos da era da alta tecnologia, onde aquilo que se pensava inimaginável passa a ser uma realidade ao alcance das mãos e dos olhos em uma fração de segundos.

Anthony Reyes[23], pesquisador americano que trabalha como consultor do FBI e da CIA, informou que membros da facção PCC[24] estão atuando em Nova Iorque. Esses criminosos não atacam instituições ou cidadãos em solo americano. O estágio nos Estados Unidos tem o objetivo de aprender e desenvolver novas armas voltadas aos crimes tecnológicos que são disparadas dos EUA contra alvos do Brasil. Essa facção começou a ser detectada pelo pesquisador no início de setembro de 2007 e foi relatada às autoridades da Policia Federal Brasileira no

[23] Anthony Reyes é internacionalmente reconhecido, professor na área de crimes cibernéticos, trabalhou como investigador de invasões de computadores, identificação de roubos, fraudes; no Departamento de Polícia de Nova York.

[24] Primeiro Comando da Capital (PCC) é uma organização de criminosos existente no Brasil que surgiu no início da década de 1990

final de setembro de 2007. Nilson Marcio de Oliveira[25], Superintendente da Área de Segurança do Banco do Brasil, informa que estes ataques são de fato uma realidade que já começa a surtir efeitos no Brasil. Ele relata que a partir de abril e maio de 2008 o nível de sofisticação dos golpes evoluiu muito. O Banco do Brasil começou a utilizar a Internet em 1995 e a *Internet Banking* (acesso ao banco via internet) foi lançada em 1997. O Departamento de Segurança do Banco do Brasil relatou que em outubro de 2001 foi lançado o primeiro ataque efetivo com o intuito de fraudar a instituição. O criminoso, em um primeiro momento, direcionou seus ataques e golpes diretamente contra o Banco do Brasil. Posteriormente esses ataques passaram a ser lançados contra os correntistas, uma vez que o Banco do Brasil investiu milhões em equipamentos tecnológicos de defesa. Com o passar do tempo, os criminosos passaram a perceber que não tinham chance contra os sistemas de defesa dos bancos e aqueles que conseguiam sucesso eram obrigados a despender recursos muito mais caros e sofisticados, sendo que nem sempre os resultados eram aqueles esperados.

O Superintendente do Banco do Brasil informa também que, segundo pesquisas do Banco, aquelas instituições públicas ou privadas que não realizarem investimentos maciços e compulsivos em segurança da informação estão fadadas à extinção. Para o Banco do Brasil, o sucesso da rede bancária está fundamentado hoje em dois pilares básicos: o primeiro deles é a cooperação constante a nível nacional e internacional. Para tanto informou que atualmente existe um grupo de estudos da Febraban[26] que se reúne com diversos setores da

---

[25] Sr. Nilson Mário de Oliveira foi entrevistado pelo pesquisador na ocasião do Seminário Internacional
Crimes Cibernéticos e Investigações Digitais, ocorrido em 28 de maio, Auditório Nereu Ramos, Brasília, 2008.

[26] A Febraban – Federação Brasileira de Bancos é a principal entidade representativa do setor bancário brasileiro. Foi fundada em 1967 para fortalecer o sistema financeiro e suas relações com a sociedade e contribuir para o desenvolvimento econômico e social do País. O objetivo da Federação é representar seus associados em todas as esferas – Poderes Executivo, Legislativo e Judiciário e entidade representativas da sociedade – para o aperfeiçoamento do sistema normativo, a continuada melhoria da produção e a redução dos níveis de risco. Também busca concentrar esforços que favoreçam o crescente acesso da população em relação a produtos e serviços financeiros. Disponível:

sociedade dentre eles a Polícia Federal Brasileira. O grupo é composto ainda por diversas outras instituições públicas e privadas no exterior. O segundo fator crítico de sucesso é o investimento maciço em novas tecnologias capazes de fazer frente à sofisticação desses novos ataques. Ele explica que o Banco do Brasil é favorável à promulgação de uma lei capaz de impor maiores conseqüências ao criminoso. É preciso criar, segundo ele, uma consciência geral de que o criminoso será duramente punido por seus atos ilícitos.

Líder da Comissão Parlamentar de Inquérito de Combate à Pedofilia, o senador Magno Malta[27],quando entrevistado por este pesquisador, elogiou a operação Carrossel da Policia Federal, que prendeu 700 pedófilos, detectou 3.700 páginas de redes de propagação da pedofilia, muitas delas eram dotadas de um sistema de agenciamento do encontro do pedófilo com crianças. O Senador baiano elogiou ainda o auxilio da *safernet*[28] que juntamente com seu líder, Dr. Thiago Tavares[29,] desenvolveu um *software* capaz de localizar pedófilos ao redor

---

<http://www.febraban.org.br/Arquivo/Quemsomos/Perfil%20Institucional.pdf> - Acesso 30 maio 2008.

[27] Senador Magno Malta lidera a CPI da Pedofilia. Informações deste capítulo colhidas através de entrevista do pesquisador durante o Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais', realizado na Câmara dos Deputados no dia 28 de maio – Auditório Nereu Ramos, Brasília.

[28] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos e econômicos, de duração ilimitada e ilimitado número de membros, sem vinculação político partidária, fundada em 20 de Dezembro de 2005 por um grupo formado por cientistas da computação, professores, pesquisadores e bacharéis em Direito, reunidos com o objetivo de materializar as diretrizes e linhas de ação empreendidas ao longo dos anos de 2004 e 2005, quando estiveram diretamente envolvidos na realização de pesquisas e no desenvolvimento de projetos sociais relacionados ao combate a pornografia infantil (pedofilia) na Internet no Brasil. Disponível: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/QuemSomos> Acesso 31 maio 2008.

[29] Thiago Tavares Nunes de Oliveira é professor da Faculdade de Direito da Universidade Católica do Salvador, onde leciona as disciplinas Direito da informática, Informática Jurídica, Projeto de Pesquisa em Direito e Monografia Final. Desde 2000 tem participado dos principais congressos e fóruns internacionais sobre Propriedade Intelectual, Governança da Internet e Software Livre, com destaque para a Conferência Regional da América Latina e Caribe, preparatória para a II fase da Cúpula Mundial da Sociedade da Informação (WSIS) e da V Assembléia Anual do INHOPE, realizada em Atenas, Grécia, em outubro de 2005. Suas pesquisas e trabalhos científicos já foram apresentados em dezenas de congressos internacionais no Brasil e exterior. Foi o Secretário Geral do III Congresso Internacional de Direito e Novas Tecnologias da Informação que reuniu 700 especialistas de 7 países e 23 estados brasileiros em Agosto de 2004, em Salvador-Bahia, para discutir os impactos jurídicos e

do mundo. Destacou ainda o Senador que tem sido muito importante a luta brasileira contra a pedofilia o auxilio do governo americano, o qual tem disponibilizado todos os esforços para auxiliar as autoridades brasileiras.

O parlamentar informou que o Senado Federal tem trabalhado juntamente com a Procuradoria Geral da República, a PF, para auxiliar assinatura de diversos "Termos de Ajustamento de Conduta[30]" com o *Google*[31], *Orkut*[32], *Myspace*[33] no

---

sociais da Internet no Brasil. Cursou o Internet Law Program do Berkman Center For Internet and Society, da Harvard Law School. Pesquisador concursado do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas(CTS/FGV), atualmente cursa o mestrado em Desenvolvimento e Gestão Social na Universidade Federal da Bahia, é conselheiro e coordenador do Núcleo de Pesquisa do Instituto Brasileiro de Política e Direito da Informática(IBDI) e integra, desde novembro de 2004, a subcomissão intersetorial instituída pela Secretaria Especial de Direitos Humanos da Presidência da República do Brasil responsável pela elaboração do Plano Nacional de Enfrentamento à Pedofilia e Pornografia Infantil na Internet. É ainda Administrador pela UFBA, regularmente inscrito e habilitado pelo Conselho Federal de Administração. Trabalhando a frente da Presidência e Diretoria de Projetos da SaferNet Brasil, é o responsável pelo planejamento, articulação e gestão dos projetos da primeira organização social do Hemisfério Sul dedicada exclusivamente a defesa e promoção dos Direitos Humanos na Sociedade da Informação. Disponível: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/ThiagoTavares> Acesso 31 maio 2008.

[30] Termo de Ajustamento de Conduta - Instrumento extrajudicial por meio do qual as partes se comprometem, perante os procuradores da República, a cumprirem determinadas condições, de forma a resolver o problema que estão causando ou a compensar danos e prejuízos já causados. O TAC antecipa a resolução de problemas de uma maneira mais rápida e eficaz do que se o caso fosse a juízo. Se a parte descumprir o acordado no TAC, o procurador da República pode entrar com pedido de execução, para o juiz obrigá-lo a cumprir o determinado no documento. Disponível: < http://noticias.pgr.mpf.gov.br/servicos/glossario> Acesso 31 maio 2008.

[31] Google Inc. (NASDAQ: GOOG) é o nome da empresa que criou e mantém o maior site de busca da internet, o Google Search. O serviço foi criado a partir de um projeto de doutorado dos então estudantes Larry Page e Sergey Brin da Universidade de Stanford em 1996. Este projeto, chamado de Backrub, surgiu devido à frustração dos seus criadores com os sites de busca da época e teve por objetivo construir um site de busca mais avançado, rápido e com maior qualidade de ligações. Brin e Page conseguiram seu objetivo e, além disso, apresentaram um sistema com grande relevância às respostas e um ambiente extremamente simples. Uma das propostas dos criadores do Google era ter uma publicidade discreta e bem dirigida para que o utilizador perca o menor tempo possível, sem distrações. Disponível:<http://pt.wikipedia.org/wiki/Google> - Acesso 30 maio 2008

[32] O Orkut (ou orkut) é uma rede social filiada ao Google, criada em 24 de Janeiro de 2004 com o objetivo de ajudar seus membros a criar novas amizades e manter relacionamentos. Seu nome é originado no projetista chefe, Orkut Büyükkokten, engenheiro turco do Google. Tais sistemas, como esse adotado pelo projetista, também são chamados de rede social. É a rede social com maior participação de brasileiros, com mais de 23 milhões de usuários. [2] Nota sobre o nome: apesar de Orkut ser um nome próprio, na programação visual do site (títulos e logos) a palavra está em minúscula (orkut). Disponível:< http://pt.wikipedia.org/wiki/Orkut > Acesso 30 maio 2008.

[33] MySpace é um serviço de rede social que utiliza a Internet para comunicação online através de uma rede interativa de fotos, blogs e perfis de usuário. É a maior rede social do

sentido de que estas empresas possam enviar as autoridades, imagens, vestígios, provas, dados e informações de qualquer natureza. Demais informações, úteis e que possam levar na prisão de pedófilos e o desmantelamento das redes de pedofilia.

As provas dos crimes cibernéticos possuem um alto grau de volatividade, ou seja, quando se está analisando um sítio que está no ar, operando na rede mundial de computadores, estes de uma hora para outra se "apagam". Nesse sentido, a missão do serviço de perícias e crimes cibernéticos do Instituto Nacional de Criminalística da Policia Federal tem tido como objetivo validar e preservar as provas dos crimes praticados com o uso do espaço cibernético. O Senhor Leonardo Bueno de Melo[34] explica que a Polícia Federal atualmente tem uma Unidade de Combate aos crimes cibernéticos composta por delegados, investigadores e outros profissionais de carreira que têm por prática a investigação propriamente dita. Por outro lado, trabalham os peritos criminais federais do setor de crimes cibernéticos na materialização da prova para o mundo jurídico. As duas vertentes acima mencionadas trabalham com grande integração. Na visão do senador Malta, os provedores deveriam ser obrigados a entregarem os *logs*[35] dos usuários contendo as informações capazes de levar à identificação de criminosos. Ele relata ainda que em outros países o grande problema é o ataque da rede de *botnets*[36]. Este tipo de ataque possibilita a rede ou facção

---

Estados Unidos e do mundo com mais de 110 milhões de usuários [2]. Inclui um sistema interno de e-mail, fóruns e grupos. MySpace é um site muito ativo, com novos membros entrando no serviço diariamente e novos recursos adicionados com freqüência. A crescente popularidade do site e sua habilidade de hospedar MP3s fez com que muitas bandas e músicos se registrassem, algumas vezes fazendo de suas páginas de perfil seu site oficial. Em 18 de julho de 2005, a News Corporation (dona da Fox, DirecTV etc.), conglomerado de mídia de Rupert Murdoch, anunciou que iria comprar a Intermix Media, a empresa dona do MySpace, por US$ 580 milhões. Disponível: <http://pt.wikipedia.org/wiki/MySpace > Acesso 30 maio 2008.

[34] MELO, Leonardo Bueno. Crimes Digitais e Segurança Cibernética. *In* Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008.

[35] Os logs são registros de atividades gerados por programas de computador. Disponível em: <http://www.htmlstaff.org/cartilhaseguranca/cartilha-07-incidentes.html> Acesso 30 maio 2008.

[36] Devido à facilidade e acesso a computadores e redes de alta velocidade as *botnets* têm um grande campo para se desenvolver. No entanto, deve-se ter uma maior preocupação, não apenas pelo usuário, que deve tomar precauções, mas também das autoridades, pois devem

criminosa bloquear serviços urgentes de interesse público que têm um grande grau de dependência do uso da Internet. Relata que este tipo de ataque ainda não é tão grande no Brasil, mas é alvo de grande preocupação da Policia Federal Brasileira.

Conforme Jaime Edgardo Jara Retamal[37] – Presidente do Grupo de Trabalho Latino-Americano sobre Delitos Tecnológicos da Interpol[38], a referida agência mantém uma cooperação muita ativa com o Departamento de Policia Federal brasileiro com o objetivo de oferecer respostas aos crimes cibernéticos. Tanto a Interpol quanto o Brasil fazem parte da rede 24/7[39]. Esta rede tem o objetivo de possibilitar que policiais tenham acesso a fontes de informação e provas de delitos cometidos a partir de outros países, 24 horas por dia, 7 dias por semana. Atualmente, para o combate ao crime cibernético, a Interpol defende um trabalho regional na América Latina. Segundo estudos, para que se possa evoluir ações efetivas de combate aos crimes cibernéticos na América Latina a

---

criar dispositivos para detectar e neutralizar essas redes o mais rápido possível. Essas redes podem ser utilizadas para uma infinidade de ações que vão deste ataques de negação de serviços como o de envio indiscriminado de mensagens não solicitadas. PEOTTA Laerte, AMARAL,Dino. Honeypot de Baixa Interação como ferramenta para detecção de tráfego com propagação de Botnests. *Proceedings of the second international conference on forensic computer science investigation* (ICoFCS`2007)/ABEAT(ed.)- Guarujá, Brasil, 2007,p 84.- ISSN-1980-1114.

37 RETAMAL, Jaime Edgardo Jara. Cooperação Internacional. *In:* Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008.

38 International Criminal Police Organization (Interpol) A Organização Internacional de Polícia Criminal, mundialmente conhecida pela sua sigla Interpol, é uma organização internacional que ajuda na cooperação de polícias de diferentes países. Surgiu em Viena, na Áustria, no ano de 1923. Hoje sua sede é em Lyon, na França [1]. A Interpol não se envolve na investigação de crimes que não envolvam vários países membros ou crimes políticos, religiosos e raciais. Trata-se de uma central de informações para que as polícias de todo o mundo possam trabalhar integradas no combate ao crime internacional, o tráfico de drogas e os contrabandos. Disponível: <http://pt.wikipedia.org/wiki/International_Criminal_Police_Organization> Acesso 31 maio 2008

39 Uma rede de comunicações mundial segura permite aos agentes da Interpol e países membros contatar um ao outro a qualquer hora. Conhecida como I-24/7, a rede oferece acesso constante à base de dados da Interpol. Notícia sobre a rede 24/7 disponível no site: < http://www.brasilcontraapedofilia.org/2008/05/03/interpol-faz-operacao-para-prender-foragidos-no-exterior/> Interpol faz operação para prender foragidos no exterior.
< http://pessoas.hsw.uol.com.br/interpol1.htm>

cooperação regional se mostra mais efetiva entre aqueles países de uma determinada região ou cultura.

Outros grupos de cooperação e resposta aos crimes cibernéticos são transitórios. Um recente grupo de combate aos crimes cibernéticos é composto pelos seguintes países: Chile, Espanha, Venezuela, Itália e Brasil. Ou seja, a Interpol verificou neste caso que esses países unidos têm o potencial de oferecer uma resposta mais rápida e efetiva a um determinado problema por diversos fatores; sejam eles culturais seja porque os determinados delitos têm ligação com criminosos que estejam utilizando equipamentos tecnológicos oriundos destes países.

Muitas vezes um país é convidado a fazer parte da força tarefa não porque está sendo cometido algum tipo de delito em suas fronteiras, mas porque reúne uma equipe que já enfrentou um problema semelhante no passado e soube dar uma resposta capaz de conter ameaça cibernética internacional. Retamal informou que quando reunidos profissionais em equipe, cada país geralmente arca com as despesas de seu homem durante as operações.

Quando um determinado grupo se reúne são definidos procedimentos e formas de trabalhos comuns, portanto uma lei que venha a disciplinar a apreensão e preservação de provas deve ser uniforme. De modo que uma mesma prova apreendida através de procedimentos adotados em um país possa ter validade na visão do Poder Judiciário de outro país. É cada vez mais comum que um criminoso pratique o delito em um País contra alvos muitas vezes em outros continentes. Se ambos os países envolvidos pretendem que estes criminosos sejam punidos é necessário que não apenas as políticas e estratégias sejam comuns, é necessário que a forma de convalidação e preservação das provas em ambos os países sejam semelhantes.

Na visão de Cristine Hoepers[40] – Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil CERT.br[41]/ NIC.br[42]/ CGI.br[43],a

[40] HOEPERS,Cristine. Cooperação Internacional. *In* Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008.

Cooperação que o Brasil vem adotando com outros Países é fundamental para que possa se preparar para enfrentar as futuras ameaças que vem surgindo em função do aumento de incidentes que vem sendo monitorado pelo CERT.br. Informou ainda a mencionada autoridade do (CERT.br) NIC.br/ CGI.br que o Brasil vem criando vários grupos especifico para monitorara e oferecer idéias ao Governo Brasileiro e empresas privadas quando são intimidadas por ameaças.Estes grupos atualmente são de diversos setores. Relatou que não são grupos de investigação, mas procuram gerar mecanismos para que o governo brasileiro possa responder e impedir aos ataques cibernéticos.

O grupo CERT.Br/NIC.br/CGI.br , atuam em uma rede de cooperação que conta nos dias de hoje como 180 grupos silenciosos ao redor do mundo, são os chamados *CSIRTS*[44]. Pela quantidade de *CSIRTS* hoje existentes ao redor do

---

[41] CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.
O CERT.br é o grupo de resposta a incidentes de segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. O CERT.br é responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil. Disponível:<http://www.cert.br/> Acesso 30 maio 2008.

[42] O Núcleo de Informação e Coordenação do Ponto br é uma entidade civil, sem fins lucrativos, que desde dezembro de 2005 implementa as decisões e projetos do Comitê Gestor da Internet no Brasil, conforme explicitado no comunicado ao público e no estatuto do NIC.br. Dentre suas atribuições estão: o registro e manutenção dos nomes de domínios que usam o <.br>, e a distribuição de endereços IPs, através do Registro.br; o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet brasileira, através do CERT.br; a promoção da infra-estrutura para a interconexão direta entre as redes que compõem a Internet brasileira, através do PTT.br; divulgação de indicadores e estatísticas e informações estratégicas sobre o desenvolvimento da Internet brasileira, através do CETIC.br;o suporte técnico e operacional ao LACNIC, Registro de Endereços da Internet para a América Latina e Caribe. Disponível:< http://nic.br/sobre-nic/index.htm> Acesso 30 maio 2008

[43] O Comitê Gestor da Internet no Brasil (CGI.br) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança na Internet pioneiro no que diz respeito à efetivação da participação da sociedade nas decisões envolvendo a implantação, administração e uso da rede. Com base nos princípios de multilateralidade, transparência e democracia, desde julho de 2004 o CGI.br elege democraticamente seus representantes da sociedade civil para participar das deliberações e debater prioridades para a internet, junto com o governo. Disponível:< http://www.cgi.br/sobre-cg/definicao.htm Acesso 30 maio de 2008.

[44] CSIRTs, do inglês Computer Security Incident Response Teams.

mundo, verifica-se a imensidão das ameaças que rondam o espaço cibernético prontas para o ataque a rede pública e privada de acesso a Internet .

O Senhor Adalton Martins[45], Chefe da Divisão de Repressão a Crimes Cibernéticos da Polícia Federal informa que a referida Unidade já prendeu cerca de 600 pessoas desde 2003, por ações contra o patrimônio, como roubo de senhas de bancos e cartões de crédito, pedofilia e até mesmo venda de drogas anabolizantes pela *Internet*.

Comenta que apesar disso, não há inquéritos abertos ou investigações em andamento sobre o jogo *on-line*, e hoje não encontra maiores obstáculos para conquistar os corações e o bolso dos brasileiros.

O chefe dessa divisão da PF, delegado Adalton de Almeida Martins, admite que o Brasil está atrasado no combate aos crimes praticados na rede mundial de computadores. "Ou a gente se especializa nisso, nas unidades Policiais, na Polícia Federal e nas Polícias Civis que já estão trabalhando nesses crimes em alguns Estados, ou vamos perder a guerra". Ouso divergir deste posicionamento uma vez que como dito anteriormente o Brasil conta com o Instituto Nacional de Criminalística da Polícia Federal como um dos mais modernos e completos do mundo.

O delegado menciona que na sua visão os brasileiros que ajudam a arregimentar apostadores para sítios de jogos, mesmo que estejam com base no exterior, podem ser responsabilizados como co-autores do delito, com pena prevista de até um ano. O grande problema, no entanto, de acordo com Adalton Martins é a falta de uma legislação nacional que tipifique os crimes na rede mundial de computadores. Por esse motivo, o Brasil não tem conseguido assinar acordos internacionais de cooperação para o combate aos crimes cibernéticos, como o acordo de Budapeste, ratificado há três anos pela União Européia.

A convenção foi assinada pelos países da Comunidade Européia no dia 23 de novembro de 2001, mas começou a valer em julho de 2004. Até março

---

[45] MARTINS,Adalton. Cooperação Internacional. Palestra proferida no Auditório Nereu Ramos, Brasília, 28 maio 2008. (Adalton Martins - Chefe da Divisão de Repressão a Crimes Cibernéticos da Polícia Federal)

deste ano, 19 países já haviam ratificado o tratado. O Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça ainda estuda os aspectos jurídicos da convenção, mas a maior dificuldade está na falta de leis específicas, no Brasil, sobre os crimes na *web*.

Mediante uma visita a superintendência da Polícia Federal verificou-se que em São Paulo a Polícia Federal ainda não tem uma unidade de trabalho formal para esses delitos. No Seminário Internacional Crimes Cibernéticos e Investigações Digitais da Câmara dos deputados no dia 28 de maio de 2008[46], o Delegado confirmou essa informação sobre a Polícia Federal.

Outro problema enfrentado pelos policiais é a lentidão nas investigações dos crimes ligados à Internet. Durante muitos anos a polícia se valeu de especialistas em informática para auxiliar nas investigações. Segundo relata, esse fato prejudicou algumas investigações e troca de informações, porque as informações iam para um *expert*, que sabia qual era o *software*, a placa-mãe e tudo, mas não sabia quem estava praticando o delito.

A Advogada Patrícia Peck[47] especializada em delitos digitais afirma que o IP[48] da máquina não pode ser confundido com o autor do delito. Ainda mais que

---

[46] Seminário Crimes Cibernéticos e Investigações Digitais.O Conselho de Altos Estudos e Avaliação Tecnológica, sensível à questão, promove, por iniciativa do Dep. Colbert Martins, o Seminário Crimes Cibernéticos e Investigações Digitais, com o objetivo de incorporar contribuições que possam aprimorar o substitutivo do Senador Eduardo Azeredo, com vistas a uma adequação do ordenamento jurídico brasileiro na reformulação da legislação relacionada à temática. Disponível: <http://www2.camara.gov.br/internet/eve/crimesDigitais/index.html > Acesso 30 maio 2008.

[47] Patrícia Peck Pinheiro - Advogada especialista em Direito Digital, formada pela Universidade de São Paulo, com especialização em negócios pela Harvard Business School e MBA em marketing pela Madia Marketing School. É autora do livro “Direito Digital” pela Editora Saraiva, além de participação nos livros e-Dicas e Internet Legal.

[48] Para que os computadores de uma rede possam trocar informações entre si é necessário que todos os computadores adotem as mesmas regras para o envio e o recebimento de informações. Este conjunto de regras é conhecido como Protocolo de comunicação. Falando de outra maneira podemos afirmar: “Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo protocolo de comunicação”. No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino, “entenda” as informações no formato que foram enviadas pelo computador de origem. Dois computadores com diferentes protocolos instalados, não serão capazes de estabelecer uma comunicação e nem serão capazes de trocar informações. Para se comunicar em uma rede baseada no protocolo TCP/IP, todo equipamento deve ter, pelo menos,

um computador pode estar em rede ou mesmo o criminoso na maioria das vezes utiliza o computador de outra pessoa para cometer ilícitos.

O Delegado Adalton de Almeida Martins afirma que atualmente a Polícia Federal realiza o monitoramento "telemático", explicando que esse tipo de monitoramento é feito a partir de programas criados especificamente para monitorar delitos na Internet, tudo com autorização judicial.

Jean-Charles De Cordes[49] que atua como Chefe da Divisão de Combate aos Crimes Cibernéticos e Crime Organizado do Conselho da Europa, afirma que atualmente o Conselho da Europa se preocupa em conhecer os padrões lógicos dos ataques relacionados aos crimes cibernéticos ocorridos em diversos continentes e países. Segundo ele, essas estatísticas são importantes para que se possa conhecer a forma de ataque e também os seus sistemas de propagação pela rede mundial de computadores.

Com estas informações a divisão de combate aos crimes cibernéticos do Conselho da Europa é capaz de traçar formas conjuntas de cooperação mais efetivas aos diversos incidentes que vem ocorrendo na Europa. O conselho ainda se preocupa com o bom equilíbrio e respeito para com as liberdades individuais, zelando sempre que possível para que a intimidade e privacidade do cidadão europeu sejam respeitadas. Recentemente foi assinado um protocolo com vistas ao combate a pedofilia.

Conforme diz o Professor Roberto Zanotti[50] tem merecido uma especial atenção por parte da Itália e dos demais países do Conselho da Europa as ações sistêmicas e coordenadas de combate à pedofilia. O Senhor Jean-Charles De Cordes menciona que realmente os países da Europa estão firmemente unidos

---

um número IP e uma máscara de sub-rede, sendo que todos os equipamentos da rede devem ter a mesma máscara de sub-rede".

[49] CORDES, Jean-Charles de. Convenção de Budapeste. *In* Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008.

[50] Professor Titular de Direito Penal Econômico da Escola Superior da Polícia Tributária e da "Accademia della Guardia di Finanza" e Direito Penal da "Università di Roma LUMSA". Membro Integrante da Delegação Oficial da Ordem dos Advogados de Roma. Advogado. Pesquisador. Autor de Obras Jurídicas. Conferencista no Primeiro Seminário Internacional de Direito Digital coordenado pelos Professores Antonio Carlos Morato e Liliana Minardi Paesani, ocorrido na FMU (Faculdades Metropolitana Unidas)

pelo ideal de combate a pedofilia e nesta missão tem contado com o governo brasileiro e suas autoridades como fortes aliados no combate aos crimes direcionados as crianças (em reportagem, Jean-Charles comenta acerca da cooperação entre países). Entende esse especialista que é importante a redação de um instrumento internacional completo e robusto capaz de trazer as definições técnicas necessárias para que todo um arcabouço de profissionais de diversos países possa trabalhar de uma forma integrada e uniforme, tornando assim uma mesma ação válida juridicamente em diversos países. Explica que se tivermos legislações sem uniformidade, uma prova que seja colhida pelo país membro do Conselho da Europa e que precise ser avaliada por uma Corte de um País que esteja fora das disposições estabelecidas pela Convenção de Budapeste, certamente esta Corte poderá tornar sem efetividade uma determinada ação policial destinada à coleta de provas.

Um grande problema enfrentado pelos países é o cumprimento de cartas rogatórias. Ele entende que as mesmas para terem efetividade devem ser trocadas e cumpridas on-line em tempo real sob pena de se tornarem vazias as ações das autoridades em diversos países. No futuro ainda teremos um judiciário que deverá funcionar também de forma on-line 24 (vinte e quatro) horas por dia, para expedição de mandados e proclamação de diversas decisões tais como a apreensão de provas e o decreto de prisão de potenciais criminosos perigosos.

A falta de uma metodologia e legislação[51] e auditoria são fatores a serem levados em consideração. Segundo Marcos da Costa, Diretor-Tesoureiro da OAB-SP e

---

[51] Retrospectiva 2005. Tecnologia impulsionou acesso à informação jurídica. Sobre os Cyber Crimes, muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, bem como na rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente, conforme Parecer da Comissão do Senado que discute atualmente o tema mencionado. Disponível: <http://conjur.estadao.com.br/static/text/40300,1
Disponível: <http://conjur.estadao.com.br/static/text/44818,1>. Fraude pela Internet
Policial que desviou dinheiro não tem liberdade. Parecer de 2.006, Da Comissão de Educação, sobre o Projeto de Lei da Câmara nº 89, de 2003 e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática, leia íntegra do Parecer no endereço http://conjur.estadao.com.br/static/text/45697,1. Para muitos doutrinadores, defendem

especialista em Direito de Informática "Há situações novas que configuram os chamados crimes atípicos, que clamam por uma legislação própria, pois não se enquadram nos tipos penais em vigor".[52]. Por conta dessa lacuna, a Polícia Federal[53] e a Justiça tratam de determinados delitos pela legislação comum.

Já no início de 2006, a imprensa anunciava que "A fraude virtual representa 80% da perda de bancos com roubo"[54]. Na verdade trata-se de furto qualificado. Exemplos não nos faltam diariamente desta modalidade criminosa, assim, esses crimes admitem sua consecução via Internet, por exemplo: pedofilia, violação de direito autoral, divulgação de segredos, furto ou roubo de informações, do roubo ou extorsão, furto, calúnia, difamação, injúria, falsa identidade, preconceito ou discriminação, crimes contra a inviolabilidade de correspondência, crimes contra propriedade intelectual e industrial, fraudes, engenharia social.

---

que, em tese, os estudos do Código Penal Brasileiro e da Legislação Complementar, teriam verificado que as condutas praticadas por meio eletrônico estão tipificadas na legislação existente. Acredito que face às anomalias existentes o rumo do Sistema Público de Escrituração Digital e da Nota Fiscal Eletrônica uma lei especial deve se aprofundar para a criação de novos meios de sua defesa que serão específicas e multidisciplinares aos seus meios. Já defendi em 2006 na FIESP sobre a necessidade de um protocolo de cooperação técnica entre o Instituto Nacional de Criminalística da Polícia Federal e a Administração Fazendária dos Estados. A Administração Tributária dos Estados publicou a recomendação, disponível: www.portalfiscal.se.gov.br/WebPortalFiscal/notaFiscalEletronica/materias_publicadas.jsp?news=principal.html - 20k . Acesso 24 maio 2008.

[52] Matéria de Capa do Jornal do Advogado da OAB-SP Nº 306 / maio de 2006.

[53] Comento que o monitoramento eletrônico melhorará em muito a eficácia da ação fiscal, mas outras janelas de sonegação existirão.

[54] O prejuízo causado por fraudes virtuais a bancos e administradoras de cartões cresceu 20%, atingindo R$ 300 milhões no ano passado, segundo estimativas do Instituto de Peritos em Tecnologias Digitais e Telecomunicações (IPDI). Até 1995, a totalidade das perdas era relacionada a roubos de agências. Entre 1995 e 2000, esse tipo de ocorrência representou 90% do valor do prejuízo e a clonagem de cartões, 10%. "Em 2004, 80% foram ocasionados por fraudes na internet, 10% por assaltos a agências ou seqüestros e outros 10% por clonagem", afirma o diretor do IPDI, Otávio Luiz Artur. A aceleração das ações criminosas no ambiente da web é preocupante, segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br). Em 2004, as tentativas de fraudes bancárias representavam apenas 5% dos incidentes de segurança da informação. Em 2005, esse percentual saltou a 40%. Os bancos investem fortemente em segurança interessados nos baixos custos do uso da internet banking. Enfrentam, porém, a ação agressiva de *hackers*, leia-se *crackers* e consideram que o fator humano - curiosidade, ganância e desconfiança - como no conto do bilhete premiado, (grifo nosso), ainda figura como calcanhar-de-aquiles. Gazeta Mercantil - 11/01/06 P.C1. Onde lê-se *hacker* o correto é *cracker,* comento.

Engenharia social, nas palavras de George Dawel (2005, p. 72), citando *SANS Intitute,* pode ser definida como sendo "a 'arte' de utilizar o comportamento humano para quebrar a segurança sem que a vítima sequer perceba que foi manipulada." De modo mais simples, as pessoas ingenuamente fornecem informações importantes por serem prestativas ou educadas e por confiarem nas outras pessoas. Pessoas mal intencionadas utilizam-se da Engenharia Social para conseguir informações preciosas para depois preparar seu ataque.

Importante mostrar o *modus operandi* do Engenheiro Social, definido de acordo com Marcelo e Pereira (2005):

> Traçar a trajetória de seu alvo, até conseguir um ponto do qual possa penetrar no mundo social ou empresarial do mesmo, é o objetivo inicial do engenheiro.
> O mesmo tem que criar um disfarce, seja elaborado ou não, para realizar o primeiro contato com o seu alvo. Normalmente as técnicas e formas mais utilizadas são as seguintes:
> a) contato telefônico – Deste modo o engenheiro tem como objetivo levantar as primeiras informações. Contudo ele toma sempre os seguintes cuidados:
>
> - Procura utilizar um aparelho telefônico público.
> - Procura identificar o cargo de cada pessoa na empresa.
> - Nunca tenta alguma coisa sem ter posse de todas as informações necessárias sobre: o local, pessoa(s), horários de trabalho, horário(s) de almoço/lanche, etc.
> - Procura não ser reconhecido por ninguém, no caso de visita ao vivo, se disfarça.
>
> O telefone é ainda uma das suas maiores ferramentas de ataque, ou seja basta levantar informações e poderá sim chegar ao seu alvo.
> b)Por *e-mail* – Com a utilização cada vez maior da *Internet*, muita coisa passou a ser feita via *e-mail*, incluindo envio de dados importantíssimos. A Engenharia Social se utiliza de forjar, ou melhor, passar por outro indivíduo ou organização para buscar informações do alvo. A instalação de Keyloggers e backdors disfarçados em arquivos tentadores (foto de mulheres nuas, relatórios importantes, etc.) ainda causam vítimas. E uma modalidade muito perigosa, o “fishing”, está ainda fazendo vítimas, principalmente de forma bancária.
> c) Engenharia Social *on the fly* – Esta modalidade é a mais ousada e arriscada para o engenheiro, já que ele aparece pessoalmente no alvo. Normalmente neste momento ele já está se passando por alguém, em busca de alguma informação sem importância. Pode estar se passando por um pesquisador de algum instituto, um vendedor, um faxineiro, funcionário de firma de manutenção, entregador, etc. Esta prática

> normalmente não e feita pelos iniciantes e requer um indivíduo experiente e dono de todas as informações necessárias.
> Essas três formas ainda provocam muitas situações com vítimas e com roubo de informações ou dinheiro. Não existe ainda o preparo necessário das pessoas para enfrentar essas situações.

Ainda sobre os delitos, incitação ao crime, apologia ao crime, crimes contra a segurança nacional, pirataria de todas as espécies, contrabando, tráfico de drogas, de crianças e de mulheres e até mesmo podendo chegar o *ciberterrorismo*. E sobre tal delito, diz Rover (2004), comentando a definição de Pollitt: (não tenho mais acesso a este livro) na internet deve ter informações completas da obra.

> [...] cyberterrorismo é o ataque premeditado, com motivação política contra o sistema de informações de um computador, programas de computador ou arquivos armazenados em sistemas de inteligência artificial resultando danos consideráveis a pessoas ou a coisas patrocinados por grupos descontentes com o sistema políticos vigente na sociedade. [55].

Citando como exemplo de práticas terroristas, o pesquisador Pedro Bueno em seu artigo "Cyber Crimes – a trilha do dinheiro" (2007), diz que as “técnicas de crimes cibernéticos utilizadas para financiar organizações criminosas incluindo o terrorismo são comuns em qualquer grupo criminoso”, relata sobre o financiamento do crime organizado e terrorismo – compra de armas, planos de treinamento militar e estratégico.

No Brasil já se tem registros de reconhecimento da prática de cibercrimes organizados. No anexo I trazemos o Habeas Corpus n.º 88905 [56], no qual o Ministro Relator Gilmar Mendes reconhece a prática de *cibercrime* organizado no Brasil. Trata-se de marco histórico de que estas atividades criminosas já estão em plena atividade no país. Ao decidir, o relator, ministro Gilmar Mendes, destacou que a hipótese dos autos evidencia que foi preso um dos chefes do grupo hierarquicamente organizado com o fim de praticar fraudes por meio da Internet,

---

[55] POLLIT, M.M “Cyberterrorism: fact or fancy?” Disponível:<http://www.cosc.geogetown.edu/~denning/infosec/pollitt.html.>Acesso em 15/5/2002.

[56] Disponível:<http://www.stf.gov.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=HC.SCLA.%20E%2088905.NUME.&base=baseAcordaos>. Acesso 23 maio 2008

concernentes à subtração de valores de contas bancárias a partir da utilização de programa de computador denominado *Trojan*[57]. Ainda destacou a Suprema Corte:

- Organização criminosa com poder de ação indeterminado e acelerado investimento dinâmico;
- Existência de enorme associação criminosa para cometer furto mediante fraude;
- Elogio do STF ao longo e primoroso trabalho da Polícia Federal e mencionando a relevância técnica de seu parecer e trabalho de investigação;
- Agências criminosas com grandes ramificações;
- Criminosos não se conhecem;
- O grupo é organizado hierarquicamente organizado, utiliza-se de técnicas sofisticadas;
- Facilidade para cometer cibercrime;
- Trabalho do crime em ritmo acelerado com novos envolvidos surgindo a cada momento; Organização do crime a distância;
- A extensão dos delitos nunca é plenamente conhecida;
- Ataque como ondas as fraudes podem ser perpetradas na privacidade da residência ou em outro local qualquer como escritórios e locais públicos o que dificulta a investigação[58].

---

[57] Também conhecido como Cavalo de Tróia, trata-se de um programa que age como a lenda do cavalo de Tróia, entrando no computador e liberando uma porta para um possível invasor.

[58] HC 88905 / GO – GOIÁS HABEAS CORPUS, Relator(a): Min. GILMAR MENDES,Julgamento: 12/09/2006 Órgão Julgador: Segunda Turma. Disponível: <http://www.stf.gov.br> Acesso 29 maio 2008.

Rômulo Dantas[59] – Diretor Nacional do Departamento de Anti Terrorismo - Agência Brasileira de Inteligência (ABIN) – entende que não cabe à Abin tratar dos crimes cibernéticos uma vez que, a Policia Federal Brasileira vem realizando um excelente trabalho no combate aos crimes da era da Informação Digital. Menciona que a Abin atua de forma analítica no combate ao terrorismo, acompanhando a sua evolução em diversas partes do mundo, sempre atenta para ações relacionadas ao *ciber-terrorismo*. A Abin analisa ainda as infiltrações e ações voltadas a espionagem com uso de computadores e de aparelhos de alta tecnologia de interesse nacional.

Rômulo Dantas menciona que a Abin monitora a Sociedade da Informação, citou, por exemplo, que 20% de toda a receita que o Talibã aufere em termos de receita 20% dela está voltada ao uso ilícito da Internet. O Talibã inclusive disponibiliza com um campo de treinamento para terroristas e se utiliza do espaço virtual. Explicou que atualmente o governo brasileiro entende que o Talibã e a Al-Qaeda são considerados como facções terroristas.

Segundo o professor Roberto Zanetti[60], o direito penal pode parecer um instrumento muito rígido e neste sentido pouco efetivo para o combate dos crimes cibernéticos. Tais crimes se manifestam de forma muito rápida na sociedade e pode parecer para muitos uma contradição, dizer que o direito penal será capaz de acompanhar a evolução deste fenômeno da era da informática. Salienta ainda que o ambiente digital torna o homem moderno animado por novas paixões que se refletem no mundo jurídico digital. Para os pesquisadores italianos, existe uma diferença entre o criminoso que bate uma carteira no metrô e aquele que se esconde atrás de um monitor de computador. O primeiro assume o risco de sofrer um ato de violência por parte de sua vítima ou mesmo assume para si a possibilidade de cometer contra a sua vitima um ato violento para obrigar-lhe a entregar seus pertences. Por outro lado, foi traçado pelos pesquisadores italianos

---

[59] DANTAS, Rômulo. Convenção de Budapeste. *In* Seminário Internacional 'Crimes Cibernéticos e Investigações Digitais'. Auditório Nereu Ramos, Brasília, 28 maio 2008.

[60] ZANETTI, Roberto. Responsabilidade Civil e Penal no Mundo Digital. Palestra proferida no Auditório da Casa Metropolitana do Direito FMU (Faculdades Metropolitanas Unidas) São Paulo, 30 maio 2008.

o perfil do criminoso que comete ilícito atrás de um computador. Estes dificilmente cometeriam ilícitos fora do ambiente cibernético, ou seja, para o Professor o criminoso se prende a figura do computador e passa a ter uma falta de percepção da legalidade e dos conceitos éticos que regem a sociedade ao seu redor. Tais criminosos, não teriam a coragem de praticar um crime no chamado mundo real, uma vez que, a tela do computador lhe dá uma falsa sensação de impunidade.

Para o Professor Zanetti a propagação da informática faz nascerem novos interesses que precisam ser protegidos. Para ele, surge o conceito de domicílio informático e de toda forma, precisa ser protegido e tutelado pelo Estado. O cidadão tem o direito de guardar as suas informações pessoais em seu computador e tem também o direito de não ver violado este novo domicílio informático repleto de informações caras a sua esfera intima e valorativa. Para os pesquisadores e estudiosos italianos é uma realidade a disseminação de novos instrumentos informáticos e tecnológicos voltados unicamente para a prática de ilícitos de toda a natureza. Neste sentido colocam em dúvida os novos conceitos sociais de liberdade e segurança. Na Europa a prevenção à criminalidade da informática constitui temática central das rodas acadêmicas, entendendo cada vez mais o pesquisador que somente através de atos e métodos de prevenção é possível fazer frente capaz de combater os crimes cibernéticos. Para o pesquisador Italiano “é preciso ter a consciência que na era digital estamos todos interligados e a partir de um ponto, ou do equipamento de uma pessoa em outro país pode-se atingir outras pessoas em pontos ainda mais distantes”.

Comenta ainda o pesquisador que na Itália as torcidas organizadas se comunicam através da Internet e muitas vezes sua utilização não é a mais adequada. Ou seja, grupos rivais também se enfrentam na rede e marcam confrontos no mundo real. A Internet é utilizada para influenciar de forma negativa o comportamento das pessoas incitar a violência ou mesmo para que sejam preparados ataques de um grupo contra o outro.

Mesmo com a adesão da Itália a Convenção de Budapeste uma série de condutas atípicas ainda surgem todos os dias para serem decididas pelos

Tribunais Italianos. De todo modo o citado Professor entende que as autoridades da Itália puderem se estruturar melhor suas ações de combate aos crimes cibernéticos após a adesão a Convenção de Budapeste.

É sem duvida um grande desafio criar uma lei e com ela mecanismos de combate ao crime cibernético virtual e explico: qualquer lei ou diploma que venha a ser criado deve ter o poder de fazer frente a todos estes novos fenômenos da era da criminalidade virtual.

De forma oposta, existem condutas que a ação do sujeito pode se originar de pessoas que não estejam filiadas a organizações criminosas e que não são terroristas (BARROS, 2007, p. 287) os estudiosos nos trazem como exemplos: o acesso indevido de *crackers* ou *hackers.*

Ainda, existem outros milhares de exemplos desta espécie: v.g. alteração de senhas ou de meio de acesso a programas computacionais, criação, inserção em computador de dados de programa de computador com fins nocivos, violação de segredos armazenados em computador, obtenção e manutenção indevida de dados não autorizados.

As condutas em que o agente tem por objetivo a capturar um bem jurídico ao próprio sistema informático, aquelas que o objeto da ação causa lesão ou apagam bens ou dados de informática, fogem a esfera da proteção penal. Note-se que a particularidade da ação criminosa impede dd se subsumir o ato censurável a qualquer tipo pena: o conceito de “dado” ou “informação eletrônica”, em tese não se equipara a “coisa” descrita no Código Penal, o que inviabiliza a aplicação dos crimes contra o patrimônio.

Também não existe previsão legal para tipificação do sujeito ativo do delito relacionado sempre a um número de protocolo de navegação na Internet. Isso porque a máquina deste suposto agente, não raro, pode estar sendo controlada por terceiros criminosos. Também não existe previsão legal para a alteração de senha ou de meio de acesso, ou ainda de desvio de meio de acesso no caso de conexões com a rede que é desviada para páginas falsas. Também

não existe previsão legal para criação e disseminação de programa ou dados com fins nocivos e maliciosos.

2.1.1 Legislação brasileira em relação aos cibercrimes.

No Brasil, essas modalidades criminosas ainda estão caminhando lentamente, existem Projetos de Lei em tramitação no Senado, dentre eles, podemos destacar PLC 89/03, PLS 76/00 e PLS 137/00 – que tipificam os crimes de "roubo" de senhas pela Internet, a falsificação de cartões de crédito, a difusão de vírus, a divulgação de bancos de dados, o racismo e a pedofilia praticados pela Internet, entr outros delitos. O relator destes projetos é o Senador Eduardo Azeredo, que em entrevista à Agência Senado[61] afirmou que Jean-Charles de Cordes e Marco Gercke (membros do Conselho da Europa) reiteraram a posição do Conselho da Europa, o qual defende a adesão do Brasil à Convenção de Budapeste, que trata dos chamados cibercrimes.

Destacam-se também a seguir legislações inseridas para coibir algumas condutas puníveis relacionadas à informação, dentre elas:

> Inserção de dados falsos em sistema de informações, artigo 313-A, consistindo em inserir ou facilitar, o funcionário[62] autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

---

[61] Eduardo Azeredo e membros do Conselho da Europa discutem legislação sobre crimes cibernéticos. notícia disponível: <http://www.senado.gov.br/agencia/verNoticia.aspx?codNoticia=75288&codAplicativo=2.> Acesso em maio de 2008.

[62] NUCCI, Guilherme de Souza, Código penal comentado. São Paulo: Revista dos Tribunais, 2007, p. 1001. Sujeito ativo e passivo: O sujeito ativo somente pode ser funcionário público e, no caso presente, devidamente autorizado a lidar com o sistema informatizado ou banco de dados. O funcionário *não autorizado* somente pode praticar o crime se acompanhado de outro, devidamente autorizado. O sujeito passivo é o Estado e, secundariamente, a pessoa prejudicada.

Nucci (2007, p. 1001) exemplifica que “seria eliminar a informação de que algum segurado faleceu, fazendo com que a aposentadoria continue a ser paga normalmente”.

> Modificação ou alteração não autorizada de sistema de informações, artigo 313-B, que diz, modificar ou alterar, o funcionário (idem), sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Existe a majorante no parágrafo único que indica:

> Parágrafo único: As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Do mesmo modo, Nucci (idem, p. 1003) comenta:

> A primeira conduta implica em dar nova forma ao sistema ou programa, enquanto a segunda tem a conotação de manter o sistema ou programa anterior, embira conturbando a sua forma original. O objeto é o sistema de informações ou programa de informática

Houve também outra alteração no Código Penal no artigo 153, acrescentado pela Lei n.º 9.983/2000 que diz:

> Artigo 153 (...)
> §1º-ª Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
> Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

Com efeito, Nucci (2007, p. 659) analisa o tipo penal:

> A finalidade do tipo penal é impedir que uma pessoa, legítima destinatária de uma correspondência ou de um documento, que contenha um conteúdo confidencial (segredo é o que não merece ser revelado a ninguém), possa transmiti-lo a terceiros, causando dano a alguém. É indispensável que o segredo esteja concretizado na forma escrita, e não oral.

Diz também que o sujeito ativo pode ser qualquer pessoa, desde que tenha acesso, ou seja, detentor da informação sigilosa ou reservada.

A mesma Lei acrescentou o parágrafo primeiro e incisos I e II ao artigo 325, que diz:

> § 1º, inciso I, do Código Penal: Permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.
> § 1º, inciso II, do Código Penal: Utilização indevida do acesso restrito.

É importante observar que nos artigos 313-A e 313-B a tutela é a segurança do sistema de informações da Administração Pública e não de entidades particulares.

Merece consideração o recurso interposto no Tribunal de Santa Catarina por violação ao artigo 313-A do Código Penal (RAMOS JUNIOR, 2007):

> Apelação criminal - Inserção de dados falsos em sistema de informações (Art. 313-A do Código Penal) – Autoria e materialidade devidamente comprovadas – Servidora pública que a pedido de seu namorado, despachante, inseria dados falsos no sistema do CIRETRAN, liberando os certificados de licenciamento de veículos – Taxas de licenciamento de veículos não recolhidas – Desclassificação para o delito de prevaricação – Condutas que ultrapassam os limites expressos no art. 319 do Código Penal – Diminuição da pena – Arrependimento posterior – Delito praticado por dezessete vezes em continuidade delitiva, demonstrando fragilidade do arrependimento – Aumento que se mostra adequado, considerando o número de reiterações praticadas – Crime praticado em detrimento da Administração Pública Pena superior a um ano – Perda da função pública – Efeito da condenação – Recursos desprovidos.
> Tratando-se de condenação por crime praticado com abuso de dever ou violação de dever para com a Administração pública, dispensável a indicação dos motivos da decretação por estarem ínsitos na própria fundamentação do convencimento do delito praticado contra a Administração, por serem comuns, devendo a exigência de fundamentação ser específica apenas para os demais casos tratados no art. 92 do Código Penal. (TJSC, Apelação criminal n.º 2004.028935-4, de Itajaí, Rel. Des. Sólon D'Eça neves, data do julgado 19/07/2005).

Também é de importância destacar o recurso de apelação negado no Tribunal Regional Federal da 4ª Região (RAMOS JUNIOR, 2007):

> Apelação criminal. Art. 313-B e Art. 327, § 1º, ambos do Código Penal. Modificação e alteração não autorizada de sistema de informação da UFRGS. Processo administrativo disciplinar realizado no âmbito da universidade. Réu confesso. Prova testemunhal uníssona. Materialidade e autoria comprovadas. Dano demonstrado. Condenação.

> As provas colhidas no Processo Administrativo Disciplinar realizado no âmbito de Universidade, posteriormente ratificadas integralmente em juízo, são aptas a ensejar condenação.
> O réu que, na condição de bolsista (estagiário) do Centro de Processamento de Dados da UFRGS, desempenha função pública é, para fins penais, equiparado a funcionário público.
> Para a configuração do delito tipificado no art. 313-B do CP é irrelevante o prejuízo, o qual, se ocorrer, poderá ensejar a causa de aumento de pena prevista no parágrafo único do mencionado artigo.
> No caso de resultar dano para a Administração ou para o administrado, incide a majorante prevista no parágrafo único do art. 313-B, ainda que o prejuízo não seja de natureza patrimonial.
> Apelação desprovida. (TRF 4º Região, Apelação Criminal n.º 2005.71.00.016873-9/RS, Rel. Des. Federal Maria de Fátima Freita Labarrère, publicado no D.J.U. 11/10/2006).

Nessa mesma temática o artigo 241 do Estatuto da Criança e do Adolescente foi alterado pela Lei n.º 10.764/2003 que diz:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou *Internet*, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
> Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa.

Nesse sentido, Nucci (2007, p. 238 e 239) leciona: “a figura típica tem por escopo atingir todos os meios de comunicação, em especial a rede mundial de computadores (Internet)." Vale registrar que a anterior redação do art. 241, até o advento da Lei 10.764/2003, era o seguinte: “Fotografar ou publicar cena de sexo explícito ou pornografia envolvendo criança ou adolescente” (*idem*)

> A simples tomada de fotos não mais é considerada criminosa. Destarte, a ação descrita na exordial (fotografar) passou a ser atípica, face a nova redação dada ao art.241 do ECA.

As denúncias em relação a crimes de pedofilia vêm também aumentando no último ano.

> Relatório da *SaferNet*, ONG responsável pela Central Nacional de Denúncias de Crimes Cibernéticos, contabiliza mais de 35 mil denúncias, apenas em 2008. Somente de pornografia infantil, motivo da maioria das queixas, são cerca de 500 por dia.[63]

[63] NEVES, Guilherme. Flagrante de pedofilia no Orkut. Como agir? Disponível: <http://www.clicrbs.com.br/blog/jsp/default.jsp?source=DYNAMIC,blog.BlogDataServer,getBlog&uf=1&local=1&template=3948.dwt&section=Blogs&post=58651&blog=153&coldir=1&topo=3994.dwt> Acesso 30 maio 2008.

Vários escândalos relacionados com o crime supra citado estão sendo solucionados pela Polícia Federal e a CPI (Comissão Parlamentar de Inquérito) da Pedofilia, como exemplo podemos citar os crimes contidos na página de relacionamentos Orkut, "Álbuns do Orkut revelam ação de pelo menos 500 pedófilos, diz CPI"[64] Outras notícias veiculadas a respeito dos crimes de pedofilia cometidos com o auxílio da rede podem ser facilmente encontradas, como o reconhecimento da Câmara da pedofilia como crime hediondo[65] ou informações sobre o perfil do pedófilo brasileiro como sendo, em sua maioria, homens que têm entre 18 a 55 anos e faz parte das classes A, B e C[66].

No que diz respeito às denúncias para esses tipos de delitos, ela é feita conforme as informações obtidas no sítio www.denunciar.org.br*,* que é o portal da Central Nacional de Denúncias de Crimes Cibernéticos:

> Uma equipe de Analistas de Conteúdo, com formação em Direito e Ciências da Computação irá, com ajuda de ferramentas específicas, realizar uma verificação prévia dos dados recebidos. Terminada a verificação prévia, inicia-se a análise do conteúdo da denúncia propriamente dito, ocasião em que nossos analistas irão identificar ou não indícios que possam confirmar a materialidade de um ou mais crimes contra os Direitos Humanos e cuja ação penal seja pública e incondicionada a representação. Vale dizer a equipe de analistas de conteúdo além de processar as denúncias recebidas também realiza periodicamente um monitoramento dos principais serviços da rede Internet no Brasil, com o objetivo de identificar novos incidentes e registrar os indícios de crime(s). Esta ação é denominada de rastreamento pró-ativo.
>
> Comprovada a existência de indícios de crime(s), parte-se para o rastreamento das informações relevantes disponíveis publicamente na Internet com o objetivo de comprovar a sua materialidade e documentar o modus operandi e os indícios de autoria, não sendo feita nenhuma

---

64 Álbuns do Orkut revelam ação de pelo menos 500 pedófilos, diz CPI ALBUNS+DO+ORKUT+REVELAM+ACAO+DE+MAIS+DE+PEDOFILOS+DIZ+CPI.html. Disponível: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL456247-6174,00>Acesso 07 maio 2008.

65 Comissão da Câmara classifica pedofilia como crime hediondo. Disponível:<http://www.migalhas.com.br/mostra_noticia.aspx?cod=60720> . Acesso 18 maio 2008.

66 Pedófilo brasileiro é mais consumidor do que produtor de conteúdo e faz parte das classes A, B e C. Disponível em <http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia20080415204853>. Acesso 30 maio 2008

> ação de invasão ao meio investigado ou qualquer outra forma de intervenção que extrapole os limites de investigação permitidos as instituições da sociedade civil dedicadas a Defesa dos Direitos Humanos.
>
> A equipe de analistas de conteúdo, de posse das informações e evidências coletadas, produz um relatório de rastreamento e o encaminha para o Diretor de Rastreamento e Análise de Conteúdo, cargo preenchido exclusivamente por bacharel em Direito com especialização em Direito da Informática e Internet, que irá analisar, com base na legislação penal e processual penal em vigor no Brasil, e a partir dos princípios gerais do Direito e das garantias constitucionais, se há indícios suficientes para que a autoridade responsável pela persecução penal possa confirmar a materialidade do(s) crime(s) e instaurar o processo formal de investigação policial e a posterior propositura da competente ação penal.
>
> Esta notícia-crime fundamentada será enviada para o Grupo de Combate a Crimes Cibernéticos do Ministério Público Federal nos casos que guardem relação com o Estado de São Paulo, e para a Divisão de Direitos Humanos da Polícia Federal em Brasília caso as evidências coletadas envolvam outros Estados da Federação. As denúncias que não contenham evidências relacionadas ao Brasil serão encaminhadas aos Canais de Denúncia internacionais, sendo enviado um relatório simplificado e de caráter informativo para o conhecimento da autoridade brasileira.
>
> Por fim, o prestador do serviço, caso esteja estabelecido ou mantenha filial no Brasil, é notificado formalmente para proceder a remoção do material ilegal da Internet e preservar todas as provas da materialidade do(s) crime(s) e os indícios de autoria.
> Para manter a qualidade dos serviços prestados à sociedade, a SaferNet Brasil criou procedimentos de controle de qualidade e auditoria interna e externa. A instituição utiliza diversas técnicas para identificar, analisar e corrigir problemas que porventura posam ocorrer, a exemplo de ferramentas estatísticas de medição de consistência de dados, seleção aleatória de amostras para auditoria interna, etc. Além da transparência e controle externo por parte das instituições parceiras e dos denunciantes, possibilitada pelo acompanhamento em tempo real do andamento da(s) denúncia(s).[67]

A efetividade da justiça depende de diversos fatores, dentre eles da recepção das mudanças tecnológicas pelo Direito Processual, seja no âmbito cível, seja no criminal, bem como pelo judiciário e todos os órgãos envolvidos nesta tarefa. Isso tem ocorrido, entretanto, em velocidade muito aquém daquela com que caminham os avanços tecnológicos.

---

[67] Como Funciona a Central Nacional de Denúncias. Disponível< http://www.denunciar.org.br/twiki/bin/view/SaferNet/ComoFunciona> Acesso 30 maio 2008.

Muito tem sido feito no que tange à atuação dos órgãos incumbidos do combate e prevenção da criminalidade informática. Contudo, face ao dinamismo dos avanços tecnológicos, ainda há um descompasso. Uma das atitudes louváveis que podemos apontar foi a criação de delegacias ou núcleos de investigações especializados, tais como: DIG-DEIC – 4ª Delegacia de Repressão a Crimes de Informática de São Paulo (SP); DERCIFE (Delegacia Especializada de Repressão a Crimes contra Informática e Fraudes Eletrônicas), em Belo Horizonte (MG); DRCI – Delegacia de Repressão aos Crimes de Informática, no Rio de Janeiro (RJ), dentre outras.

No âmbito da Polícia Federal, a perícia de informática teve início em 01/11/1995. Posteriormente em 1996 foi criada a Unidade de Perícia de Informática da Polícia Federal. Em 2003 recebeu a denominação atual de SEPFIN (Serviço de Perícia em Informática).

O Brasil saiu na frente, já no início de 2005, o Instituto Nacional de Criminalística da Polícia Federal em Brasília já despontava para toda comunidade científica internacional como um dos mais modernos e completos do mundo (INC), constituindo mais uma arma a ser utilizada contra as ações criminosas praticadas na rede.

Temos, ainda, outras medidas, algumas de iniciativa privada, tais como: a criação da SaferNet Brasil, organização não governamental, que através da Central Nacional de Denúncias de Crimes Cibernéticos, operada em parceria com o Ministério Público Federal, oferece à sociedade brasileira e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da Internet.[68] Ademais, temos a Cartilha de Segurança da Internet, que contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet, disponibilizado pelo centro de estudos, resposta e tratamento de incidentes de segurança no

[68] Disponível:<http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome.> Acesso 30 maio 2008.

Brasil (que pode ser encontrada em http://cartilha.cert.br/). Nesse sentido, o Perito Criminal da Superintendência da Polícia Técnico-Científica de São Paulo, Orlando Ruiz, defende a necessidade de uma maior integração entre governo, usuários e a iniciativa privada para combater os crimes pela Internet. Segundo ele, esta medida traria maior eficiência contra os fraudadores do que a criação de leis específicas para crimes on-line.[69]

Não se pode deixar de mencionar a importância para o Brasil da Criação da Comissão do Direito na Sociedade da Informação da OAB/SP. A gênese da Sociedade da Informação constitui um corolário lógico de diversos processos de desenvolvimento, dentre os quais a globalização, que estimulou a idéia de infra-estrutura global de informação, propiciando a abertura das telecomunicações.

E como não poderia deixar de ser, o estudo dos crimes cibernético esta elencado dentre os objetivos de Comissão[70] de Direito na Sociedade da Informação da Ordem dos Advogados do Brasil Secção de São Paulo que reúne Professores e Pesquisadores do Brasil e do exterior.

2.2 - Mundos Virtuais e o Second Life – Estudo de Caso

Os mundos virtuais são simuladores de vida, desenvolvidos em plataforma MMORPG (*massively multi-player on-line role playing game*), pode-se dizer que são mais complexos do que os conhecidos jogos on-line porque possuem economia própria, têm influência no comportamento e no tempo de permanência de coneção das pessoas e determinam o crescimento do número de usuários conectados à rede Internet. São milhões de habitantes cadastrados nesses mundos que encontram-se localizados em vários continentes.[71]

---

[69] União entre usuários, governo e iniciativa privada aumenta a eficiência do combate a crimes virtuais. Disponível:<http://www.internetsegura.org/noticias/releases.asp?temp=5&id=35>. Acesso 20 junho 2007.

[70] Disponível:<http://www2.oabsp.org.br/asp/comissoes/comissao.asp?id_comissao=125&opcao=1> Acesso 25 maio 2.008.

[71] Disponível: <http://www.gamestudies.org/0302/castronova/. Acesso abril 2007.

Denominam-se ainda os mundos virtuais com as expressões: mundos sintéticos ou metaversos. Todavia, independente do vocabulário utilizado, a análise jurídica, econômica, social e cultural, dispensada aos referidos mundos na sociedade contemporânea, é que está suscitando estudos em diferentes países.

Dessa forma, não é possível considerar o *Second Life* apenas um jogo on-line. Cabe salientar não há vencedor ou perdedor, tão pouco objetivo específico ou temática de jogo. Por outro lado, são estabelecidas regras de conduta para tornar saudável e harmoniosa a convivência no ambiente tridimensional. Essas regras impostas pelos proprietários da plataforma, que também são os fornecedores de serviços, ou seja, é simplesmente uma segunda vida em meio virtual, ou um simulador de vida real.

Cabe destacar que ao tratarmos de conceitos, a doutrina e a jurisprudência inclinam-se por afirmar que os mundos virtuais são relativamente diferentes dos jogos on-line[72], distintamente dos autores que afirmam serem simplesmente uma versão atualizada e mais ampla. No entanto, a imprecisão por uma classificação doutrinária acarreta uma utilização ambígua da palavra "jogadores", freqüentemente empregada nos estudos científicos e nas notícias veiculadas na mídia. Os termos "usuários" e "habitantes", também são largamente utilizados com a mesma acepção.

Os metaversos pertencem geralmente a empresas privadas, que são as responsáveis pelo desenvolvimento dos programas, criação artística, administração e a funcionalidade das plataformas. Os proprietários[73] dos mundos virtuais são conhecidos como "*Gods*", visto que, em tese, são eles que ditam as

---

[72] "Some degree of confusion and category mistake would almost inevitably result from judicial attempts to interpret traditional criminal laws in order to police player behaviors in virtual worlds. Ironically, if we wish to preserve the benefits of virtual worlds as free and independent social experiments, it may be best if we keep the criminal law at a safe distance". Pág. 7. BALKIN**,** Jack M.; NOVECK, Beth Simone. ***The State of Play: law, games, and virtual worlds***. New York: New York University Press, 2006.

[73] The powers that virtual-world administrators wield are embedded in the coded rules of the virtual world, which the administrators themselves define. If this were not the case, they could not protect the game conceit.(…) Administrators of virtual worlds that feature achievement are able to change the coded rules of their virtual world retrospectively and without warning, under conditions they need only specify after the event. If this were not the case, the virtual world's ability to support identity exploration would be compromised. Balkin e Noveck, 2006, p. 43

regras apresentadas e os direitos e deveres constantes dos termos de utilização dos usuários habitantes.

Na busca permanente pela melhor forma de delinear as novas tecnologias, os mundos virtuais aperfeiçoam suas plataformas nos aspectos gráficos e funcionais, alcançando um dos principais objetivos que é representar virtualmente com detalhes minuciosos os seres humanos e o mundo real em que vivemos. É importante dizer que os habitantes dos metaversos nem sempre estão satisfeitos com as regras impostas pelos proprietários das plataformas, principalmente quando o conflito está relacionado aos direitos de propriedade intelectual sobre bens virtuais. Alguns habitantes tendem a ultrapassar os limites impostos pelos donos das plataformas, como exemplo[74]: é a venda fora do ambiente tridimensional de bens virtuais, que são proibidas pelas regras estabelecidas em muitos dos mundos virtuais.

Também no mesmo contexto podemos citar o caso judicial entre *Marc Bragg vs. Linden Lab*, no qual o autor reclama que seus bens virtuais, com valores estimados em US$ 8 mil, foram confiscados pela própria *Linden Lab.* Em sua defesa, a empresa afirma que os bens declarados pelo autor da ação foram adquiridos através de atos ilícitos. Resumindo, a ação envolve conflitos relacionados a fraude, violação de direitos de propriedade intelectual, direitos do consumidor e relação contratual[75].

Valem algumas considerações sobre os vários fatores que compõem o quadro do aumento do número de participantes nos mundos virtuais, e sua

---

[74] Disponível: <http://mail-b.uol.com.br/cgi-bin/webmail/lastowka.pdf>. Dan Hunter e F. Gregory Lastowka citam outros crimes praticados nos mundos virtuais - “Criminal activity involving virtual property and virtual currency was a foregone conclusion as soon as the property and currency became sufficiently valuable in the real world. A Japanese man hacked into another person’s virtual world account, sold her virtual house, and pocketed the proceeds. In South Korea, a 22 year old student named Choi and an accomplice manipulated a virtual world server and made off with 1.5 billion won, or approximately US$ 1.2 million. While in other reports from Korea, gangs of youths rampage across servers, looking and pillaging other people’s virtual property, and selling it off in the real world. And Indiana, a known author fenced a stolen magic mace and bragged about it on his blog.” – Virtual Crimes Dan Hunter and F. Gregory Lastowka. Acesso abril 2007.

[75] Disponível <http://www.paed.uscourts.gov/us01000.asp > Civil Action nº 06-4925 in The United States District Court for the Eastern District of Pennsylvania. Acesso agosto 2007.

influência na sociedade, dos quais podemos citar as novas tecnologias de informação e telefonia, o crescente acesso pela população à rede Internet e o baixo custo dos computadores pessoais. Esses elementos, somados à ânsia cada vez maior por interação social, informação e consumismo, estão fazendo com que pessoas passem mais tempo conectadas aos metaversos e passem a viver uma segunda vida, uma vida virtual, em um mundo também virtual, mas que têm conteúdo essencial e reflexos produzidos no mundo real, no ordenamento jurídico, na sociedade, na economia e na política.

Em períodos recentes, as salas de bate-papo (*chats*), fóruns de discussões, comunidades virtuais (*orkut, myspace*) eram os meios de comunicações on-line mais freqüentemente utilizados pelos internautas. Porém, os mundos virtuais estão paralelamente agregando desenvolvimento diverso ao *cyberspace.* Milhões de pessoas espalhadas pelo mundo, hoje habitam os mundos virtuais como o *Britannia, Norrath, The Sims On-Line, Blazing Falls, Second Life*, para ficar apenas em alguns exemplos desses mundos.

O *Second Life* é um mundo virtual, tridimensional, conectado à Internet banda-larga, e a um computador criado pela "Linden Lab"[76], e largamente desenvolvido sob a influência de 8 milhões[77] de internautas. É preciso frisar que no novo meio virtual é possível investir recursos financeiros, estudar, trabalhar, casar, ter filhos, procurar ou oferecer empregos, namorar, comprar ou vender coisas reais e virtuais, praticar atos de vandalismo e até crimes dos mais perniciosos como os de pedofilia.

Algumas estimativas da plataforma *Second Life* demonstram a sua real importância, com economia própria, e uma moeda diferenciada (o "*Linden* Dólar – L$") que tem sua cotação atrelada ao dólar real, tendo seu PIB anual estimado em 220 milhões de dólares, sua economia virtual desenvolvendo-se à taxa de 300% ao ano, com uma movimentação mensal de US$ 18 milhões.[78]

---

[76] Empresa americana, sediada na Califórnia/EUA

[77] dados de agosto de 2007 do site <http:// www.secondlife.com > Acesso agosto 2007.

[78] VIEIRA, Eduardo. Por que os mundos virtuais como o *Second Life* podem representar o início de uma nova era na web. Disponível em

O usuário da plataforma *Second Life* utiliza-se de um avatar[79]. Trata-se de personagem ou representação corporal digital e virtual criada para representá-lo no metaverso que recebe nome e sobrenome, o que é uma exigência para entrar no mundo virtual. O avatar pode ser criado espelhando-se na real imagem de seu criador, ou seja, de um ser humano, ou pode ter a semelhança de um animal ou até mesmo de um extraterrestre. Tais fatores podem ser aparentemente irrelevantes, mas aparência dos avatares representa para o seu criador uma identidade e um direito de propriedade intelectual.

Cumpre destacar que os mundos virtuais a exemplo do Second Life estão sendo analisados, pesquisados e noticiados em várias partes do mundo e em diferentes áreas, onde são realizados convenções, fóruns internacionais, seminários acadêmicos e divulgação ampla na mídia em geral, como também, em pesquisas empíricas. É extremamente relevante à discussão sobre o futuro dos mundos virtuais e os impactos que esses novos meios de imersão on-line estão causando na sociedade, principalmente para a área jurídica relacionadas aos aspectos criminológicos.

2.2.1 - Os crimes cometidos no *Second Life*

Os mundos virtuais existem desde 1985, como exemplo a plataforma *Habitat.* Assim, é importante ressaltar que os metaversos são mais complexos do que apenas jogos on-line e, por outras palavras, é um equivoco afirmar que se trata apenas de uma nova forma de entretenimento.

Em que pese o destaque da importância desses mundos, cumpre destacar que muitas pessoas que hoje habitam esses metaversos estão

---

<http://revistaepoca.globo.com/Revista/Epoca/0,,EDG76738-5990-461,00.html> Revista Época. Acesso 19 março 2007.

[79] Avatar – Rubrica: religião. Na crença hinduísta, descida de um ser divino à terra, em forma materializada. Particularmente cultuados pelos hindus são Krishna e Rama, avatares do deus Vixnu; os avatares podem assumir a forma humana ou a de um animal. - 2 - processo metamórfico; transformação, mutação.” Dicionário Houaiss da Língua Portuguesa

vivenciando conflitos reais e não apenas virtuais, tais como: invasão de privacidade, ofensas à imagem, honra, propriedade, intimidade, além de ilícitos como estelionato, contrabando, roubo, formação de quadrilha, terrorismo, lavagem de dinheiro, pedofilia, etc.

Recentemente o *Second Life* foi alvo de ações que a mídia eletrônica rotulou como terrorismo virtual[80], quando uma de suas Ilhas virtuais teria sido atacada por avatares em helicópteros, equipados com bombas atômicas, armas automáticas e AK47s. Não foi possível qualquer reação para evitar o atentado e inevitavelmente a destruição causou danos financeiros consideráveis aos proprietários da Ilha afetada. Trata-se de apologia[81] ao crime.

Talvez chamar de terrorismo esses atos de vandalismo virtual seja um pouco fora de propósito, entretanto cumpre salientar que os mundos virtuais são utilizados para diversos crimes cibernéticos. Não é ilusório, nem hipotético, afirmar que o *Second Life* pode ser utilizado entre outras coisas, para difundir, recrutar, treinar e instruir terroristas. O ato classificado como terrorismo, exposto acima, foi praticado por um grupo radical que se intitula *Second Life Liberation Army*[82], que aponta para uma possível ramificação de terroristas do mundo real.

Essa tese é reforçada pelo fato de que até o exército americano utiliza-se de metaversos para dar treinamentos e simular situações de combate, ou mesmo recrutar soldados para batalhas (BALKIN e NOVECK, 2006, p. 3). Isso talvez

---

80 "Virtual terrorists - Hunted in reality, jihadists are turning to artificial online worlds such as Second Life to train and recruit members, writes Natalie O'Brien | THE bomb hit the ABC's headquarters, destroying everything except one digital transmission tower. The force of the blast left Aunty's site a cratered mess. Just weeks before, a group of terrorists flew a helicopter into the Nissan building, creating an inferno that left two dead. Then a group of armed militants forced their way into an American Apparel clothing store and shot several customers before planting a bomb outside a Reebok store." Disponível: <http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html Acesso em agosto 2007.

81 Silva, Paulo Quintiliano dos "Crimes Cibernéticos e seus efeitos internacionais" In: Anais: Procedings of the Firts International Conference on Forensic Computer Science Investigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124pp.-ISSN 19180-1114,vide página 12. Apologia ou ao fato criminoso são alguns dos delitos apontados pelo Cientista em sua obra.

82 Disponível: <http://www.itnews.com.au/News/46333,cyberterrorists-storm-second-life.aspx>

explique de uma forma simplificada a possibilidade real da existência de terroristas no *Second Life* ou em outro metaverso.

Valem algumas considerações sobre a reportagem divulgada na TV alemã SWR, que transmitiu cenas de avatares do *Second Life* praticando atos de pedofilia. As imagens polêmicas foram apresentadas no "*Report Mainz*"[83], revelando um avatar masculino adulto praticando atos pornográficos com um avatar infantil. Diante desses fatos, a polícia alemã, ao investigar o caso, constatou que os pedófilos freqüentadores do *Second Life* não apenas simulava sexo com menores como também enviavam por e-mail fotos de crianças reais sendo abusadas sexualmente. Conforme informação do jornal britânico *The Guardian* esses encontros virtuais proibidos dentro do metaverso eram vendidos para outros avatares interessados por L$ 500, moeda local do *Second Life.* Paralelamente aos encontros, também era possível a troca de informações, fotos, e-mails e vídeos.

Os responsáveis pelas cenas transmitidas pela TV alemã foram identificados com a ajuda da *Linden Lab,* proprietária da plataforma *Second Life.* Essas pessoas poderão responder a processo criminal por oferta de pornografia de terceiros e cumpre ressaltar que, se forem condenados, terão que cumprir pena de 3 meses a 5 cinco anos de prisão, conforme determina a legislação alemã[84]. Pelo andamento das investigações, os executivos proprietários do *Second Life* também são passíveis de condenação[85].

---

[83] Disponível: <http://www.australianit.news.com.au/story/0,24897,22161699-15306,00.html> – Acesso agosto 2007.

[84] InternetspieleTummelplatz für Kinderpornografie - Moderation Fritz Frey - Peter Vogt, Oberstaatsanwalt Halle: »Wir werden versuchen diese Person namhaft zu machen. Sollte uns das gelingen, hat die Person mit einem Strafverfahren wegen Drittbesitzverschaffung von Kinderpornografie zu rechnen, und dieser Straftatbestand wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren geahndet.« Erstmals wird strafrechtlich ermittelt in Sachen Kinderpornografie und Second Life. Doch die virtuelle Welt wächst weiter, Tag für Tag. Inzwischen hat Second Life über sechs Millionen Mitspieler. Disponível: <http://www.swr.de/report/-/id=233454/nid=233454/did=2060062/1h0wega/index.html> – Acesso agosto 2007.

[85] "Il est possible que les lois contre la pornographie enfantine dans d'autres pays aient pour effet d'interdire les jeux autorisant les rapports sexuels virtuels avec des enfants virtuels. En Australie, selon les déclarations de Connor O'Brien, président de la section de droit pénal de l'Institut de droit de Victoria, dans *The Age* (journal de Melbourne), le développeur de Second Life

O assunto relacionado à pornografia infantil, distribuída e vendida na Internet aflige e preocupa autoridades de várias partes do mundo[86]. A Polícia Federal da Austrália estuda maneiras para combater a pedofilia nos mundos virtuais, porém, as investigações são altamente comprometidas. Policiais admitem a existência de grandes obstáculos para capturar os criminosos e, principalmente, para detectá-los, pois praticantes de tais atos são acobertados pelo anonimato e os criminosos podem agir 24 horas por dia.

Pode-se dizer que o *Second Life* é proibido para menores de idade. Surgem dois desafios iniciais: (i) para cada país existe uma lei específica que determina qual a idade para que o indivíduo alcance a maioridade penal, (ii) as

---

est passible de poursuites compte tenu de la diffusion d'images d'enfants dans un contexte sexuel".(...) Il est probable que toute cette publicité autour de la pédophilie virtuelle dans Second Life soit axée sur la mauvaise cible. Les jeux vidéo font l'objet de véritables contrôles judiciaires, non pas quand ils permettent aux individus de faire des choses qui, dans la vraie vie, seraient condamnables, mais quand on peut raisonnablement conclure qu'ils risquent d'accroître la criminalité dans le monde réel. A l'heure actuelle, les preuves en la matière sont plus fortes pour les jeux qui engendrent la violence que pour les réalités virtuelles qui autorisent la pédophilie. " Vices virtuels by Peter Singer - Disponível: < http://www.project-syndicate.org/commentary/singer26/French> Acesso agosto2007

[86] Magnitud de la pornografía infantil - Las investigaciones de la policía federal argentina afirman que más de 2 millones de personas se conectan a sitios de pornografía infantil – y en dos minutos, es posible acceder a 1.400 imágenes de pornografía infantil. • Protégeles, una ONG europea creada para rastrear y remover pornografía infantil del Internet, recibió 28.900 denuncias e identifico 1.800 comunidades en el mundo de abusadores de niños entre el 2001 y el 2004. • La Internet Watch Foundation (Fundacion para la Vigilancia de Internet) informó que en el 2003, recibió reportes sobre 13 newsgroups potencialmente ilegales, 24 newsgroups que regularmente hospedan imágenes de abuso infantil, así como 33 sitios de pago-para-ver (pay-per-view) y 66 sitios Web comunes que hospedaban semanalmente imágenes potencialmente ilegales de abuso infantil. • En el 2003, investigadores del Reino Unido reportaron que durante las seis semanas que monitorearon Internet, encontraron 140.000 imágenes de abuso infantil expuestas durante ese tiempo. • Un estudio del Servicio Aduanero de los Estados Unidos realizado en el 2001 encontró 100.000 sitios en Internet relacionados con la pornografía infantil. Ese mismo año, una compañía norteamericana productora de software de filtro, N2H2, reportó 231 sitios de pornografía infantil nuevos en línea cada mes – o cerca de ocho sitios por día – aunque algunos sitios desaparecieron durante los seis meses que duró el estudio. • Luego de un año revisando más de un millón de páginas Web por día, la compañía de tarjetas de crédito Visa informó haber identificado 400 sitios identificados como poseedores de pornografía infantil. El estudio formó parte de las acciones de la compañía para contrarrestar el uso de Visa en la venta de pornografía ilegal. • La policía inglesa dijo al diario The Guardian que en el 2003 el tamaño del tráfico de imágenes ilegales a través del peer2peer empequeñeció a casi todos los demás abusos a niños encontrados en la red. • En Lincolnshire, Reino Unido, un hombre fue encontrado con 450.000 imágenes pornográficas de niños. Otro hombre en Nueva York poseía un millón". Disponível:< http://nopornoinfantil.blogspot.com/2007/04/utilizacin-de-nios-y-nias-en-pornografa.html> Acesso abril 2007

informações solicitadas no site para efetuar o cadastro são falsificadas com facilidade pelas crianças que se vêm seduzidas a adentrarem nos metaversos.

O FBI esteve fiscalizando o *Second Life* sobre questões que envolviam jogos virtuais e seus agentes tiveram que criar avatares para que pudessem observar as transações ocorridas no metaverso[87]. Essa investigação resultou no fechamento de todos os cassinos, pois o governo americano proíbe jogos de azar on-line, e conforme informação da Revista Info, os diretores da *Linden Lab* e os donos dos cassinos virtuais poderão até ser presos se for comprovado algum tipo de crime. Esses são apenas alguns exemplos dos crimes e dos problemas enfrentados pelas autoridades policiais de diversas partes do mundo real.

O *Second Life* já foi intitulado como a *web* 2.0 tridimensional e, como exemplo da Internet que já é familiar, também está ocasionando conflitos jurídicos que suscitam soluções, muitas vezes imediatas, não podendo aguardar por novas leis que dificilmente irão acompanhar esses novos mundos virtuais.

2.3 - Das Provas produzidas em meio eletrônico

Antes de adentrarmos especificamente ao estudo das provas produzidas por meios eletrônicos, urge conceituarmos prova, consoante o ordenamento jurídico brasileiro. De acordo com o que leciona Fernando da Costa Tourinho Filho (2007, p. 215):

> Provar é, antes de mais nada, estabelecer a existência de verdade; e as provas são os meios pelos quais se procura estabelece-la. Entende-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio juiz, visando estabelecer, dentro do processo, a existência de certos fatos.

Em outras palavras, provar é fazer conhecer a outros uma verdade que já nós é conhecida. Humberto Theodoro Jr. apresenta dois sentidos que se pode conceituar prova no processo (2006, p. 381):

---

[87] Revista Exame Informática. FBI faz busca a cassinos do Second Life. Disponível< http://exameinformatica.clix.pt/noticias/internet/214975.htm.> Acesso Junho 2007

> 1. objetivo: isto é, como instrumento ou meio hábil, para demonstrar a existência de um fato (os documentos, testemunhas, perícias, etc);
> 2. subjetivo: que é a certeza (estado psíquico) originada quanto ao fato, em virtude da produção do instrumento probatório. Aparece a prova, assim, como convicção formada no espírito do julgador em torno do fato demonstrado.

Prova, portanto, é tudo aquilo que possa atestar garantir ou demonstrar a existência ou inexistência de alguma coisa. Dessa forma, no processo judicial, quando as partes querem demonstrar a veracidade de suas pretensões, deverão estas se utilizar de todos os meios de prova admissíveis em juízo. Pois bem, a questão de admissibilidade é um ponto de relevo no que tange a produção de provas.

A nossa Constituição Federal, de 1988, prevê em seu artigo 5.º, inciso LVI, que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos;".

Já o Código de Processo Civil prevê, expressamente, como meios de provas juridicamente admissíveis, conforme ensinamento de Humberto Theodoro Júnior[88], os seguintes:

> Os especificados pelo Estatuto Processual Civil foram os seguintes:
> I – Depoimento pessoal (arts. 342-347);
> II – Confissão (arts. 348-354);
> III – Exibição de documento ou coisa (arts. 355 e 363);
> IV – Prova documental (arts. 364-391);
> V – Prova testemunhal (arts. 400-419);
> VI – Prova pericial (arts. 420-439);
> VII – Inspeção judicial (arts. 440-443); [89]

Ainda o CPC, em seu art. 332, acerca do assunto prevê que:

> Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

O preceito supra citado é completado pelo artigo 335 do mesmo diploma legal que diz:

> Art.335: Em falta de normas jurídicas particulares, o juiz aplicará ass regras de experiência comum subministradas pela observação do que

---

88 *op. cit.*

89 *Ibidem*

> ordinariamente acontece e ainda as regras de experiência técnica, ressalvado, quanto a esta, o exame pericial.

No Processo Penal os tipos de prova encontram-se descritos nos artigos 158 a 250, dentre eles destacam-se: o exame do corpo de delito e perícias em geral, interrogatório do acusado, oitiva de testemunhas, documentos etc.

O rol de provas, segundo melhor juízo, não é taxativo, portanto, apesar da legislação processual civil e penal apontarem alguns meios de prova admissíveis no processo, qualquer outro meio poderá ser utilizado, desde que não atente contra a moralidade e não violente a dignidade humana, bem como que seja revestido de legalidade e não produzido por meios ilícitos. Daí porque também cabe uma breve diferenciação acerca das provas consideradas ilegais e ilegítimas. A prova ilícita é a obtida com infringência às normas de direito material, isto é, mediante a pratica de ilícito penal, civil ou administrativo. Ex. interceptação telefônica sem autorização judicial, confissão obtida mediante tortura. A prova ilegítima são as produzidas com infringência a dispositivos de natureza processual. Ex. no processo penal o documento exibido em plenário do júri em desacordo com o disposto no art. 475 do CPP. A inadmissibilidade nos termos do texto constitucional, no entanto, abarca tanto as prova ilícita quanto a ilegítima.

No processo penal há, ainda, o entendimento segundo o qual é admissível a utilização no processo de prova favorável ao acusado, ainda que colhida com infringência a direitos fundamentais seus ou de terceiros, numa alusão a aplicação do principio da proporcionalidade, sob a ótica do direito de defesa (GRINOVER, FERNANDES, GOMES FILHO, 2005).

Por fim, cumpre obtemperar que o direito à prova, constitucionalmente assegurado, está inserido nas garantias da ação, da ampla defesa e do contraditório, entretanto, não é absoluto, sofrendo algumas restrições, como as supra analisadas.

O Direito Processual tradicional reclama ser repensado, bem como o sistema jurídico do País, especialmente nas áreas de aplicação do Direito Processual, precisa adaptar-se às evoluções tecnológicas para que seja capaz,

efetivamente, de produzir justiça e manter a paz social. Daí porque se torna relevante a análise da admissão e validade das provas produzidas por meios eletrônicos.

Foram desenvolvidas técnicas forenses digitais a exemplo da ferramenta *Encase* que recupera dados dos discos duplicados e permite que o perito tenha alta produtividade na busca de indícios ou provas contidas na mídia suspeita. Atualmente, a *EnCase* já está sendo usada por polícias federais, civis e ministérios públicos brasileiros, como também por instituições financeiras e empresas de telecom. Tais ferramentas constituem elementos fundamentais no que tange a identificação de autoria e materialidade do delito, instando destacar que as evidências no meio eletrônico deixam provas complexas e conhecimento especializado para sua coleta.

Também a *Microsoft* Brasil e a Polícia Federal que se unem para lançar a versão local do CETS – *Child Exploitation Tracking System* ("KÉTS") ou Sistema de Rastreamento de Exploração Infantil, um projeto internacional cujo objetivo é o de combater a exploração *on-line* de crianças. A ferramenta rastreia sites suspeitos e permite intercâmbio de informações entre diferentes países além de permitir que a força policial brasileira se torne ainda mais efetiva em sua luta neste crime abominável e que não respeita fronteiras.

> Para combater a exploração sexual infantil pela Internet, a Polícia Federal, em parceria com a Microsoft Brasil, colocou em funcionamento um dos sistemas de informação mais modernos do mundo, o Child Exploitation Tracking System (CETS) ou Sistema de Rastreamento de Exploração Infantil na Internet. Hospedado na sede da Polícia Federal, em Brasília, o CETS tem, entre outras funcionalidades, um banco de dados estruturado pelos próprios investigadores, o que facilita as diligências.
> A idéia surgiu quando o policial Paul Gillespie de Toronto, no Canadá, enviou um e-mail a Bill Gates falando sobre a falta de recursos de tecnologia disponíveis para o combate à exploração infantil e pedindo ajuda para mudar esse quadro. A solicitação foi atendida e, em 2003, a Microsoft começou a trabalhar em conjunto com autoridades canadenses para projetar um software que permitisse que investigadores de todas as partes do mundo pudessem se comunicar em tempo real.
> Após o lançamento oficial em 2005, o CETS foi apresentado pela Polícia Real Montada do Canadá a corporações de vários países e a Polícia Federal do Brasil foi uma das primeiras a demonstrar interesse pelo

> sistema. Além do Brasil, Reino Unido, Itália, Espanha e Indonésia já adotaram o sistema.
> No Brasil – As etapas de planejamento e adaptação do programa à realidade brasileira começaram ainda em 2005. Durante a fase de implantação, o CETS passou por um processo de customização de suas ferramentas – cerca de 150 mil reais foram investidos pela Microsoft na tradução do sistema para a língua portuguesa e adaptação dos jargões e processos.
> O lançamento oficial do CETS ocorreu em novembro de 2006, durante a III Conferência Internacional de Perícias em Crimes Cibernéticos[90], em Brasília (DF). No evento, cerca de 200 policiais federais de todo o país fizeram o treinamento de manutenção e operação do sistema. Terminada a capacitação, voltaram para suas regiões com a tarefa de multiplicar esse conhecimento com seus colegas. A idéia é que, em pouco tempo, essa solução migre para outros estados e reúna toda a Polícia Federal. Em seguida, alcance também as polícias civil e militar, o Ministério Público e o Poder Judiciário[91].

Vale ressaltar que quase todo crime cometido, no qual há um computador relacionado, se as provas digitais não forem coletadas adequadamente, sem as ferramentas técnicas apropriadas, podem ser invalidadas em possível litígio judicial. As a prova digital[92] é extremamente frágil, de forma que, se não tratada dentro de padrões técnicos específica que não deixe rastros para dúvidas, ela pode perfeitamente ser contestada pelo acusado e anulada.

Diante desses inúmeros delitos decorrentes das mudanças provocadas pela tecnologia, 34 países que integram o Conselho da Europa, mais quatro Estados não membros (Canadá, Japão, África do Sul e EUA), celebraram a Convenção sobre o Cibercrime, em Budapeste, em 23 de novembro de 2001, com a intenção de coibir tais delitos.

A tecnologia, no entanto, no que tange a sua utilização no processo penal, ainda encontra algumas dificuldades, muito embora a Internet, devido ao

---

90 Este pesquisador esteve presente no evento de lançamento do CETS como Congressista.

91 Investigação virtual Disponível: <http://www.microsoft.com/unlimitedpotential/pt-br/InformationCenter/casos/ambiente_online_seguro_criancas_cets.mspx>. Acesso maio 2008

92 Rastros de Uso - Como meio de prova destaca-se o uso de rastros de uso: Os rastros são as suas impressões digitais em seu sistema. Sempre que você visita uma página com o seu navegador ou simplesmente abre qualquer arquivo, aquela informação é armazenada pelo Windows. Na maioria dos casos, isso é muito útil – se você quiser abrir o mesmo arquivo novamente, você pode selecioná-lo de uma lista ao invés de digitar o nome do arquivo inteiro ou procurá-lo pelas pastas novamente. Mas em alguns casos você pode querer ocultar sua atividade, porque alguns spywares podem utilizar essas informações. O Spybot-Search&Destroy pode remover alguns dos mais importantes e mais comuns rastros do seu sistema. Disponível: <http://www.spybot.info> Acesso 31 maio 2008.

seu amplo sistema de comunicação em tempo real, possa facilitar a produção de provas. Como exemplo da utilização do sistema tecnológico no processo penal, que ainda encontra certa resistência doutrinária em sua implantação, pode ser citada a Webconferência, o teleinterrogatório; o teledepoimento;o telerreconhecimento; a telessustentação; o telecomparecimento; a telessessão; a telejustificação. A teleaudiência tem sido utilizada em larga escala em diversos países do mundo, bem como por Tribunais internacionais, dentre eles o Tribunal Penal Internacional.

Vale ressaltar a utilização, pelo Ministério Público Estadual, de tecnologia multimídia, isto é, de um *software* que permite incluir trechos de diálogos relevantes, oriundos de interceptações telefônicas, sem que haja a necessidade da realização de transcrições pelos peritos, bem como imagens, nas peças de denúncia que são enviadas ao juiz. Referida tecnologia foi utilizada em interceptações feitas ao longo de investigações sobre os ataques do PCC. A utilização de tecnologia multimídia agiliza o processo e soluciona, ao menos parcialmente, o problema apresentado, por exemplo, pelo perito Ricardo Molina, qual seja, de falta de equipamentos e preparo dos profissionais (MANSO e GODOY, 2007)[93]. Além disso, o Núcleo de Identificação Criminal, que faz o trabalho de perícia, atestando que o material não sofreu cortes ou falsificações, bem como identificando as vozes gravadas, tem trabalho acumulado para mais de quatro anos, o que ocasiona o descumprimento dos prazos legais dos processos (THOME, 2007).

O Direito Processual, *lato sensu*, tem tentado acompanhar, embora de maneira ainda insuficiente, os avanços tecnológicos que caracterizam a denominada Sociedade da Informação, "tendo por finalidade o aproveitamento deste sistema de comunicação como mais um instrumento de apoio para a

[93] Referido perito cita como exemplo da falta de preparo de alguns profissionais a inutilização da fita, no crime que vitimou o prefeito de Santo André, Celso Daniel, pelos investigadores do caso, obtida através do circuito interno de TV do restaurante em que o prefeito jantou pouco antes de ser seqüestrado e que constituía item fundamental para a investigação. Devido ao manuseio incorreto do material este restou danificado e perdeu sua utilidade.

realização de atos forenses." .(BARROS, 2007, p. 282). Na mesma lógica, analisa os aspectos para obtenção de provas ensina:

> Para facilitar o descobrimento da verdade na apuração de delitos praticados por meio da rede, o Senado Federal tenciona incluir, nos projetos de lei que visam regulamentar a matéria(...).
> (...) uma norma de exigência para os provedores nacionais de internet, para que mantenham, pelo prazo mínimo de três anos, os dados de conexões e comunicações relativos à identificação do endereço IP (protocolo de Internet), data, horário de início e término da conexão e as troca de *e-mail*, informações estas que serão mantidas em sigilo, cujo acesso somente se dará por ordem judicial. (BARROS, idem)

Com efeito, o Manual prático de investigação, publicado pelo Ministério Público Federal e Comitê Gestor da Internet no Brasil fazem as seguintes considerações:

> De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características:
>
> a) possuem formato complexo (arquivos, fotos, dados digitalizados etc);
> b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;
> c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.[94]
>
> (...) uma das mais importantes evidências que podemos coletar é o chamado número IP (Internet Protocol). O número IP é uma identificação que todos os computadores que acessam a internet possuem; ele aparece no formato A.B.C.D, onde A, B,C e D são números que variam de 0 a 255 (por exemplo, 200.158.4.65). O IP deve estar acompanhado da data, hora exata da conexão ou comunicação e o fuso horário do sistema.[95]
>
> (...) nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC.Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.

---

[94] Manual Prático de Investigação de Crimes Cibernéticos. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

[95] Idem

2.3.1 - Local e Competência

Em relação ao local do crime o Brasil adotou a teoria da ubiqüidade de acordo com o que prescreve o artigo 6º do Código Penal, ou seja, o local é onde ocorreu ação ou omissão bem como onde se produziu ou deveria produzir o resultado.

No que tange a competência, ela não é fácil de ser determinada uma vez que a Internet rompe fronteiras. Pelo seu caráter transnacional, pode ser que o autor esteja em um país e a vítima em outro. Ou mesmo o fato criminoso pode ocorrer em um local e se consumou em outro completamente diferente e daí surge à dúvida, de quem é a competência para julgar tais delitos?

Viável é a solução obtida pelo Ministério Público Federal, no Manual prático de Investigação[96] e que transcrevemos:

> Nos termos do artigo 109, inciso IV, da Constituição brasileira, compete aos juízes federais processar e julgar os crimes cometidos em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Assim, é competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso(...)
> Quanto a hipótese prevista no inciso V do artigo 109 da Constituição, ou seja, os crimes previstos em tratado ou convenção internacional, quando iniciada a execução no país o resultado tenha ou devesse ter ocorrido no estrangeiro, vale lembrar que as condutas tipificadas no artigo 241 do Estatuto da Criança e do Adolescente e também o crime de racismo (tipificado na Lei 7.716/89) têm previsão em convenções internacionais de direitos humanos. Como a consumação delitiva normalmente ultrapassa as fronteiras nacionais quando os dois crimes são praticados através da internet, a competência para julga-los pertence à Justiça Federal.
> A competência da Justiça Federal para processar e julgar a divulgação na Internet de material pornográfico envolvendo crianças e adolescentes já foi reconhecida por quatro Tribunais Regionais Federais (1ª, 3ª, 4ª e 5ª Regiões) brasileiros.
> Outros delitos não abrangidos pelas hipóteses acima mencionadas – por exemplo, os crimes contra honra de particular, praticados através da rede – deverão ser investigados e processados no âmbito das Justiças Estaduais, já que o simples fato do crime ter sido cometido por meio da internet não é suficiente para justificar a competência da Justiça Federal.

---

96 Idem

A competência de acordo com o disposto no artigo 70 do Código de Processo Penal será onde se consumou a infração adotando a teoria do resultado; o § 1º do artigo mencionado diz caso a execução se inicie no território nacional e a infração se consumar fora dele a competência será o lugar onde tiver sido praticado o último ato de execução no Brasil; e o § 2º será competente onde mesmo que parcialmente tenha produzido ou deveria produzir o resultado.

2.3.2 - Informatização do Processo Judicial

Entrou em vigor a lei 11.419/2006 que trata da Informatização do Processo Judicial, alterando a lei 5.869/73 no que diz respeito principalmente a atos judiciais, tais como, envio de petições, de recursos e a prática de outros atos processuais, fazendo com que a publicação eletrônica substitua qualquer outro meio de publicação oficial excetuando os casos específicos exigidos em lei. Dessa forma o Judiciário dará um valioso passo em direção à redução da burocracia imprimindo maior agilidade aos processos e será favorável para todos. Ganham com a informatização do poder Judiciário a sociedade, assim como as partes envolvidas no litígio. O processo virtual está sendo implantado em todos os órgãos do Poder Judiciário Brasileiro. O disposto nessa lei aplica-se aos processos civil, penal e trabalhista de acordo com o artigo 1º, § 1º da lei 11.419/2006[97], bem como aos juizados especiais, em qualquer grau de jurisdição.

O sistema já inaugurado garante a segurança na transmissão eletrônica dos dados, bem como das peças processuais e serão desenvolvidos pelos órgãos do Poder Judiciário que deverão utilizar preferencialmente código aberto[98], acessíveis por meio da rede mundial de computadores.

---

[97] (...) Aplica-se o disposto nesta Lei, indistintamente, aos processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição. Lei 11.419/2006.

[98] O termo código aberto, ou *open source* em inglês foi cunhado pela *OSI (Open Source Initiative)* e se refere ao mesmo software também chamado de software livre, ou seja, aquele que respeita as quatro liberdades definidas pela Free Software Foundation. Qualquer licença de software livre é também uma licença de código aberto, a diferença entre os dois está no discurso. Enquanto a FSF usa o termo "Software Livre" para trazer um discurso baseado em

Um dos primeiros problemas, é que a atividade jurisdicional não pode ser exercida por um computador. Não podemos vir a ter despachos ou mesmo decisões de mero expediente produzidas por computadores, ainda que o judiciário precise com urgência agilizar os processos em trâmite e também combater o excesso de trabalho dos Magistrados e Serventuários da Justiça. Nas palavras de Almeida Filho (2007, p. 2) “não podemos permitir que este processo eletrônico encontre modificações a ponto de termos sentenças cartesianas emitidas por um computador”.

Existem sentenças emitidas por um computador na área Tributária. O Projeto da Nota Fiscal Eletrônica regido por convênios, portarias e protocolos permite que a Administração Fazendária venha a cercear a emissão de Nota Fiscal Eletrônica toda vez que o sistema verificar a existência de problemas fiscais do comprador ou vendedor. As informações são meramente alimentadas e nunca é a máquina a rigor que julga. Nosso pensamento é processado desta forma. Quando falamos em automação é que sempre colocamos nosso pensamento em um *input* imediato. O programador carrega. Primeiro o normal. Tudo isso vai se discutir depois. O Cartório vai certificar o prazo. Quando falamos em julgamento e aquilo que é mero processamento que é feito anteriormente. Na implantação do processo eletrônico o restante é mero processamento. Tudo feito no sistemaque é medido pelo juiz. Às vezes a própria revelia tem realmente especificidade. A Revelia em função de todas elas de 100 teremos esta especificidade. Na Argentina já se estuda a possibilidade de sentença totalmente eletrônica. Aplica-se um formulário. Nos casos de aplicação da sentença na esfera pela o Juiz aplica uma forma de questionário para determinar a pena. A sentença é uma coisa julgamento é outra. Muitos advogados mencionam que ficaria muito objetiva a decisão.

---

questões éticas, direitos e liberdade, a OSI usa o termo "Código Aberto" para discursar sobre um ponto de vista puramente técnico, sem conflitar questões éticas. Esta nomenclatura e discurso foram forjados por Eric Raymond e outros fundadores da OSI para apresentar o software livre a empresas de uma forma mais agradável a visão das corporações. Disponível: <http://pt.wikipedia.org/wiki/Open_source> Acesso maio 2008

O julgamento da ação se inicia pelo crivo do advogado. O advogado deve admitir que a ação seja possível e tangível. O Juiz na verdade processa todas as informações e profere um juízo de valor. Anteriormente muitos juízes indeferiam petições que eram feitas pelo computador.

A discussão que se trata de processo ou procedimento é de grande relevância para termos uma uniformidade de atos processuais em todo o Brasil. Neste sentido a "discussão se se, trata de processo ou procedimento não é mero capricho processualístico, mas o temor de termos legislações estaduais por força de competência concorrente" (ALMEIDA FILHO, 2007, p. 2). Sob este aspecto é relevante a experiência dos Estados em relação à implantação da Nota Fiscal Eletrônica.

Em função do aumento da Sonegação Fiscal, a Secretaria da Receita Federal, juntamente com os Estados, começou a estudar a implementação de um sistema que pudesse controlar as obrigações tributárias dos contribuintes em tempo real. Este projeto foi copiado do Chile que introduziu em 2003 com amplitude o projeto da Nota Fiscal Eletrônica. Neste sentido, vê-se que o Legislador e os processualistas que pretendem se debruçar sobre o Processo Eletrônico têm muito a analisar ao estudar a evolução do processo tributário eletrônico no Brasil. Uma vez que este é mais avançado, sendo estudada sua implementação desde 1993 no Brasil. Analise econômica do direito é relevante apenas em alguns casos. Em alguns pontos podemos fazer esta análise econômica como nos casos do interrogatório por videoconferência.

2.3.3 - Da Comunicação Eletrônica dos Atos Processuais e do Processo Eletrônico

O Sistema de processo eletrônico foi desenvolvido pelo Conselho Nacional de Justiça (CNJ), em *software* livre e será repassado gratuitamente a Tribunais de todo pais, favorecendo dessa maneira todos os envolvidos no processo judicial. É imprescindível para o sucesso desse sistema que os

profissionais que irão manuseá-lo sejam treinados, além de fazer sempre *backup* dos arquivos, pois se houver alguma indisponibilidade de documentos o que foi criado para a celeridade se transformará em uma morosidade maior e até mesmo na paralisação de alguma operação.

Existe um Projeto de Lei nº 3030/2008 apresentado pelo deputado Carlos Bezerra ao Congresso Nacional e caso o mesmo venha a ser transformado em lei, a prática de atos processuais por meio eletrônico restará limitado aos portadores de certificado digitais, e o que vem a ser certificado digital?

Para ser obter uma assinatura digital é necessário procurar uma Autoridade Certificadora, tais como a ICP-Brasil (Infra-Estrutura de Chaves Públicas) e essa têm a função de verificar a identidade do usuário e lhe fornecer uma chave. Essas informações são introduzidas em um registro conhecido como certificado digital[99].

O processo judicial digital inicia um significativo avanço da tecnologia nas ações da Justiça, é um momento histórico da segurança da informação que traz os princípios básicos da informação que são a confidencialidade, integridade e disponibilidade, associados à legalidade e autenticidade, e o artigo 2º parágrafo 2º da citada Lei trata de alguns dos requisitos citados:

> Art. 2º(...).
> Parágrafo 2º: "Ao credenciamento será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações".

Para que os advogados e outros profissionais do Direito tenham acesso ao sistema eletrônico é necessário o cadastramento no Poder Judiciário que requer o compromisso de acessar periodicamente o sítio do Tribunal. A este é

---

[99] O certificado digital do Poder Judiciário Brasileiro - CertJUS é o certificado digital emitido pela AC Certisign JUS (A AC CertiSign JUS, criada em 19 de maio de 2006, com validade até 2011, é a primeira Autoridade Certificadora a comercializar no varejo as cinco opções de certificados da AC-JUS: CertJUS Cidadão, CertJUS Advogado, CertJUS Institucional, CertJUS Empresarial e o CertJUS Equipamento Servidor.), em conformidade com a ICP-Brasil, indicado para servidores públicos, advogados, pessoas físicas e jurídicas e entidades governamentais. O certificado digital CertJUS proporciona ao seu titular toda a segurança da tecnologia de Certificação Digital Disponível:< http://www.certisign.com.br/produtos/certJUS> Acesso maio 2008.

atribuído registro e o meio de acesso ao sistema, resguardando o sigilo, a identificação e autenticidade das comunicações, de acordo com o artigo 2º e parágrafo 1º da Lei que disciplina:

> Art. 2º: O envio de petições, e recursos e a prática de atos processuais em geral por meio eletrônico serão admitido mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.
> Parágrafo 1º: "O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado".

Foi criado o Diário da Justiça Eletrônico que disponibiliza a informação dos atos do Poder Judiciário e possui uma seqüência de vantagens em relação ao modo tradicional, em relação aos desempenhos da tecnologia da informação.

A comunicação feita através do Diário da Justiça eletrônico substitui qualquer outro órgão de publicação de intimações, salvo as pessoas relacionadas no artigo 222 do Código de Processo Civil. O processo eletrônico trará mudanças de comportamento com o trabalho 12 horas por dia.

Há um conflito na redação do artigo 3º, parágrafo único do diploma legal, e conforme com o que ensina o Professor José Carlos de Araújo Almeida Filho (2007, p. 214-215):

> O maior problema na redação do art. 3º diz respeito ao seu parágrafo único, que contém contornos de inconstitucionalidade.
> Nos termos do art. 172 do CPC, "o atos processuais realizar-se-ão em dias úteis, das 6 (seis) às 20 (vinte) horas". Com a redação conferida pelo parágrafo único do art. 3º, no Processo Eletrônico os prazos serão praticados até as 24 horas do seu último dia.
> O Prof. Dr. Humberto Theodoro Júnior traz uma importante observação quanto ao prazo estatuído no art. 172 do CPC, advertindo que "o horário útil para protocolar petições não é o genérico do *caput* do art. 172, onde se prevê a eventualidade de atos processuais até as 20 horas. Quando o recurso ou outro ato depender de protocolo, o que fixa o momento final de sua possibilidade é o término do expediente assinalado pela lei de organização judiciária".
> Pela redação do parágrafo único se vê que não estamos diante de eventualidade, mas de verdadeira prática do ato processual até o último segundo do dia de seu vencimento:
> "Parágrafo único. Quando a petição eletrônica for enviada pra atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia".

> Neste sentido, quem se utiliza do Processo Eletrônico possui uma diferenciação, ferindo princípios de igualdade e isonomia,e, em assim sendo, violando-se de forma literal o art. 5º, *caput*, da Constituição.

Segue a regra que dispõe que os prazos processuais terão início no primeiro dia útil a ser considerado como data da publicação[100]. Ou seja, de certo modo houve uma dilatação do prazo já que esse será considerado no primeiro dia útil que na verdade será entendido como segundo dia útil conforme o artigo 4º, parágrafo 3º que diz que a data da publicação será o primeiro dia útil seguinte ao da disponibilização da informação no Diário da Justiça[101].

Contudo o Dr. Eduardo Francisco Marcondes[102], advertiu que nem tudo será fácil de se resolver com a intimação via Diário da Justiça Eletrônico. Argumenta que as dificuldades começarão a aparecer nos casos em que a página do Diário Oficial Eletrônico for clonada, se a intimação não foi publicada, se houve falha no sistema elétrico. Indagações começam a surgir tais como, em caso de queda do o sistema será prorrogado para o dia seguinte, o prazo. Mas quanto tempo o sistema deverá ficar fora do ar para que o prazo seja devolvido. O prazo será devolvido integralmente, ou parcialmente? Como é feita a prova em relação à queda do sistema? Quanto tempo o sistema esteve inoperante? (O professor entende se ficar 2 minutos o sistema parado é suficiente para que seja devolvido o prazo). Ficou indisponível prejudicou alguém basta à palavra. O Tribunal deve provar que o sistema não ficou fora o ar. Por quanto tempo precisa ficar fora para considerar que o prazo será prorrogado? Pelo principio da razoabilidade, se o sistema cair na parte da manhã durante 15 minutos, ou se o sistema caiu às 23:00 horas do dia do prazo, cada caso terá que ser analisado separadamente. A tecnologia irá trazer temas novos a serem discutidos.

---

[100] Artigo 4º: "Os tribunais poderão criar *Diário da Justiça* eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como a comunicação em geral".

[101] Artigo 4º (...).

[102] O Magistrado na qualidade de Juiz Assessor do Presidente do Tribunal de Justiça de São Paulo – TJ/SP profereiu palestra no II Ciclo de Palestras do Contecioso Administrativo Tributário. O evento foi realizado na data de 31 de outubro de 2007, no Aditório da AFRESP Associação dos Agentes Fiscais de Rendas do Estado de São Paulo Avenida Brigadeiro Luís Antônio, 4843.

Atualmente a jurisprudência pacífica do STJ é no sentido de não considerar justa causa para relevar o prazo a publicação nos sítios dos Tribunais (ALMEIDA FILHO, 2007, p. 228-230):

> PROCESSO CIVIL. EMBARGOS DE DIVERGÊNCIA. REABERTURA DE PRAZO. INFORMAÇÕES PRESTADAS VIA INTERNET. NATUREZA MERAMENTE INFORMATIVA. AUSÊNCIA DE JUSTA CAUSA. ART. 183, §1º, DO CPC.
> As informações prestadas via *Internet* têm natureza meramente informativa, não possuindo, portanto, caráter oficial. Assim, eventual erro ocorrido na divulgação destas informações não configura justa causa para efeito de reabertura de prazo nos moldes do art. 183 §1º, do CPC.
> Embargos de divergência rejeitados.
> (EREsp 503.761/DF, Rel. Ministro FELIX FISCHER, CORTE ESPECIAL, julgado em 21.09.2005, DJ 14.11.2005 p. 175)
>
> PROCESSO CIVIL – AGRAVO DE INSTRUMENTO – NEGATIVA DE PROVIEMENTO – AGRAVO REGIMENTAL DESPROVIDO – INTIMAÇÃO – DIÁRIO DE JUSTIÇA – DEVOLUÇÃO DE PRAZO – NÃO CABIMENTO.
> 1 – A intimação das decisões do poder Judiciário, quando feita pela imprensa, o é pela publicação no Diário de Justiça, conforme preceitua o art. 236 do Código de Processo Civil.
> 2 – Não se constitui fundada razão para devolução de prazo o argumento da agravante d que aguardava o andamento do processo na *Internet* para interposição do recurso.
> 3 – Agravo regimental desprovido.
> (AgRg no AgRg no Ag. 655.774/RJ, Rel. Ministro JORGE SCARTEZZINI, QUARTA TUMA, julgado em 04.08.2005, DJ 05.09.2005 p.422.)
>
> PROCESSO CIVIL. EMBARGOS À EXECUÇÃO. ACOMPANHAMENTO PROCESSUAL VIA INERNET. INFORMAÇÕES EQUIVOCADAS. RECONHECIMENTO DE JUSTA CAUSA. RESTITUIÇÃO DO PRAZO.
> 1. Acórdão que negou provimento à apelação sob o fundamento de que o prazo para o oferecimento dos embargos à execução inicia-se da juntada aos autos do mandado de citação cumprido, e não da data da informação obtida pelo Sistema Informatizado de Consulta Processual, cujo objetivo reside tão-somente em facilitar o acompanhamento de processos, via *Internet*, não tendo qualquer respaldo na legislação processual. Recurso especial que suscita dissídio jurisprudencial entre o aresto recorrido e o julgado desta Corte, que entendeu que informações errôneas prestadas pelo Tribunal via *Internet* configuram justa causa, devendo o juiz assinar novo prazo para a prática do ato.
> 2. As informações processuais prestadas por sítios eletrônicos da Justiça, ainda que dotadas de credibilidade, não são dotadas de caráter oficial, amparados em Lei 3. Nos casos específicos de citação realizada por oficial de justiça, no bojo do processo de execução, cumpre à parte executada o dever de acompanhar o andamento do feito pelos diversos meios disponíveis, visto que com a citação já se encontram presentes os subsídios suficientes ao oferecimento da defesa. O fato de constar no sistema de informações data diversa daquela em que efetivamente ocorreu a juntada do mandado cumprido não exime a parte de zelar pela

> observância do prazo para a oposição de embargos do devedor. Assim, não há que se falar em prejuízo que justifique a restituição do prazo.
> 3. Recurso especial não-provido.
> (REsp. 756.581/BA, Rel. Ministro JOSÉ DELGADO, PRIMEIRA TURMA, julgado em 16.08.2005 p. 255).[103]

Não podemos admitir que a jurisprudência continue neste caminho, admitindo que as informações são meramente informativas. Quando tratamos do *senso* e *contra-senso* da informatização judicial no Brasil, observamos que avançamos de um lado e temos um verdadeiro anacronismo de outro (ALMEIDA FILHO, 2007, p. 230).

Imagine um fórum totalmente informatizado, por onde não circulam folhas de papel. Pois existe este fórum, o primeiro do Brasil. Este foi inaugurado na terça-feira, 26 de junho pelo governador José Serra e pelo presidente do Tribunal de Justiça de São Paulo, desembargador Celso Luiz Limongi. A solenidade ocorreu às 11h30, na própria sede do novo espaço, trata-se do Foro Regional XII[104] **-** Nossa Senhora do Ó, região Oeste da Capital.

Se houver a necessidade de enviar o processo digital para um local que não houver a disponibilidade de recebimento digital, a pessoa deverá transformar esse processo digital em processo físico e a sua tramitação deverá ser totalmente física.

Os atos processuais serão comunicados diretamente a área restrita dos interessados através da assinatura digital, já que este é o detentor da mesma e será considerada realizada a intimação no dia em que o intimado efetivar a consulta e caso seja em dia não útil será considerada o primeiro dia útil seguinte**[105]**.

> Art. 5º: As intimações serão feitas por meio eletrônico em portal próprio aos que cadastrarem na forma do art. 2º desta Lei, dispensando-se a publicação no órgão oficial, inclusive eletrônico.
> Parágrafo 4º: Em caráter informativo, poderá ser efetivada remessa de correspondência eletrônica, comunicando o envio de intimação e

---

103 Idem

104 Disponível: <http://www.saopaulo.sp.gov.br/sis/lenoticia.php?id=85469&c=6> Acesso 1 abril 2008.

105 Artigo 5º Parágrafo 2º: " Na hipótese do §1º deste artigo, nos casos em que a consulta se dê em dia não útil, a intimação será considerada como realizada no primeiro dia útil seguinte.

> abertura automática do prazo processual nos termos do §3º deste artigo, aos que manifestarem interesse por esse serviço.[106]

A Lei 11.419/2006 em seu artigo 9º acrescentou ao artigo 237 do Código de Processo Civil o parágrafo único, O mesmo trata das citações, intimações e notificações através do meio eletrônico que será realizado com mais eficiência e em menor tempo se utilizado corretamente (ALMEIDA FILHO, 2007, p. 265).

> Entendemos ser de bom alvitre eu as citações sejam realizadas pelos meios ordinários. Não somente em termos de problemas técnicos, mas em virtude de possibilidade de interceptação de dados de telemática – o que configura crime, nos termos da Lei 9296/96, em seu art. 10.

O artigo 8º reforçou o chamado "processo virtual". É, pois facultado aos Tribunais desenvolver seus próprios sistemas eletrônicos de processamento de ações judiciais, de forma parcial ou integralmente digital utilizando preferencialmente a Internet ou Intranet[107], porém todos os atos processuais serão assinados eletronicamente na forma da Lei. O e-mail é de caráter meramente informativo. Do acesso do advogado ao sistema decorre a sua intimação. A lei não obriga ninguém a acessar o sistema. Para aqueles que

---

106 Com a Informatização, a tendência é o aumento de fraudes. As fraudes através de e-mail são uma prática comum. Desde um simples "telegrama on-line a uma mensagem de envio de voz ou de algum comentário que diga respeito à pessoa, é uma prática corriqueira na Internet. Com o advento da Lei 11.419/2006, contudo, as fraudes por e-mail tendem a ampliar: intimações, citações etc. Nosso BLOG já havia informado este tipo de fraude, mas é sempre bom mantermos o leitor atento a novas possibilidades. Recentemente recebemos uma "intimação" do Ministério Público Federal, mas de tão primário, sequer se pode levar em consideração.
O autor do e-mail usa um e-mail genérico. O e-mail que está circulando é o que se apresenta abaixo (e não cliquem em nada):
"Procuradoria Regional da Justiça Coordenação de Defesa dos Interesses Difusos e Coletivos – CODIN Procedimento investigatório n.º 354/2008.
O Ministério Público da Justiça, no desempenho de suas atribuições institucionais, com fundamento nos artigos 127 e 129, inciso VI da Constituição Federal e artigo 8º, inciso VII, da Lei Complementar n.º 75, de 20 de maio de 1993, INTIMA Vossa Senhoria a comparecer na Procuradoria Regional do Trabalho, no dia 19 de maio de 2008, às 10:30 horas, a fim de participar de audiência administrativa, relativa ao procedimento investigatório em epígrafe, em tramitação nesta Regional, conforme despacho em anexo abaixo. Anexo Despacho.doc
http://doiop.com/flogao.com.br/polyanaromano
SAF Sul Quadra 4 Conjunto C - Brasília / DF - CEP 70050-900 - PABX: (61) 3031-5100″
**O cabeçalho do e-mail demonstra a ingenuidade…Disponível: <http://blog.processoeletronico.com.br/2008/04/13/com-a-informatizacao-a-tendencia-e-o-aumento-de-fraudes/ > Acesso 30 maio 2008

107 Resumidamente, o conceito de intranet pode ser interpretado como uma versão privada da Internet, ou uma mini-Internet confinada a uma organização.

aderirem ao sistema receberão uma comunicação de inteiro teor do Tribunal. Se a parte acessa o sistema já se da por intimada. Caso contrário a intimação ocorre 10 dias após o recebimento deste comunicado e a partir daí começa a correr o prazo.

No que se refere ao Direito Processual Penal e Infracional, está afastada a citação eletrônica de acordo com o artigo 6º:

> Artigo 6º: Observadas as formas e as cautelas do art. 5º desta Lei, as citações, inclusive da Fazenda Pública, excetuadas as dos Direitos Processuais Criminal e Infracional, poderão ser feitas por meio eletrônico, desde que a íntegra dos autos seja acessível ao citando.

Ainda sobre o artigo 6º, vale observar que a intimação eletrônica pode ser feita também para a Fazenda Pública que valerá como se fosse intimação pessoal para os efeitos legais.

Em relação às cartas precatórias, rogatórias e de ordem de todos os Poderes serão feitas preferencialmente por meio eletrônico o que gerará maior celeridade no cumprimento das mesmas.

Para se conferir validade jurídica a um documento eletrônico é necessário a Assinatura Digital[108] e o próprio texto da lei disciplina no seu artigo 8º parágrafo único a seguir:

> Art. 8º (...)
> Parágrafo único: "Todos os atos processuais do processo eletrônico serão assinados eletronicamente na forma estabelecida nesta Lei".

No que determina sobre distribuição da petição inicial, a juntada da contestação, bem como os recursos, se darão de forma automática sem intervenção do cartório ou secretaria e se adaptada no formato digital será fornecido recibo eletrônico de protocolo. O uso da petição eletrônica sem a certificação digital não garante a integridade, a veracidade dos dados transmitidos, o que possibilitará interceptação, modificação do conteúdo e outros

[108] A assinatura digital se faz por meio dos conceitos de chave pública e privada que ocorre da seguinte maneira: é necessário que o destinatário tenha um documento eletrônico e uma chave pública do usuário, então será "criptografado" o documento e o receptor usarão a chave privada adequada para "descriptografar" o mesmo.

delitos. A garantia dessas informações só será possível se adotada conjuntamente com a assinatura digital, a criptografia, preservando as partes e garantindo seu acesso ao Judiciário.

Os atos que tiverem prazo determinado serão considerados tempestivamente os efetivados até 24 (vinte e quatro) horas do último dia, caso o sistema do Poder Judiciário se torne indisponível, será prorrogado para o primeiro dia útil à resolução do problema e/ou falhas técnicas. Os Tribunais deverão investir em segurança, pois como é sabido o Brasil é o país com o maior número de *crackers* especialistas no mundo.

Referente à validade jurídica dos documentos eletrônicos, não são somente os produzidos eletronicamente, bem como os extratos digitais e esses documentos digitalizados pelas partes terão a mesma força probante dos originais devendo o detentor dos documentos preserva-los até o trânsito em julgado da sentença, afinal de contas problemas podem ocorrer e preservar os originais é o melhor para posterior reenvio. Vale destacar o significado de documentos eletrônicos:

> Segundo o Decreto italiano nº 513/97, documento eletrônico é a "representação eletrônica (ou digital) de atos, fatos ou dados juridicamente relevantes" . Na mesma direção, a Portaria do Ministério da Fazenda nº 528/96, de 02 de setembro de 1996, publicada no D.O.U em 10/10/96, que regulamentou o Sistema Setorial de Gestão de Documentação e Informações – SGDI, do Ministério da Fazenda, dispõe que "compreende-se por documento, qualquer que seja o suporte utilizado, o conjunto de informações que registre o conhecimento humano, de forma que possa ser utilizado como elemento de consulta, estudo e prova". Na mesma linha o ordenamento jurídico brasileiro prevê atribuição de maior força probante aos documentos eletrônicos em razão da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 que institui a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), viabilizando a utilização de ferramentas derivadas da certificação digital.

Em relação à regulamentação desta Lei em comento, fica a encargo dos órgãos do Poder Judiciário no âmbito de suas respectivas atribuições.

2.3.4 - Videoconferência

A videoconferência permite total interação entre o magistrado e o interrogado e os demais sujeitos processuais, com tecnologia audiovisual.

O Plenário do Congresso Nacional aprovou o Projeto de Lei 7227/06 do Senado que torna regra geral o uso da videoconferência nos interrogatórios e nas audiências judiciais das quais participe o juiz, o acusado preso e seu defensor.

Com a adoção da videoconferência haverá uma economia processual e um maior número de policiais estará à disposição da sociedade para protegê-las, além da redução do custo do translado do preso. Caso não seja possível realizar a videoconferência, a proposta mantém a autorização para realizar a audiência ou interrogatório no presídio, desde que seja garantida a segurança do juiz e dos funcionários da Justiça como determina o Código de Processo Penal. Além dos réus, as testemunhas presas também poderão ser ouvidas por videoconferência. No futuro poderá ser utilizada a videoconferência para o cumprimento de cartas precatórias. O ideal que em todos os casos é que seja possibilitada a presença física do Juiz.

A Ministra Ellen Gracie entendeu que interrogar um réu por videoconferência não ofende suas garantias constitucionais de acordo com o Habeas Corpus 76.046. (ver anexo III)

2.3.5 - Responsabilidade dos Provedores

Para os provedores de acesso suas ações na maioria dos casos estão relacionadas à teoria da culpa o que será necessário demonstrar a existência de imprudência, negligência ou imperícia para a responsabilização. Quanto à divulgação do conteúdo se a informação apenas trafegar pelo provedor não há nenhuma responsabilização, mas se o provedor editar o conteúdo aí sim ele terá responsabilidade solidária.

A legislação sobre a responsabilidade dos provedores é deficiente, não há no ordenamento uma lei para preservação dos registros de provedores de acesso, conforme expõe o Manual de prático de investigação[109]:

> Os provedores de acesso mantêm arquivos com o registro (log) de todas as solicitações que recebem. Esses registros contêm informações essenciais, como a procedência do usuário, a freqüência com que retorna ao site e seus hábitos de navegação.
> Ocorre que: a) nem todos os provedores de acesso possuem arquivos de *logs*; b) aqueles que os mantêm, o fazem por períodos muitos curtos (poucos meses); c) não há controle acerca das informações declaradas pelo usuário (nome verdadeiro, número do CPF, endereço). É comum o criminoso fornecer informações falsas em seus registros eletrônicos.
> O Comitê Gestor de Internet no Brasil recomendou às companhias telefônicas e de cabo que reservem, para o serviço de provimento de acesso, centrais que permitam a identificação inequívoca da origem da chamada, de modo que os provedores de acesso (UOL, MPF, Terra, Globo, IG) à Internet possam identificar sua origem. Esta regulamentação está sendo aplicada somente em relação às operadoras de telefonia (Telefônica, TELEMAR etc.), mas não aos provedores de acesso. À Falta de uma legislação específica para os provedores, o Ministério Público tem celebrado "termos de compromisso", obrigando-os a manter, por um prazo mínimo, os *logs* dos usuários objetivando com que eles:
> a) divulguem campanhas contra a pornografia infantil e contra os crimes de ódio;
> b) orientem o público sobre a utilização não criminosa de salas de bate-papo, grupos e fóruns de discussão, *blogs*, páginas pessoais e outros serviços disponibilizados ao usuário;
> c) insiram, nos instrumentos de adesão ao serviço, cláusula que preveja a rescisão do contratual na hipótese do usuário valer-se do provedor para veicular fotografias e imagens de pornografia infantil, ou idéias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação;
> d) mantenham *link* pelo qual os usuários possam noticiar ao provedor signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum eletrônico, ou outro serviço prestado pelo próprio provedor;
> e) informem imediatamente ao Ministério Público Federal, quando tomem conhecimento de que abrigam pornografia infantil ou conteúdo manifestamente discriminatório, assegurada a proteção ao sigilo dos dados telemáticos;
> f) preservem e armazenem, pelo prazo mínimo de 6 (seis) meses, o registro de *logs* de acesso discado e, quando possível, também os IPs originários dos usuários dos serviços de *web page*, salas de bate-papo, *fotologs*, fóruns de discussão *on-line* e outros;
> g) solicitem e mantenham os dados cadastrais informados por seus assinantes de acesso;

[109] Idem

h) exijam que os novos usuários informem o número de algum documento validável de identificação, como por exemplo o número do RG ou do CPF.

Em notícia, o presidente da Associação de provedores criticou a forma como se responsabilizam os provedores de Internet*:*

> O presidente da Associação Brasileira dos Provedores de Internet, Antonio Tavares, defendeu há pouco, em seminário da Comissão de Direitos Humanos, a auto-regulamentação como melhor alternativa para a rede de computadores. Ele criticou as propostas no sentido de que os provedores de internet assumam a responsabilidade criminal por ilícitos praticados na rede.
> "O provedor não tem como verificar se as informações dadas pelos usuários são ou não verdadeiras. Não fugimos de nossos deveres, mas não podemos ficar com toda a responsabilidade", argumentou.
> Tavares também pediu a tramitação separada de alguns dispositivos do Projeto de Lei 84/99, que tipifica os crimes cometidos na internet. "É preciso cuidado ao legislar para não gerar atitudes negativas", recomendou.
> Identificação de internautas
> O professor de Ciências da Computação da Universidade de Brasília (UnB) Pedro Antonio Dourado de Resende, especialista em segurança da informática, disse duvidar da eficácia de mecanismos para identificar os usuários de internet. Ele observou que alguns dispositivos podem ser ineficientes e prejudiciais à economia.
> O secretário-executivo do Fórum Nacional pela Democratização da Comunicação, James Görgen, criticou as restrições ao software livre mantidas pelo Projeto de Lei 84/99. "Hoje, uma pessoa pode ser presa apenas por querer saber do software livre, mesmo sem ter a finalidade comercial", comentou.[110]

[110] Provedores recusam responsabilidade por crimes na internet. Disponível: <http://www2.camara.gov.br/internet/agenciacamara/chamadaExterna.html?link=http://www.camara.gov.br/internet/agencia/materias.asp?pk=94970> Acesso 14 novembro 2006.

3. Análise Constitucional da Nota Fiscal Eletrônica (NF-e)

A Nota fiscal eletrônica é um projeto coordenado pelo ENCAT (Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais) e desenvolvido em parceria com a Receita Federal, que tem por finalidade a alteração da sistemática atual de emissão da nota fiscal em papel, por nota fiscal eletrônica, com validade jurídica para todos os fins[111]. Neste sentido, foi publicado o Protocolo de Cooperação n. 03/2005, celebrado entre a União, por intermédio da Receita Federal do Brasil, os Estados e o Distrito Federal, por meio de suas Secretarias de Fazenda, Finanças, Receita ou Tributação e os Municípios (representados pela Associação Brasileira das secretarias de finanças dos municípios das capitais – Abrasf), com o fito de implantar a nota fiscal eletrônica como integrante de um projeto fiscal mais abrangente. Trata-se do "SPED": sistema público de escrituração digital, bem como, objetivando atender aos interesses das administrações tributárias e facilitar o cumprimento das obrigações acessórias pelos contribuintes. Tal medida se coaduna com o disposto no inciso XXII, do art. 37, da Constituição Federal, incluído pela Emenda Constitucional 42/2003, que dispõe:

> As administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, atividades essenciais ao funcionamento do Estado, exercidas por servidores de carreiras específicas, terão recursos prioritários para a realização de suas atividades e atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio.

---

[111] Portal da Nota Fiscal Eletrônica. Disponível em: http://www.nfe.fazenda.gov.br/portal/Default.aspx. Acesso em: 12.10.07.

Ainda, no campo da legislação pertinente, o Conselho Nacional de Política Fazendária – CONFAZ, celebrou o ajuste 07/05, para instituir a NF-e a ser utilizada pelos contribuintes do IPI e ICMS, apresentando, inclusive, em seu parágrafo único, a definição de NF-e. Ainda, temos os ajustes Sinief 04/06 e 05/07, que instituíram a nota e o documento auxiliar da nota fiscal eletrônica (Danfe), e suas alterações, bem como, o Ato Cotepe 72/05, vem a regulamentar as especificações técnicas da nota eletrônica, com reedições do "Manual de Integração — Contribuintes", contendo o detalhamento técnico e as especificações do sistema.

Paulatinamente é estratégia dos Estados tornarem a Nota Fiscal Eletrônica e o SEPED obrigatórios para diversos setores. Nesta linha a partir de setembro de 2008, a nota fiscal eletrônica vem se tornando obrigatória para mais sete setores: automotivo, de bebidas alcoólicas e refrigerantes, medicamentos, cimento, frigorífico, de aços semi-acabados e laminados, planos ou longos, relaminados, trefilados e perfilados, de ferro-gusa e fornecedores de energia elétrica.

O tema remete a Sociedade a reflexões, uma vez que a adesão que seria voluntária, repentinamente foi anunciada como obrigatória no final do ano de 2.007. Neste toar, em abril de 2008 passou a ser obrigatório o controle eletrônico para os setores de combustíveis líquidos e cigarros.

A proposta aparente da NF-e se destina a trazer benefícios para os contribuintes, na medida em que aumenta a competitividade das empresas brasileiras pela racionalização das obrigações acessórias, bem como tem como palanque a dispensa a emissão e guarda de documentos em papel.

Em relação à administração tributária, igualmente, prega vantagens, tendo em vista que pretende acarretar a padronização e melhoria na qualidade das informações, racionalização dos custos e uma fiscalização mais eficaz. Entretanto, estes investimentos feitos pela Receita Federal do Brasil, nos últimos anos, em sistemas informatizados que visam o cruzamento de dados de movimentações financeiras, ao mesmo tempo em que contribuem para uma maior

eficácia na fiscalização das atividades das empresas e das pessoas físicas, podem servir como obstáculo à emissão de notas fiscais e interferência na atividade econômica das empresas [112].

Trazemos como exemplo as dificuldades hoje encontradas em relação ao modelo vigente que se pretende substituir. Nesta vereda cuida os jornais de todo o Brasil a reportar que empresas de São Paulo, Minas Gerais e Rio têm encontrado grandes dificuldades de toda ordem quando tentam obter autorização para providenciar a impressão de seus documentos Fiscais. Estas empresas têm recorrido aos Tribunais Brasileiros para poderem emitir seus documentos Fiscais.

Nesse toar, tem sido informado pela mídia que as Secretarias das Fazendas dos mencionados Estados estão criando obstáculos para a liberação da Autorização de Impressão de Documentos Fiscais (AIDF) ou mesmo limitando de forma ilegal o número da quantidade de talões de notas para aquelas empresas com débitos fiscais. É uma disputa antiga entre fisco e contribuintes.

Pela nova sistemática do controle fiscal on-line, as Administrações Fazendárias pretendem superar este problema com as disputas judiciais. Pela regulamentação da NF-e o Fisco passa a gozar de permanente controle sobre a permissão ou denegação quanto à emissão de nota fiscal do contribuinte.

Ou seja, a Nota Fiscal Eletrônica pode vir a ser denegada automaticamente pelo sistema de informatizado da administração tributária, toda vez que o contribuinte solicite a autorização para emissão do mencionado documento fiscal e o sistema venha a apontar problemas ligados à regularidade fiscal do emitente ou receptor da nota eletrônica.

Ou seja, o fisco resguarda o direito de exercer o poder de “rejeitar” o uso da nota eletrônica, a todo o tempo, em caso de irregularidade fiscal do contribuinte emissor da nota ou mesmo do contribuinte destinatário. Cumpre dizer que à administração fazendária, não confere o direito de recurso administrativo ao

---

112 Queiroz, Luiz. Sistemas da Receita retornam aos cofres públicos o que foi sonegado. 20/08/2007 Disponível em <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=9237&sid=16&tpl=printerview > acesso em maio de 2008.

contribuinte e reserva-se a escolha de para, quem, quando e onde deve ocorrer o faturamento das empresas. Ou seja, trata-se de uma sentença administrativa cartesiana e eletrônica emitida por um sistema de computadores (ALMEIDA FILHO, 2007)[113] que passará a vedar o faturamento das empresas nestes casos.

Esta tutela restritiva informatizada padece de flagrante inconstitucionalidade, ao vedar o faturamento de empresas, por fere o princípio do contraditório e da ampla defesa, bem como, do direito de resposta e do devido processo legal na esfera administrativa. Ademais, a sentença denegatória ou de rejeição fazendária é feito pelo sistema de *Web Services* da Administração Fazendária, e não pelas mãos do homem. Portanto são decisões eletrônicas automáticas e, portanto, carentes de fundamentação cerceando a defesa de contribuintes na fase administrativa e, por sua vez, procura dificultar o ingresso do contribuinte na esfera fase judicial.

A Constituição, por sua vez, veda a imposição do Estado de todo o tipo de diferenças entre contribuintes, em função de "irregularidade fiscal", uma vez que todos podem discutir débitos tributários. Ademais, a ação da administração vai contra os princípios da Livre Iniciativa e dos princípios norteadores da Justiça fiscal do Estado Democrático e Social de Direito que conquistamos a duras penas e batalhas.

Por outro lado, pelo sistema tradicional, as sentenças de primeiro grau e acórdãos têm sido favoráveis aos contribuintes em relação ao sistema tradicional na obtenção da AIDF[114]. O panorama deve piorar muito com a implantação da nota fiscal eletrônica. Ou seja, mesmo após a obtenção do "ato de concessão", ou seja, a "autorização" para transmissão de notas fiscais eletrônicas, continua o Contribuinte a depender de um processo de autorização eletrônico da Secretaria da Fazenda dos Estados para poder realizar o seu faturamento.

---

[113]. O autor menciona que no Processo Eletrônico não podemos permitir que o mesmo modifique o processo de modo a permitir sentenças cartesianas emitidas por computador.

[114] A Autorização de Impressão de Documentos Fiscais é aquela que o Contribuinte vem a solicitar a Administração Tributária autorização para mandar produzir em uma Gráfica licenciada um determinado lote de documentos fiscais. Após a obtenção desta autorização, seja pelas vias tradicionais, seja através de ação judicial, não precisa o contribuinte solicitar autorização a Administração Tributária para realizar faturamento ou o uso dos documentos fiscais.

A nota eletrônica gravada pela Administração Fazendária Estadual com status “Denegado o uso” por força de “irregularidade fiscal”, do emitente ou do destinatário, não poderá ser utilizada pelo contribuinte. Em outras palavras, o número da NF-e denegado não poderá mais ser utilizado, cancelado ou inutilizado.

Na nova sistemática do controle fiscal on-line, as Administrações Fazendárias têm permanente controle sobre a permissão ou denegação da solicitação da nota fiscal do contribuinte, após a averiguação de problemas ligados a sua regularidade fiscal. Ou seja, o fisco se resguarda o direito de exercer o poder de “rejeitar” o uso da nota eletrônica, a todo o tempo, em caso de irregularidade fiscal do contribuinte emitente ou mesmo do contribuinte destinatário. Cumpre dizer que à administração fazendária, não confere o direito de recurso administrativo ao contribuinte e reserva-se a escolha de para, quem, quando e onde ocorre o faturamento das empresas. Ou seja, trata-se de uma sentença administrativa cartesiana e eletrônica emitida por um sistema de computadores[115] que irá vedar o faturamento.

O sistema de cruzamento de dados, as Administrações Estaduais Fazendárias poderão negar a emissão da nota fiscal eletrônica se o vendedor ou comprador tiverem problemas fiscais de “natureza grave”, ou mesmo, mera irregularidade fiscal momentânea. Ou mesmo, por outros critérios subjetivos pautados na expressão “irregularidade fiscal”. Não existe um critério estabelecido.

> Cláusula sexta, Previamente à concessão da Autorização de Uso da NF-e, a administração tributária da unidade federada do contribuinte analisará, no mínimo, os seguintes elementos: I - a regularidade fiscal do emitente; II - o credenciamento do emitente, para emissão de NF-e; III - a autoria da assinatura do arquivo digital da NF-e; IV - a integridade do arquivo digital da NF-e;V - a observância ao leiaute do arquivo estabelecido em Ato COTEPE;VI - a numeração do documento.
>
> Cláusula sétima Do resultado da análise referida na cláusula sexta, a administração tributária cientificará o emitente:I - da rejeição do

115 [] ARAÚJO ALMEIDA FILHO, José Carlos de. Processo eletrônico e teoria geral do processo eletrônico. Rio de Janeiro: Forense, 2007. O autor menciona que no Processo Eletrônico não podemos permitir que o mesmo modifique o processo de modo a permitir sentenças cartesianas emitidas por computador.

> arquivo da NF-e, em virtude de:a) falha na recepção ou no processamento do arquivo;b) falha no reconhecimento da autoria ou da integridade do arquivo digital;c) remetente não credenciado para emissão da NF-e;d) duplicidade de número da NF-e;e) falha na leitura do número da NF-e;f) outras falhas no preenchimento ou no leiaute do arquivo da NF-e;II - da denegação da Autorização de Uso da NF-e, em virtude da irregularidade fiscal do emitente;III - da concessão da Autorização de Uso da NF-e;.§ 1º Após a concessão da Autorização de Uso da NF-e, a NF-e não poderá ser alterada.§ 2º Em caso de rejeição do arquivo digital, o mesmo não será arquivado na administração tributária para consulta, sendo permitido ao interessado nova transmissão do arquivo da NF-e nas hipóteses das alíneas "a", "b" e "e" do inciso I do "caput".§ 3º Em caso de denegação da Autorização de Uso da NF-e, o arquivo digital transmitido ficará arquivado na administração tributária para consulta, nos termos da cláusula décima quinta, identificado como "Denegada a Autorização de Uso".§ 4º No caso do § 3º, não será possível sanar a irregularidade e solicitar nova Autorização de Uso da NF-e que contenha a mesma numeração.§ 5º A cientificação de que trata o "caput" será efetuada mediante protocolo disponibilizado ao emitente ou a terceiro autorizado pelo emitente, via internet, contendo, conforme o caso, a "chave de acesso", o número da NF-e, a data e a hora do recebimento da solicitação pela administração tributária e o número do protocolo, podendo ser autenticado mediante assinatura digital gerada com certificação digital da administração tributária ou outro mecanismo de confirmação de recebimento.§ 6º Nos casos dos incisos I ou II do "caput", o protocolo de que trata o § 5º conterá informações que justifiquem de forma clara e precisa o motivo pelo qual a Autorização de Uso não foi concedida.[116]

Atualmente o contribuinte somente poderá confeccionar, mandar confeccionar ou utilizar os impressos fiscais previstos em lei, mediante requerimento e prévia autorização, ou “ato de concessão chamado de AIDF”, ou a obtenção de regime especial [117] da Secretaria da Fazenda.

Ocorre que, atualmente, depois de superada esta etapa pelo Contribuinte, seja na fase administrativa ou na esfera judicial, não existe mais interferência ou

---

[116] AJUSTE SINIEF 07/05, Publicado no DOU de 05.10.05. Republicado no DOU de 07.12.05. Alterado pelos Ajustes 11/05, 02/06, 04/06,05/07. Cláusula nona Fica instituído o Documento Auxiliar da NF-e - DANFE, conforme leiaute estabelecido em Ato COTEPE , para uso no trânsito das mercadorias ou para facilitar a consulta da NF-e, prevista na cláusula décima quinta. § 6º O DANFE poderá conter outros elementos gráficos, desde que não prejudiquem a leitura do seu conteúdo ou do código de barras por leitor óptico. § 7º Os contribuintes, mediante autorização de cada Unidade da Federação, poderão solicitar alteração do leiaute do DANFE, previsto em Ato COTEPE, para adequá-lo às suas operações, desde que mantidos os campos obrigatórios.

[117] Existem os chamados impressos de segurança. Para adquirir os mesmos o contribuinte deve preencher certos requisitos de confiabilidade para emissão do documento. Esta autorização para compra e emissão e impressão simultânea de documentos discais depende da concessão de regime especial a ser outorgado pelas administrações fazendárias.

vínculo do fisco com a etapa de processamento ou autorização para emissão das notas fiscais dos contribuintes.

Vale dizer que, uma vez outorgada pelo Estado a concessão para autorização de impressão de documentos fiscais (AIDF), o Estado não interfere na iniciativa empresarial. Destarte, após esta etapa de obtenção da AIDF, a empresa está livre de controle, seja on-line ou em tempo real, para comercializar seus produtos e realizar o faturamento sem maiores interferências. A empresa fica sujeita apenas ao regular processo de fiscalização e posterior autuação fiscal prevista em lei. Ou seja, no processo de fiscalização tradicional, o contribuinte não tem maiores obstáculos diretos ao realizar seu faturamento e pode realizar a competente defesa administrativa.

Como mencionado, o mesmo já não ocorre com a Nota Fiscal Eletrônica – "NF-e". Como dito, não existem garantias de livre faturamento, posteriormente ao ingresso do contribuinte no mencionado projeto, cumprindo metas, realizando investimentos, mesmo após obter seu "Ato de Credenciamento" com a homologação de seu sistema de emissão de NF e, ulterior, geração eletrônica de personificação digital da nota eletrônica (DANFe). Ou seja, o contribuinte não usufrui das mesmas garantias e liberdade fiscal inerente aos meios convencionais. Com efeito, o ingresso no sistema e "ato concessório" e tudo o mais que antecede a geração da nota, não representa garantia de que o contribuinte, conforme sua necessidade e expectativa, venha a obter a autorização de emissão da Nota Eletrônica.

A Fazenda do Estado passa a gozar de um permanente poder de interferência e acompanhamento (on-line) em tempo real das operações comerciais de contribuintes. O referido facilita e fortalece o controle e a fiscalização por meio de intercâmbio e cruzamento constante de informações entre as administrações tributárias federal, estadual e municipal.

É simples entender o funcionamento: o contribuinte emite um arquivo eletrônico que contém informações fiscais da operação comercial. O arquivo será transmitido à Secretaria da Fazenda. Após o estágio de verificação da autoria e

integridade do documento fiscal poderá ser emitido, ou não, a chamada "autorização de uso da NF-e". Junto com a autorização o fisco devolverá um protocolo, sem o qual o contribuinte não poderá realizar o trânsito da mercadoria. Em resumo, o arquivo digital da NF-e, depois de criado e emitido, só poderá ser utilizado como documento fiscal após esta expressa e cabal autorização fiscal.

As Secretarias de Fazenda e a Receita Federal disponibilizarão consulta da NF-e aos que tiverem a chave de acesso do documento eletrônico.

Nessa esteira, apenas considera-se Nota Fiscal Eletrônica, o documento emitido e armazenado eletronicamente de existência apenas digital, com o intuito de documentar operações e prestações, cuja validade jurídica é garantida pela assinatura digital[118] do emitente (autoria e integridade) e somente pode ser utilizada como documento fiscal válido, após receber pela fazenda a autorização de uso, antes da ocorrência do fato gerador [119].

Ou seja, em tese, empresas que tenham "pendências" ou subjetivas "irregularidades fiscais", ou seja, todos aqueles que não estiverem com suas "obrigações em dia", poderão vir a ter suas notas eletrônicas rejeitadas. Sem maiores fundamentos, e respostas, o Estado passa a gozar de um "super" poder eletrônico de fiscalização. Explico: o Fisco, pela redação dos Convênios e Protocolos celebrados no Confaz, pode a qualquer tempo, e sem aviso prévio, exercer a opção de barrar a autorização da Nota Eletrônica e a respectiva impressão do DANF-e. Em contrapartida, os contribuintes não terão, em seu

---

[118] Esta validade jurídica citada é de autoria e integridade. Terceira pessoa ao cometer ilícito poderá emitir indevidamente notas fiscais sem a real autorização e manifestação de vontade do contribuinte.

[119] O Órgão Público ou empresa receberá o DANFE juntamente com a mercadoria e deverá realizar a verificação da validade jurídica da respectiva NF-e na seção Consulta ou no site www.nfe.fazenda.gov.br, utilizando-se de sua chave de acesso. Com a consulta, o destinatário tem garantia da existência e validade da NF-e. Curioso notar que o Portal que trata da NF-e reduz esta verificação a mera informação de existência e validade computacional e não menciona garantia a verificação pelo fisco de autoria e integridade. Sabemos que a Nota existe é valida, mas pode ser conferida e novamente conferida a qualquer tempo. Realizada a consulta descrita acima e verificada a existência e a validade da NF-e, e não autoria e integridade, o DANFE poderá ser utilizado como documento hábil para a comprovação documental junto à auditoria do Tribunal de Contas, em substituição às Notas Fiscais em papel modelos 1 ou 1A.

poder, notas fiscais tradicionais ou impressos de formulários de segurança em volume razoável para faturamento.

Em outras palavras, o direito de comprar e vender, ou de ir e vir, em termos comerciais vai ser em breve mitigado, cada vez mais restringido, como forma de obrigar o contribuinte a realizar o pagamento de seus tributos. A Nota Fiscal Eletrônica pode ser barrada até o contribuinte sanar a irregularidade fiscal.

O Controle eletrônico por seu lado, procura travar uma batalha sem precedentes contra a sonegação fiscal. A motivação é nobre, mas a ação fiscal parece não ter limites. Outra medida semelhante foi anunciada pela Procuradoria Geral da Fazenda Nacional. Foi anunciado que, com fundamento na Lei Complementar 104/2001, ao alterar o artigo 198 do Código Tributário Nacional, teria flexibilizado o sigilo fiscal quando disse que não é vedada a divulgação de informações relativas a inscrições na Dívida Ativa. Neste sentido, a PGFN menciona que contribuintes em débito terão seus nomes enviados para o SERASA.

Não se pode negar que a legislação referente à rejeição da nota eletrônica e inovação do controle via SERASA, violam de forma cabal e irretorquível a regra *in casu*, de aplicabilidade imediata, prevista no artigo 170 parágrafo único da Constituição Federal, que garante a livre iniciativa [120]. Por outro lado, o Estado não tem o poder de exercer esta "tutela punitiva tecnológica " (BARROS, 2007) e assim, limitar a atividade econômica dos contribuintes. Em relação ao controle do poder público via SERASA temos a súmula 547 do Supremo Tribunal Federal, mencionando que o contribuinte em débito não pode ser impedido de exercer suas atividades profissionais.

O envio e rejeição de uma nota fiscal pela Internet não é o mesmo de enviar uma petição pela mesma via aos nossos Tribunais, por meio de certificação digital. Trata-se da interferência do Estado na atividade privada do contribuinte, conforme as regras pré-estabelecidas na página 65 *"usque"* 68 do "manual de integração – Contribuinte".

---

120 Constituição Federal de 1988, art. 5º, inciso XIII.

O Professor Marco Antonio de Barros (2007), ao comentar os meios tecnológicos a serviço do Estado, menciona que:

> (...) nas relações que se formam entre o Estado e os cidadãos, o ideal almejado pela sociedade consiste em que o Estado seja aberto às pessoas, ou seja, que se apresente livre dos conhecidos entraves burocráticos que só servem para distanciar as pessoas que procuram resguardar seus legítimos interesses. Vale dizer, o Estado não foi criado para atuar como fator de enfraquecimento da Cidadania. Ao contrário, o Estado deve se aproximar do cidadão.

Ademais, os Convênios e Protocolos não têm critério legal razoável, pautado em elementos de juridicidade capaz de revelar aos tutelados, em que eventos, ou até que importância o sistema de *Web service* eletrônico vai considerar o contribuinte no estágio de "irregularidade fiscal". Ou seja, foi adotado critério de ordem subjetiva da fiscalização on-line em tempo real, que deve certamente limitar a ação de certos setores da economia, ou determinados contribuintes, ocasionando o trancamento do faturamento e, por sua vez, a concorrência desleal. O lesado é o Estado - Cidadão – Arrecadador[121]

Como dito, a rigor, a atividade dos Estados não pode ter por finalidade interferir na atividade econômica privada, mas apenas regulamentá-la. A administração fazendária, ainda que o propósito seja nobre, criando o controle do fisco em tempo real, acaba por interferir e controlar o faturamento das empresas. Ou seja, não pode ser concebida esta restrição on-line, a qual, conforme nossa pesquisa e interpretação, certamente, vai gerar uma leva de ações judiciais.

O Professor Hugo de Brito Machado (2007) leciona que:

> [...] a utilização de meios indiretos para compelir o contribuinte ao pagamento de tributos, devidos ou não, é prática antiga, não obstante seja pacífica a jurisprudência que afirma a falta de amparo jurídico para a imposição do que se têm denominado sanções políticas. É inescondível a prática reiterada, em todos os níveis, dessa atitude abusiva, a demonstrar que as autoridades da Fazenda Pública não têm o mínimo respeito pelo entendimento do Poder Judiciário. Começaremos examinando a garantia constitucional da livre iniciativa econômica, para deixarmos claro que o direito de exercer qualquer atividade econômica é

[121] Entendemos o Estado - Cidadão- Arrecadador na forma como foi colocada quando o Estado passa ser o próprio prejudicado por determinada estratégia de governo, e posteriormente o lesado em última análise é o Cidadão.

> independente do dever de efetuar o pagamento dos tributos, até porque a Fazenda Pública dispõe de meios para a cobrança de seus créditos e que não se justifica substituir estes meios pela imposição de sanções políticas, entre elas, a proibição de impressão de blocos de notas fiscais, como forma de compelir o contribuinte a pagar o tributo, devido ou não, para poder exercitar sua atividade. Depois examinaremos em que consiste essa forma de sanção política, para demonstrar que sua aplicação não atende ao interesse do Fisco de manter sob controle a prática de fatos geradores de tributo para ensejar a cobrança dos tributos correspondentes, e, por outro lado, inviabiliza inteiramente a atividade do contribuinte. Demonstraremos a seguir que essa prática contraria a jurisprudência firmada pelos tribunais superiores, e não se harmoniza com o princípio da razoabilidade. Finalmente, indicaremos o caminho a ser trilhado pelo contribuinte para o controle eficaz do arbítrio praticado pelos agentes públicos na relação tributária".

Para alguns setores pesquisados[122], este novo procedimento do fisco em tempo real, além de não trazer qualquer vantagem relativa a custo ou "otimização" de processos de faturamento, ao contrário, é mais caro, oneroso e arriscado aos contribuintes que vierem a aderir esta sistemática. Dentro de uma empresa nenhum executivo quer assinar como responsável [123] pela implantação deste projeto, sabendo que a Nota Fiscal Eletrônica de uma organização econômica

---

[122] Segundo dados da Associação Brasileira da Indústria de Formulários, Documentos e Gerenciamento da Informação. Entrevistamos seu presidente Antônio Leopoldo Curi na data de 18 de maio de 2.008.

[123] Reunião Controle de Acesso/Sped – 04 a 06 de setembro – Fortaleza A equipe do Sped se reuniu no período de 4 a 6 de setembro, em Fortaleza-CE, para discussão dos aspectos operacionais de Download, Dados Agregados e Controle de Acesso ao Ambiente Nacional do Sped, temas de interesse geral das empresas em face à importância das informações a serem disponibilizadas por elas.Como todo o trabalho que vem sendo efetuado no projeto, a divulgação das decisões que direcionarão os trabalhos futuros é uma forma de dar transparência e tranqüilizar a comunidade empresarial quanto ao desvelo que a equipe de desenvolvimento terá em relação aos aspectos de sigilo e segurança das informações a serem repassadas aos usuários do Sped. Dentre as decisões tomadas, ressaltam-se: - as informações contábeis detalhadas somente serão disponibilizadas a partir de documento Digital assinado que as requeira.Além da assinatura digital no documento, somente pessoa previamente cadastrada poderá baixar as informações;- efetuado o download, a informações sobre o tal procedimento ficarão, imediatamente, acessíveis ao titular da escrituração; - também ficarão disponíveis para o titular da escrituração, as informações sobre o acesso a "dados contábeis agregados".A reunião, coordenada pela Receita Federal, foi promovida pela Secretaria de Fazenda do Ceará e teve a participação dos usuários do Sped (Banco Central, CVM, Susep, DNRC, Jucemg, Serpro, Prefeituras de BH, RJ e Fortaleza, Secretarias de Fazenda do Ceará e Santa Catarina, RFB)e do coordenador do comitê gestor das empresas piloto. Obtido por meioeletrônico no endereço: http://www.sped.fazenda.gov.br/noticias.aspx?id=4

pode ser denegada em função de “irregularidade fiscal do emitente ou irregularidade fiscal do destinatário” [124].

O Professor Ives Gandra da Silva Martins, ao comentar o projeto de controle on-line, afirma que:

> [...] se tal sistemática for imposta implicará afronta pelo Confaz dos princípios norteadores da administração pública da razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência, pelo caráter coercitivo implícito limitador da atividade econômica. E também contrário, diga-se, à orientação jurisprudencial do Supremo Tribunal Federal manifestada nas súmulas 70, 323 e 547, que não admitem a interdição de estabelecimento como meio coercitivo para cobrança de tributo, a apreensão de mercadorias como meio coercitivo para pagamento de tributos e a vedação de a autoridade proibir o contribuinte em débito que exerça suas atividades profissionais.

Outro ponto que vale ressaltar novamente é que não existe qualquer apelo ecológico pela redução do consumo de papel. Especialistas ambientais consultados revelam que na verdade o lixo eletrônico é de natureza grave e de difícil reciclagem. A indústria nacional produtora de papel é uma das mais premiadas em todo o mundo pelos seus maciços investimentos no meio ambiente sustentável. Portanto, para estes especialistas inexiste apelo ecológico ou redução de impacto ambiental em função da adesão de empresas a este projeto. Aqueles que comentam em sentido contrário certamente não consultaram a área de meio ambiente da empresa, ou mesmo, não contrataram uma empresa de consultoria e auditoria ambiental.

Para economia com cartuchos e suprimentos de impressão a Laser ou Jato de tinta, muitas empresas informaram[125] que pretendem utilizar o DANFE pré-impresso, contendo elementos gráficos[126]. Portanto, é fraco e carente de estudo o argumento da “economia pela redução de custo de papel”.

---

[124] Conforme páginas 65 “usque” 68 do Manuel de Integração Técnica entre Fisco e Contribuinte disponível na Internet.

[125] Dados pesquisados em maio de 2.008 junto a Associação Brasileira da Indústria de Formulários, Documentos e Gerenciamento da Informação- ABRAFORM.

[126] AJUSTE SINIEF 07/05, Publicado no DOU de 05.10.05. Republicado no DOU de 07.12.05. Alterado pelos Ajustes 11/05, 02/06, 04/06,05/07. Cláusula nona Fica instituído o Documento Auxiliar da NF-e - DANFE, conforme leiaute estabelecido em Ato COTEPE , para uso

Conforme comentamos em outras oportunidades, a legislação é insuficiente, prematura, nas próprias deliberações e protocolos dos órgãos fazendários. Este projeto foi uma adaptação do Projeto Chileno, país onde se encontra vigente o imposto único (IVA) e com PIB semelhante ao da Cidade de Campinas. A Guerra Fiscal tem sido apontada por especialistas como um forte impeditivo à implantação da nova obrigação acessória que, em alguns casos, o contribuinte favorecido com incentivo fiscal concedido por outra unidade da Federação fará uma "denúncia espontânea on-line".

Apesar de todos os esforços do Governo Federal, os Estados não chegam a acordo sobre fim de incentivos. São anos de intensas discussões. Contudo os Estados analisando o processo com perdas de receita em suas fronteiras não conseguiram chegar a um senso comum junto ao Governo Federal para pôr termo ao conflito fiscal. O convênio para a convalidação dos benefícios fiscais e sua extinção após 2011 não obteve acordo de Goiás que tem implantado o TARE, bem como do Espírito Santo, que goza do Fundo de Desenvolvimento das Atividades Portuárias do Espírito Santo (Fundap) desde 1970. Este último foi aceito pelo Estado de São Paulo por muitos anos, inclusive, autorizando o desembaraço aduaneiro diretamente em solo Paulista, sendo recolhido o Imposto aos Cofres Capixabas. Vários Estados do Nordeste também tem evitado o consenso no corpo do Conselho Nacional de Política Fazendária (Confaz).

A decisão, para ser válida no âmbito do CONFAZ, necessita de unanimidade de seus membros, uma vez que a mesma ainda não foi alcançada. Os secretários decidiram apenas encaminhar ao governo e ao Congresso uma proposta da maioria. Em tese a decisão caberá aos parlamentares.

---

no trânsito das mercadorias ou para facilitar a consulta da NF-e, prevista na cláusula décima quinta. § 6º O DANFE poderá conter outros elementos gráficos, desde que não prejudiquem a leitura do seu conteúdo ou do código de barras por leitor óptico. § 7º Os contribuintes, mediante autorização de cada Unidade da Federação, poderão solicitar alteração do leiaute do DANFE, previsto em Ato COTEPE, para adequá-lo às suas operações, desde que mantidos os campos obrigatórios.

Mesmo minoritários no Congresso, os Estados contrários ao fim da guerra fiscal vem apontando uma série de obstáculos para a aprovação da emenda constitucional da reforma tributária, que vai prever a proibição de novos incentivos fiscais e a extinção progressiva dos atuais incentivos.

As empresas que futuramente aderirem unicamente, e 100%, ao sistema eletrônico, que tenha aderido a incentivos fiscais ou possuam pendências ou discussões com as administrações fazendárias, ou mesmo as empresas que não se utilizam de incentivos, devem mensurar de forma muito eficiente o volume de notas fiscais que deverão ficar disponíveis na eventualidade de contingências como: rejeição, denegação por problemas fiscais genéricos, queda do sistema, problemas de lentidão na internet por ausência de infra-estrutura de comunicação, vírus, ataque de *crackers*, problemas na rede, crimes cibernéticos, crimes tecnológicos, ataque de negação de serviços, dente outras ameaças. Os investimentos em segurança devem ser maciços e constantes.

A empresa também deve ficar atenta à obrigatoriedade de armazenar e proteger suas informações fiscais em meio próprio ou servidor próprio, relativas à NF-e. O Poder Público também tem seu servidor, seu banco de dados, mas essas informações só ficam abertas no sistema da fiscalização, por um determinado período de tempo. Após este período, tais informações são resumidas ou , até mesmo, podem ser deletadas. Apesar de o Fisco compartilhar das mesmas informações o Convênio prevê que a obrigação de manutenção das informações cabe ao contribuinte quando demandado a realizar sua apresentação.

De acordo com as normas mencionadas, não está previsto na legislação se o Estado deverá fornecer esses dados. Por isso, se a empresa tiver uma perda de arquivos, pode até recorrer à via judicial para não ter que arcar com o prejuízo e exigir que o Estado as forneça. Agora, tudo isso no plano das hipóteses, e da pesquisa, uma vez que estamos em uma fase de transição.

No dia 15 de agosto, a imprensa[127] noticiou o despacho do juiz Fernão Borba Franco, da 14ª Vara da Fazenda Pública de São Paulo, beneficiando uma empresa varejista do ramo farmacêutico. A decisão intima a Fazenda paulista a expedir autorização para as notas fiscais tradicionais da empresa, no prazo de 24 horas, sob pena de multa diária de R$ 5 mil. "Deve ser advertido de que sua recusa caracteriza, em tese, ato de improbidade administrativa, com prejuízos ao erário, dada a incidência da multa", completou o juiz na decisão. No caso de uma Nota Fiscal Eletrônica o tema pode ficar mais complicado, uma vez que a fiscalização pode alegar que a empresa consentiu ser fiscalizada em tempo real e aderiu aos termos do Projeto, não podendo mais solicitar as Notas Fiscais em papel.

Uma das advogadas que defendeu a empresa, Thaís de Ávila Marquez, explicou que entrou com mandado de segurança com pedido de liminar para que a empresa possa imprimir quantas notas forem necessárias. "A Fazenda estava concedendo notas parcialmente. Por exemplo, se a empresa solicitava 30 mil notas, eram liberadas 5 mil" disse a advogada. A defensora alegou ofensa à Constituição Federal, com relação ao livre exercício de atividade econômica, independentemente de autorização de órgãos públicos.

---

127 Notícia publicada na Gazeta Mercantil de quinta feita 16 de agosto de 2.007. Dentre os trechos interessantes na notícia também se comenta sobre a Nota Fiscal Eletrônica. Regime-especial O procurador-chefe da Procuradoria Geral do Estado de São Paulo, Clayton Eduardo Prado, argumenta que o Fisco só age assim com as empresas que são super devedoras, que por vários meses declaram débito e não pagam ou quando a procuradoria não localiza nenhum patrimônio delas. "Dispositivo do regulamento do ICMS do estado de São Paulo prevê imposição de um regime especial nessa hipótese", alega o procurador. Para Prado, são casos que apenas pela execução fiscal, sem uma ação preventiva, a Fazenda não conseguiria impedir grave lesão ao erário público. Outras decisões A advogada Letícia Ritter, do Martinelli Advocacia Empresarial, já obteve sentença do Tribunal de Justiça do Rio Grande do Sul (TJ-RS) liberando a AIDF para uma cliente. "Há súmulas do Supremo Tribunal Federal (STF) que protegem o contribuinte nesse caso", afirma. No dia 30 de julho, o Supremo concedeu liminar à Med Express Comércio de Medicamentos e Materiais Médico Hospitalar com base nessas súmulas. O advogado Eurivaldo Neves Bezerra, do escritório Neves Bezerra Advogados Associados, tem aproximadamente 300 ações ajuizadas em nome de empresas que tiveram a AIDF barrada pela Fazenda fluminense e em 90% dos casos julgados foi concedida a liminar. "Se a empresa está devendo e o Fisco ainda bloqueia a emissão de notas fiscais, como a empresa vai faturar para quitar seus débitos?", questiona o advogado. Em alguns casos, Bezerra pede que a Fazenda seja responsabilizada caso venha sofrer por ficar impossibilitada de emitir notas fiscais. Para ele, a instalação da Nota Fiscal Eletrônica (NF-e) deve agravar essa situação. "Vai ficar mais fácil para o Fisco identificar quem está devendo e bloquear a emissão digital", afirma o advogado.

Vale lembrar, igualmente, a assinatura do protocolo ICMS de n° 30/06/2007, por alguns Estados, alterando as disposições do Protocolo ICMS 10/07. O Referido estabelece a obrigatoriedade da utilização da Nota Fiscal Eletrônica (NF-e) para os setores de fabricação de cigarros e distribuição de combustíveis líquidos. Previsão é abril de 2.008. A obrigatoriedade se aplica a todas as operações destes contribuintes, ficando vedada a emissão de Nota Fiscal modelo 1 ou 1-A pelos mesmos.

O SRF informa[128] que atualmente existem muitas discussões internas dentro do SPED para saber dentro do "staf" da empresa, quem será o responsável legal previamente cadastrado junto a SRF (titular da escrituração), pelo acesso e envio das notas fiscais eletrônicas e outros arquivos eletrônicos.

A equipe de desenvolvimento tem preocupação em relação aos aspectos de sigilo e segurança das informações a serem repassadas aos usuários do Sped. Dentre as decisões tomadas, ressaltam-se: - as informações contábeis detalhadas somente serão disponibilizadas a partir de documento Digital assinado que as requeira. Além da assinatura digital no documento, somente pessoa previamente cadastrada poderá baixar as informações; - efetuado o *download*, a informações sobre o tal procedimento ficarão, imediatamente, acessíveis ao titular da escrituração; - também ficarão disponíveis para o titular da escrituração, as informações sobre o acesso a "dados contábeis agregados".

Atualmente, cerca de oitocentas empresas consultadas[129] demonstram grande preocupação com perda de dados e informações. Muitas empresas do projeto piloto e integrantes da segunda fase do projeto nos fóruns de discussão levantaram grande preocupação em relação ao armazenamento dos livros e

---

[128] Conforme dados colhidos do Senhor Gerson A. Prochnow, Supervisor da Equipe Nota Fiscal Eletrônica ambiente Nacional, informou em palestra em São Paulo no escritório Pinheiro Neto em outubro de 2.007.

[129] O Pesquisador proferiu treinamento para 800 empresas em 2.006: CEAD-CONTMATIC PHOENIX - Curso Especial de Aprimoramento e Desenvolvimento da CONTIMATIC, http://www.contimatic.com.br/. Treinamento apresentado: Pontos polêmicos sobre a Implantação da Nota Fiscal Eletrônica e o atual cenário das fraudes virtuais. Local/Data: Auditório Nobre da Matriz - CONTMATIC PHOENIX (agosto e setembro de 2.006). CISP - Central de Informações São Paulo. Tema apresentado: Inovação e a Nota Fiscal Eletrônica. Local/Data: Auditório CISP (novembro de 2.006).

arquivos fiscais. Explicaram que anteriormente ao Projeto SPED, as informações fiscais da empresa ficavam divididas em vários livros. Com o SPED todas as informações fiscais dos contribuintes ficam armazenas em um único banco de dados e sistema. Na eventualidade de rompimento, perda ou captura por terceiros, perde-se todos os dados locados no sistema da Receita Federal.

A SRF menciona[130] a falta de capacidade para atuar no SPED em ambiente de alto desempenho. A SRF comenta a falta de capacidade atual da SRF em receber dados, simultaneamente acima de 600MB, em conjunto com outros. Ou seja, vários arquivos enviados simultaneamente por várias empresas acima de 600MB poderiam congestionar o sistema de recebimento. Atualmente os especialistas da SRF estão fazendo vários testes para envio em ambiente de alta capacidade, bem como, estudando e criando soluções para compactação.

Os especialistas da SRF, no momento de indagação de contribuintes mencionam nos Fóruns de discussão de forma consciente que, tanto o SPED e NF-e estão em fase piloto e que no papel tudo é lindo, mas na hora de aplicar os testes no dia a dia, as empresas têm tido problemas.

Como visto, após a concessão administrativa ou Judicial da Autorização de Impressão de Documentos Fiscais, o contribuinte não sofrerá interferência direta e on-line advinda das novas tecnologias voltadas à fiscalização. Ou seja, contribuintes terão em seu poder notas fiscais em volume suficiente para o exercício de sua atividade econômica. As empresas que aderirem a Nota Eletrônica espontaneamente, ou por estarem obrigadas, serão fiscalizadas na forma on-line e poderão ter suas notas denegadas em função de problemas fiscais do emitente ou receptor da nota, a critério das administrações fazendárias.

O cenário atual da utilização da nota fiscal eletrônica no país nos é dado, por exemplo, por uma pesquisa da visão empresarial conduzida pela Associação Brasileira de e-Business, finalizada em junho de 2007 e que entrevistou 75 empresas de grande e médio porte, das quais 72% apresentam faturamento anual

---

130 Conforme dados colhidos do Senhor Gerson A. Prochnow, Supervisor da Equipe Nota Fiscal Eletrônica ambiente Nacional, informou em palestra em São Paulo no escritório Pinheiro Neto em outubro de 2.007.

superior a R$ 100 milhões. O resultado encontrado demonstra que metade dessas companhias considera não ter conhecimentos suficientes para adotar o projeto. E, mais do que isso, só pretende fazê-lo quando algum tipo de lei torná-la obrigatório[131].

Estas pesquisas se revelam também com cerca de 2.000 executivos de grandes e médias empresas entrevistados pela nossa equipe durante as 20 últimas palestras ministradas. Os executivos da área fiscal, ambiental, tecnologia da informação, cada qual em sua área tem uma preocupação, em síntese, revelam ter algum tipo de receio, insegurança ou desconhecimento em relação ao projeto.

Apesar de tantas propagandas fantasiosas sobre economia de custos e vantagens para as empresas, os resultados do projeto, Nota Fiscal Eletrônica estão abaixo do esperado e o SEPD ainda apresenta dificuldades[132]. Outra recente notícia informa que quando da implantação e posterior oficialização do Projeto, em agosto de 2005, a previsão era a de que até o fim de 2007 fossem emitidos 100 milhões de notas ao mês. “Mas desde setembro do ano passado, quando a primeira nota virtual foi emitida no país até ontem, o sistema gerou pouco mais de 1,1 milhões de notas no total”. Ou seja, em quase um ano de funcionamento o resultado é cem vezes menor do que o esperado [133]

Ademais, poucas são as empresas verdadeiramente interessadas ou preocupadas com o surgimento da obrigatoriedade da NF-e da noite para o dia.

Em maio de 2.007, o ministro da Fazenda, Guido Mantega, anunciou que o governo federal disponibilizará R$ 300 milhões para todos os estados brasileiros investirem na modernização de ações de combate à sonegação fiscal. Entretanto,

---

131 CIO Magazine - julho/2007

132 Advogados entrevistados participaram do encontro. Obtido por meio eletrônico: http://www.sped.fazenda.gov.br/noticias.aspx?id=3. Apresentação SPED na ABRASCA Dando continuidade à agenda comum de eventos para divulgação do projeto em parceria com as entidades participantes do seu projeto-piloto, a equipe de supervisores do SPED proferiu palestra sobre o SPED e NF-e, no dia 23 de agosto, na Associação Brasileira das Companhias Abertas (ABRASCA), em São Paulo – SP. O arquivo contendo a apresentação poderá ser baixada no sítio da Associação (www.abrasca.org.br) ou no item “download” deste sítio.

133 VALOR ECONÔMICO - LEGISLAÇÃO & TRIBUTOS. Empresas reduzem gastos com uso de notas fiscais eletrônicas. São Paulo. Jornalista Leonardo Morato, publicado no dia 23.08.07.

ainda há uma falta de consenso entre os estados em função da guerra fiscal. Exemplo disso é o Estado do Paraná que declarou em 2006, e até meados de fevereiro de 2007, não ter intenção de aderir ao projeto NF-e, embora, posteriormente, tenha refletido melhor e regredido na sua posição.

Vale lembrar, ainda, que atualmente tem sido realizado trabalho de grande mérito pelo Ministério da Fazenda, juntamente com governos regionais, para alcançar um consenso sobre a NF-e até setembro de 2007, mas este ainda é insuficiente, tendo em vista, a existência de pressão política da Receita Federal e de alguns Estados. O Projeto em 2005 era veiculado como infalível. A Polícia Federal informou em 2006, que inexiste projeto eletrônico infalível.

Na verdade o BNDES e BID foram chamados para financiar infra-estruturas tecnológicas para atender as exigências do Projeto. (governo e empresas), cujo valor estimado fora de 600 milhões de dólares divididos de forma igualitária entre governo e empresas.

É translúcido que a estratégia de implantação é Nacional, assim, espera-se que contribuintes, voluntariamente e gradualmente, se interessem por se tornarem “emissores da Nota Fiscal Eletrônica”. Entretanto, projeções e pesquisas realizadas acerca do assunto, revelam a insatisfação das empresas. Algumas, em parte, fundamentadas no fato da Secretaria da Fazenda de São Paulo, atualmente, ter declarado no corpo do RICMS/SP, que poderá futuramente estabelecer a obrigatoriedade da emissão de Nota Fiscal Eletrônica - NF-e - por meio dos seguintes critérios (...): I - valor da receita bruta dos contribuintes; II - valor das operações e prestações; III - tipos de operações praticadas; IV - código de atividade econômica exercida.

Em suma, as maiores preocupações e dúvidas dos contribuintes estão nos quesitos: segurança, multas, capacidade da SRF para prover armazenamento, envio e resposta. Resta saber se estas poderão ser superadas para que seja possível a aplicação efetiva e, conseqüente, obtenção das vantagens oriundas da utilização da NF-e;

3.1 - Os crimes tributários praticados por meio de sofisticadas tecnologias

Como visto, está em pauta a discussão sobre a NF-e, implementada, pelo CONFAZ com apoio da Receita Federal com o objetivo de substituir as tradicionais notas fiscais impressas e demais procedimentos acessórios para a entrega de informações ao Fisco. Cada vez mais, são comuns as falhas nos programas e procedimentos eletrônicos, levando muitas vezes a fiscalização a erro. Se além dos meios puramente eletrônicos entendemos que nesta fase inicial o contribuinte deve ter o direito de contar com meios de provas adicionais, alem do meio eletrônico. Caso contrário, por ausência de provas eletrônicas, em função de problemas sistêmicos do novo sistema poderá ser condenado.

Para ilustrar, é interessante mencionar que existe um trabalho doutrinário[134]; que trata de erro ocasionado por programa de computador, o qual teria gerado informações fiscais erradas do Contribuinte, durante o procedimento de fiscalização, de tal sorte, culminou na lavratura do auto de infração e imposição de multa. O Contribuinte em sua defesa argumentou em síntese que toda informação gerada estava incorreta pelo conjunto de componentes lógicos de seus computadores e sistema de processamento de dados, bem como, o programa e a rotina do conjunto de instruções que controlam o funcionamento de seus computadores agiram de forma incorreta. Ou seja, argumentou-se falha no suporte lógico na operação do programa.

Posteriormente, em função do ocorrido, o mesmo Contribuinte, requereu prazo para apresentar a Fiscalização elementos que pudessem comprovar de forma cabal o cumprimento da obrigação principal e acessória e teve êxito. Em um segundo momento, a fiscalização diligenciou novamente na sede do contribuinte e colheu provas tradicionais.

---

[134] Trata-se de trabalho que foi apresentado por contribuinte em sua defesa administrativa junto ao Egrégio Tribunal de Impostos e Taxas da Secretaria dos Negócios da Fazenda do Estado de São Paulo. O Pesquisador atualmente milita como Juiz da Corte Administrativa Fiscal.

Vamos imaginar que diante de uma falha ocasionada por efeitos desconhecidos, o Contribuinte não tenha provas materiais suficientes, uma vez que extinto o documento fiscal tradicional e todo o sistema de escrituração fiscal. Mas pergunta-se, quem teria esse interesse?

As próprias empresas sonegadoras poderão forjar invasões com o intuito de causarem tumulto processual e anulação de processos por falta de provas. Com as notas fiscais e escrituração toda feita via Internet prevemos o mesmo perigo do cibercrime ao Estado e Contribuintes, uma vez que sua especialidade destas facções é quebrar códigos e cometer fraudes.

Especialistas explicam "grampo" de Internet[135], visando à clonagem de notas fiscais eletrônicas é tão possível quanto o telefônico, bastando para tanto, possuir tecnologia para tal o que não é muito difícil. No caso das notas fiscais eletrônicas onde o usuário tem que aguardar a autorização da SEFAZ para circular com a mercadoria deve-se ter cautela especial com "*Mail Bomb*" que visa inundar um computador com mensagens eletrônicas com fluxo contínuo de mensagens visando deter o recebimento de mensagens importantes.

O "*smurf*" é outro tipo de ataque de negação de serviço. Os "*Sniffers*" são úteis para gerenciamento de redes. Contudo nas mãos de criminosos, permitem furtar senhas que ligam o contribuinte a SEFAZ, além de apanhar outras informações. Infelizmente o aspecto segurança sempre fica em segundo plano, pois é um dos empecilhos evolução do projeto com vistas a rápida disseminação da nova tecnologia. Vejam-se as empresas com a tecnologia "*WI-FI*". Para as grandes corporações nasceram com uma demanda crescente de praticidade, velocidade e facilidade. O sistema emite sinais em ondas de rádio em um raio de 300 metros que não são barrados por paredes, possibilitando assim que um atacante capte o sinal mesmo estando fora da empresa, assim o invasor recebe o sinal da rede e fica lendo os pacotes de dados que são trocados entre os computadores, sabendo tudo que se passa. Em todos os casos citados, em que

---

135 Conforme o especialista consultado nada data de 20 de setembro de 2.008, Giovanni Casagrande da empresa Central de Domínio: www.centraldedominio.com.br , sobre as potenciais vulnerabilidades do projeto Nota Fiscal Eletrônica.

pesem as opiniões em contrário, qualquer crime por meio eletrônico bem sucedido, o "*cracker*" se beneficiará do anonimato, e das penas brandas.

À conta do que se expôs, torna-se imperiosa a necessidade de que se aprofundem os estudos sobre as garantias contra perdas e invasões dos contribuintes e preservação de sua presunção de boa fé.

O que se pretende demonstrar com esta pesquisa é que o Brasil ao lançar novos projetos sofre do que chamamos de "teoria dos projetos perfeitos e invioláveis".

Vamos lembrar que em 1996 surgiam os equipamentos de emissão de cupom fiscal e com eles a idéia de que era o fim das fraudes fiscais no varejo. Passados cerca de doze anos viu-se que tais equipamentos não foram capazes de conter ou diminuir as fraudes no varejo. O mesmo ocorre com a nota fiscal eletrônica que nasce com a promessa de diminuir as fraudes e combater a sonegação fiscal.

Como dito o Brasil não tem boas experiências com o lançamento de equipamentos de controle tecnológico, não só as polêmicas em torno do emissor de cupom fiscal – ECF[136], temos ainda a Adulteração das Urnas Eletrônicas - denunciado em 2003, por professores universitários; Fraude no Painel do Senado conforme Relatório da Unicamp (2.001); e alguns pesquisadores relatam quanto fracassoda criptografia[137].

Para o caso de fraudes praticadas com o uso do Emissor de Cupom Fiscal temos um exemplo claro de crime tributário praticado com o uso de tecnologia e sem o emprego da Internet. Em operações realizadas pela

---

[136] As informações colhidas nesta pesquisa relacionadas ao equipamento de emissão de cupom fiscal, os chamados ECFs, foram colhidas junto a Diretoria e Presidência da Associação Brasileira da Indústria de Formulários, Documentos e Gerenciamento da Informação-ABRAFORM.

[137] Rezende, Pedro Antonio Dourado de Rezende. Professor Doutor do Depto. de Ciência da Computação, Universidade de Brasília 7 de Outubro de 2003. Privacidade e Riscos num mundo de chaves públicas. Relatório sobre o tema "Privacidade e Responsabilidades na Infra-estrutura de Chaves Públicas ICP-BR",I Fórum sobre Segurança, Privacidade e Certificação Digital ITI -Casa Civil da Presidência da República. Acesso dia 7 de outubro de 2008. Fonte: http://www.cic.unb.br/docentes/pedro/trabs/forumiti.htm,acessado em maio 2008.

Fiscalização no Estado de São[138] Paulo, verificou-se que diversas redes varejistas se utilizavam de Equipamentos de Cupom Fiscal que são controlados remotamente via cabo.

Esta alteração remota tinha o seguinte procedimento: no momento da compra o consumidor recebia em cupom fiscal como valor real da compra. Através do mencionado controle, é armazenado um valor cerca de 70% inferior ao valor real da compra na memória fiscal do equipamento. Esta alteração foi possível em função deste controle eletrônico à distância.

A memória fiscal ao ser verificada pela fiscalização não detecta o valor real da compra e o imposto passa a incidir sobre ma base de cálculo 70% inferior em cada operação. O crime da era da tecnologia tem sido descoberto uma vez que a equipe de fiscalização verifica que os consumidores saem do balcão portando um pedaço de papel comum que por vezes é jogado fora. Ou seja, a prova colhida[139] pelo fisco no chão do estabelecimento varejista e posteriormente apensado ao auto de infração e como prova em processo crime.

O cupom fiscal é impresso em papel térmico, normalmente de cor amarela, que deveria durar pelo menos 5 anos em condições normais de temperatura e pressão. Ocorre que, em menos de 3 meses, esse documento fiscal falso, em alguns casos, simplesmente apaga-se, sendo impossível fazer a leitura dele.

Algumas lojas ainda tiram cópia para entregar ao cliente; outras, apenas alertam-no; mas, a maioria sequer avisa ao consumidor, o qual porventura pode ter algum problema com o produto e o documento de compra, já apagado, não provar nada.

---

[138] Conforme pesquisas realizadas nos processos no Tribunal de Impostos e Taxas de São Paulo sem divulgar o nome de contribuintes ou dados que possam comprometer a quebra do sigilo fiscal.

[139] Verifica-se ainda que a fiscalização pauta suas ações com base nas diferenças encontradas nas declarações informadas pelas Administradoras de Cartões: além do pagamento atualizado do imposto não recolhido, o contribuinte será apenado com multa equivalente à 80% do valor corrigido.

Esta artimanha da era digital tem facilitado à sonegação de imposto (ICMS), exime a responsabilidade do comerciante diante de um possível defeito em mercadoria vendida. Lesam-se a Fazenda e, na outra ponta, o consumidor.

Em outros casos é realizada uma fraude no software de comunicação entre o ECF e a impressora, que impede que o cupom seja impresso na hora da venda embora possibilite o registro da venda do produto no computador da empresa.

O bloqueio é feito remotamente pelo funcionário, acionando uma determinada "tecla". [140]

No mês de maio e início de junho de 2008, os discos rígidos dos computadores de 71 dos 145 estabelecimentos visitados foram copiados para serem analisados pelo setor de Inteligência Fiscal da secretaria. Será verificada se há nesses discos um programa que bloqueia a impressão do cupom fiscal. [141]

A legislação tributária proíbe o desenvolvimento de programas que bloqueiam o ECF. Ela prevê ainda o princípio da concomitância, isto é, o cupom fiscal deve ser impresso assim que digitado ou capturado (por "scanner") o código do produto vendido.

Por isso, o equipamento não pode armazenar em sua memória cada um dos itens da venda para só imprimir o cupom fiscal após o registro do último.

Outra irregularidade fiscalizada na operação foi o uso de ECF não autorizado ou não re-lacrado. A re-lacração é determinada pela secretariada, depois que foram detectadas alterações no software básico do equipamento. O programa original de controle do ECF é substituído por um fraudulento.

Como visto a fraude é aplicada diretamente no software do equipamento de Cupom Fiscal. A Inteligência Fiscal, em tese, relata que conseguiu simular o

---

[140] Conforme pesquisas o fisco paulista orienta os comerciantes a substituírem espontaneamente os programas aplicativos irregulares por outros que estejam em conformidade com a legislação tributária para evitar que a fiscalização comprove a fraude. Se a fraude for comprovada, será aplicada multa de R$ 7.440,00 para cada cópia do programa em utilização no estabelecimento. A empresa que desenvolveu o software também será multada no mesmo valor.

[141] Conforme informações colhidas na Secretaria da Fazendo do Estado de São Paulo.

sistema de fraude dos contribuintes, nos computadores da Secretaria da Fazenda do Estado de São Paulo. Esta técnica é conhecida como “virtualização”. Através dela, inteligência fiscal informa[142] que garantirá a verificação precisa das irregularidades, com provas mais conclusivas para subsidiar autos de infração.

A Inteligência Fiscal conseguiu processar estes dados capturados em computadores de duas redes varejistas que foram fiscalizadas.

Entendo que as formas de coleta de provas e a legislação estão ficando cada vez mais técnicas e os profissionais da área jurídica devem estar preparados para impugnar provas de cunho tecnológico colhidas pelos agentes da fiscalização.

Mutatis mutandis, o que deve ser avaliado é que não existe uma legislação acompanhada de um manual de procedimentos técnicos que venham a servir de espinha dorsal a amparar e dar legitimidade as ações da Fazenda Estadual. Os procedimentos técnicos adotados pelo fisco são de caráter unilateral dificultando a defesa de contribuintes. Nesta batalha tecnológica[143] a fiscalização, não é vedada a produção da prova com uso de tecnologia. Ao contribuinte deve ser dada a oportunidade de conhecer previamente a forma e os procedimentos de colheita da prova técnica. Desta forma, teremos um processo tributário mais transparente e de forma a garantir o cumprimento do princípio do contraditório de da ampla defesa.

Para a implantação da Nota Fiscal Eletrônica deve-se minimizar o elevado custo, bem como, amenizar os riscos da certificação digital, acrescida da falha no armazenamento. Este conjunto põe em risco a viabilidade do Projeto NF-e. Nesta fase de adaptações e testes, o Contribuinte deve manter em seu poder os meios de prova tradicionais.

---

142 Fonte: Informativo CAT nº. 90 de setembro de 2008. Publicação mensal interna do Conselho Superior da Coordenadoria da Administração Tributária da Secretaria da Fazenda do Estado de São Paulo.

143 No mês de maio e julho de 2008, os auditores do fisco paulista encontraram 27 emissores de cupom fiscal sem autorização de uso, 11 não re-lacrados e 21 com uso cessado não comunicado ao Fisco. Foram ainda apreendidas 18 cópias em CD do programa aplicativo que faz o equipamento funcionar. A Fazenda aplicou 25 multas, cada uma no valor de R$ 2.232,00.

Por outro lado, outro benefício esperado e divulgado a sociedade, diz respeito à “Redução do consumo de papel, com impacto ecológico” “favorável”. Contudo, por prazo indeterminado deverá o contribuinte, para facilitar o controle, o trânsito da mercadoria com uma NF-e autorizada, deverá ser feito acompanhado de um documento auxiliar, impresso em papel comum, intitulado DANF-e (documento auxiliar da NF-e).

O projeto da NF-e é muito oportuno, mas a administração pública, na qualidade suplementar de controle e suporte a fiscalização. Por seu lado, deve o contribuinte estar preparado para as fraudes virtuais e continências inesperadas. A Legislação não prevê prazo para os atos de comunicação entre o Fisco e Contribuinte. Ou seja, não existe um prazo estipulado a Administração Tributaria para oferecer a resposta de aceite ou de recusa a Nota Fiscal Eletrônica em função de sua forte dependência do sistema de comunicação pela Internet.

Até que a legislação esteja bem definida, o Contribuinte terá de armazenar suas notas fiscais como sistema paralelo de segurança. Enquanto a obrigação quanto à segurança e autenticidade não for compartilhada com a SRF, não se poderá exigir a utilização deste documento fiscal eletrônico, imputando exclusivamente ao contribuinte a obrigação arcar com elevados custos de implantação, além de ter o ônus de provar a legalidade sistêmica deste.

Não estamos falando mais em “comércio eletrônico”, mas na relevância das informações técnicas entre Fisco e Contribuinte e a delimitação de responsabilidades. Ou seja, o projeto carece de validade jurídica, uma vez que esbarra nas relações de competência privativa da União para Legislar sobre o temário de forma sistêmica - relações de comunicação.

Dentro deste cenário, percebe-se que o Contribuinte, o “Estado/Cidadão/ Arrecadador” poderá “pagar a conta”.

3.2 – Sobre a Segurança na Confecção e Emissão de Notas Fiscais

Sobre a necessidade da manutenção do papel para emissão e impressão de documentos fiscais é oportuna a análise da resposta da Diretoria da Policia Federal quando se manifestou sobre o Convênio 10/05[144], aprovado pelo Conselho Nacional Fazendária.

O Chefe da Seção de Documentoscopia do Instituto de Criminalística da Polícia Federal (INC), Carlos Maurício de Abreu, enfatiza independente da escolha do papel a ser utilizado para a Fabricação de documentos fiscais o mesmo, deve ser acrescido de tarja calcográfica bem elaborada, contendo o brasão correspondente, imagem latente, microtextos positivos e negativos, desenhos de fundo impressos em *offset* com pelo menos duas tintas apagáveis com irisamento e fundo anticopiativo, numeração tipográfica com tinta penetrante e código de barras repetindo a mesma numeração.

Ou seja, a Informação de n° 071/2005 subscrito também pela Diretoria da Polícia Federal, deixou bem claro que deveria ser unido o papel ao sistema de impressão.

Soube-se que há mais ou menos dois anos, teve início no Órgão de apoio técnico ao CONFAZ, COTEPE e G3 uma proposta de idealização de uma alteração aos citados Convênios 58/95, 131/95, 55/96 e 111/01, que tratam da Impressão calcográfica[145] de Nota Fiscal em folha solta, mediante decorrente de um pleito formalizado pela empresa , tradicionalmente detentora de monopólio na fabricação doméstica de papel contendo “marca-d'água” fabricado pelo processo de Fabricação exclusivo denominado “*mould-made*”.

O novo Convênio, 10/05 em tese, permite uso apenas à “marca d’água” como dispositivo de segurança para ser utilizado como nota fiscal.

---

[144] Este convênio trataria em sua redação original da emissão de documentos fiscais com o elemento de segurança marca d água. Ocorre que o Instituto Nacional de Criminalística entendeu que a esta marca poderia ser falsificada em larga escala e que os documentos fiscais para impressão simultânea de documentos fiscais deveria

[145] Impressão Calcográfica é aquela que temos no dinheiro que se utiliza também do Papel moeda com a utilização da marca d água como elemento de segurança.

A ABRAFORM, responsável pela emissão de parecer técnico, atestando a capacidade do estabelecimento gráfico para confecção de documentos fiscais em formulário contínuo ou plano contestou administrativamente em vários órgãos a validade do novo Convênio. Segundo a entidade, esta sendo levado o alerta às autoridades de todo Brasil advertindo que a fabricação do insumo (papel com marca d´água) isoladamente como “Nota Fiscal”, beneficia a sonegação fiscal e Roubo de cargas em todo o Brasil.

No estudo apresentado pela entidade foi demonstrado o risco ao processo de arrecadação de todas as unidades da Federação e da União pela utilização do papel com marca d água como elemento de segurança. O Relato histórico e comparativo a nota fiscal eletrônica é pertinente, uma vez que este novo projeto prevê a impressão do Documento Auxiliar da Nota Fiscal Eletrônica em um documento em branco sem a adição de nenhum elemento intrínseco de segurança no Documento Auxiliar da Nota Fiscal Eletrônica.

Por seu lado a Diretoria da Polícia Federal emitiu Parecer Técnico atestando que o papel com "marca d´água" pode ser simulado por meio de uso de tintas ou produtos químicos.

Hoje, as notas fiscais em folhas soltas em impressora laser são emitidas de acordo com Convênio 58/95, e posteriores modificações que estabelece rígidas normas para o formulário em questão. O mesmo passou a ser denominado pela legislação como “formulário de segurança", que contém impressão de tintas e efeitos especiais que garantem alto grau de controle para as instituições fiscais. Ou seja, estas notas fiscais contêm diversos elementos e meios de segurança intrínseca.

A interpretação errônea do Parecer Técnico da Polícia Federal demonstrava que o insumo isolado, o papel com “marca d’água”, em tese poderia ser mais seguro e barato além de ser usado como meio de resolver todos os problemas de segurança de documento tributários acessórios, como também ofereceria melhoria da segurança do sistema fiscal e de arrecadação como um todo.

Contudo, o Instituto Nacional de Criminalística esclareceu que, no parecer, não foram analisados o sistema de arrecadação, ou o sistema de segurança gráfica, ou implicações relacionadas ao sistema de arrecadação. Menciona a Polícia Federal que a utilização da "marca d´água" é viável no sistema de impressão caso "a Fiscalização estiver treinada para reconhecê-la". A informação do o Instituto Nacional de Criminalística, subscrito pela Diretoria da Policia Federal, alerta que o ideal seria a conjugação do insumo e a Impressão calcográfica. Ou seja, a adição de mais de uma forma de segurança intrínseca.

Note-se que a Nota Fiscal Eletrônica não tem como acessório quaisquer documentos de ordem suplementar com acréscimo de sistema de segurança intrínseca. O Projeto se apóia totalmente na forma de controle via internet já descrita. Durante esta pesquisa procuramos apontar que a forma de controle puramente eletrônica historicamente esta sujeita a falhas e a astúcia dos fraudadores.

Ao contrário do que muitas pessoas imaginam os cheques não foram substituídos pelas transações eletrônicas[146], uma vez que dotados de um duplo controle. Ou seja, do controle eletrônico e formas de segurança intrínseca do documento capaz de identificar o usuário.

Defendemos que a nota fiscal eletrônica, nesta primeira fase, para ser um documento capaz de combater a sonegação fiscal deve se pautar no controle eletrônico e também nas formas de identificação e de autenticidade de documentos de primeiro nível[147].

Na hipótese de fraudes fiscais nas Notas Fiscais Eletrônicas diversas perícias técnicas de informática serão feitas com grande complexidade técnica. A análise de segurança e idoneidade que dependa de exames de laboratórios

---

[146] Conforme informações da ABRAFORM que congrega como seus associados as cinco maiores empresas Brasileiras de Segurança Gráfica, Fabricantes e impressores dos cheques de instituições financeiras.

[147] Elemento de segurança de primeiro nível de documentos é aquele que possibilite a documentos representativos de valores como o dinheiro e notas fiscais serem identificados pela visão ou pelo tato. Pela visão temos o exemplo da marca d água, pelo tato temos à tarja calcográfica áspera. Ambos os elementos estão presentes no dinheiro que circulam ao redor do mundo.

técnicos são válida para investigação de crimes e criminosos não para o uso corrente transacional como se espera do trânsito de documentos fiscais em larga escala, como os da nota fiscal eletrônica.

Veja que quando o documento fiscal eletrônico for adulterado, não existirá outro documento de segurança acrescido de outros elementos de intrínsecos de segurança capaz de atestar se aquela transação eletrônica corresponde ao fato gerador de operação tributária ou não.

A segurança do sistema de arrecadação está pautada em uma série de atividades onde a segurança do documento fiscal ou mesmo o impresso de segurança fiscal são apenas um dos elementos.

O Convênio que trata da Nota Fiscal Eletrônica favorece a indústria de tecnologia. Contudo este novo processo de revolução informacional tributária contraria todas as tendências de segurança e Jurídicas Mundiais, que tratam e direcionam os sistemas de tributação para duplos e até de triplos sistemas de segurança na transação de documentos que representativos de informações sensíveis, de grande valor agregado, como é o caso das notas fiscais. O Estado no trato do dinheiro público não deve e não pode correr riscos desnecessários.

A era tecnológica e informacional pode ser vista também como um caminho ao monopólio da tecnologia, capaz de gerar desemprego em massa, com o respectivo aumento do preço final das notas e documentos fiscais, auxilia a venda casada de suprimentos tecnológicos com impactos ambientais, a toda a cadeia.

Na forma como idealizado o projeto da Nota Fiscal Eletrônica, pode acontecer o mesmo que ocorreu com o projeto do ECF e como visto, pode auxilia em um processo de circulação de cargas roubadas e o derrame de notas fiscais frias no mercado, atingindo diretamente o ESTADO CIDADÃO ARRECADADOR o bem maior a ser tutelado pelo estado neste processo.

Neste trabalho procura-se demonstrar a ação das quadrilhas e facções criminosas que tem como característica a mutação e evolução de seu *modus operandi*.

Por outro lado a era informacional a Nota Fiscal Eletrônica pode ser criada para que possamos avançar rumo a criação de novas formas de reciclagem de máquinas e equipamentos, com a respectiva redução do impacto ambiental. No campo da geração de empregos, deve ser um ponto fulcral para a geração de novos postos de trabalho. É o que se espera. A simples combinação de preço entre comprador e vendedor será capaz de burlar a fiscalização on-line.

3.3 – Múltiplas visões sobre a Nota Fiscal Eletrônica e o Sistema Público de Escrituração Digital.

Como visto merecem especial atenção as mudanças atuais no cenário econômico decorrentes do rápido crescimento do comércio eletrônico, como também a implementação do trânsito de documentos públicos pela rede mundial de computadores no Brasil.

Deve-se meditar que para que o Estado possa implementar o projeto de utilização da Nota Fiscal Eletrônica e do Sistema Público de Escrituração Digital, é necessário haver elevada disponibilidade de sistema – on-line, 24 horas, sete dias por semana. Ou seja, o sistema Fazendário Nacional e da Secretaria da Receita Federal (SRF) têm que adotar um conjunto de características especiais que estejam sempre em operação.

A Administração Tributária deve possuir equipe técnica de plantão, vinte quatro horas por dia sete dias por semana. Por seu lado, as empresas que emitem grande quantidade de documentos fiscais deverão se preparar para processos de contingência. O ferramental técnico esta sendo preparado, e exige um maciço investimento em segurança e ferramental técnicos e equipes especializadas.

Cabe mencionar que atualmente nem os bancos possuem um sistema de *back-up*[148] ou de disponibilidade de serviço 24 horas. Não porque os bancos não

---

148 Conforme Giovanni Casagrande Diretor da Central de Domínio

possam tê-los, mas porque o custo é demasiadamente elevado, o que sobrecarrega as instituições financeiras (o que pode ser comprovado ao se tentar acessar um banco via internet às 3 horas da manhã). Além disso, na hipótese de falhas, a Fazenda e as empresas devem ter uma máquina "*Hot-Swap*"**,** ou seja, quando uma máquina falhar, for invadida, ou vierem às contingências, os dados devem ser transferidos para outra máquina.

Diversos segmentos da sociedade[149] informam que nem todos os pontos do projeto da NF-e estão totalmente esclarecidos, apesar de haver um compromisso das Secretarias de Fazenda (SEFAZ) e da Receita Federal de que toda a infra-estrutura estará preparada para acomodar o alto volume de dados gerados por este projeto.

Segundo estudos da ABRAFORM as empresas precisarão fazer um alto investimento para adequar seu ambiente de tecnologia da informação (TI) às necessidades do projeto. A ABRAFORM indaga que mesmo com o Estado fornecendo o sistema de gestão para as médias e pequenas empresas teme pelo suporte tecnológico necessário ao funcionamento da infra-estrutura. Além disso, ainda não está claro se os outros Estados adotarão os mesmos procedimentos. Complementando tal colocação, a adequação das pequenas e médias empresas precisará de investimento em infra-estrutura ou suporte e manutenção da base de *software* e *hardware*.

A Fazenda do Estado de São Paulo afirmou em 2006 que realizou um investimento em infra-estrutura de R$ 15 milhões. Trata-se de um baixo valor para uma cadeia recíproca de troca de informações de documentos públicos. Os crimes cibernéticos pó os cibercrimes são uma das ameaças ao projeto.

Cibercrimes é o termo pelo qual são conhecidos os crimes praticados com o uso da internet plugados através de equipamentos de informática. Trata-se de uma espécie de crimes de alta tecnologia, sendo que este é o gênero e aquele a espécie. Vimos que o uso de outras tecnologias sobre os quais já falamos na

---

[149] Conforme a Associação Brasileira das Indústrias de Formulários, Documentos e Gerenciamento da Informação –ABRAFORM.

primeira seção desta pesquisa. Tais crimes têm evoluído na sua forma de praticar, como evoluem os sistemas e equipamentos de informática. O impacto causado por este processo tem sido discutido em conferências, simpósios congressos e palestras no mundo todo.

Olavor José Anchieschi Gomes define: c*racking* é a atividade exercida pelo c*racker* – esta palavra é utilizada para melhor definir o modo de atuar deste *ciber-espião* e significa romper, quebrar, danificar, entre outras ações. A partir deste contexto pode-se definir este personagem – o *cracker* - como alguém que emprega sua inteligência para o crime e utiliza suas horas de estudo para criar ferramentas a fim de comprometer a segurança de redes governamentais e privadas.

A Polícia Federal recomenda que os pais estejam atentos, pois jovens com alto grau de conhecimento em linguagens de programação e sistemas operacionais podem ser alvos de organizações criminosas. As agências do crime estão recrutando ou seqüestrando estes adolescentes. As atividades destas organizações incluem, entre outras, acessos não autorizados, danos a todo e qualquer tipo de sistema, espionagem e clonagem de celulares e de páginas da *web*. Geralmente, essas ações são tidas como ilegais, mas são muito sofisticadas e atinge nocivamente toda a sociedade. Estudiosos argumentam que não há previsão específica para tais delitos nem leis e procedimentos que permitam à Polícia e ao Ministério Público serem mais efetivos nas investigações.

Ajunte-se a isso a informação de que a demanda por investigadores nesse setor é pequena.

Existem, atualmente, na Internet, diversos grupos formados por estes *crackers* especializados na troca de códigos e procedimentos para clonagem de telefones celulares, para a captura de informações, desbloqueio de telefones furtados, alterando o serial e senhas dos referidos aparelhos, entre outros procedimentos. A lei, em tese, não proíbe tal conduta, porque estamos em fase preparatória ou de criação de ferramentas para cometer o delito. Obviamente, o Auditor Fiscal de Rendas e a Polícia deveriam estar treinados, como um todo,

para avaliar esses “atos de comunicação” que normalmente se passam em código em uma linguagem que apenas o criminoso compreende.

O chefe do Serviço de Perícias em Informática da Polícia Federal, Paulo Quintiliano [150], explica que é muito difícil identificar todas as fraudes. ‘‘Quando o valor do golpe é alto, os bancos denunciam. Não temos como calcular o número de pequenos delitos não relatados pelas instituições’’, diz Quintiliano. Para Amazonas (2004) "Os bancos não têm interesse de comunicar certos roubos para não perder a credibilidade frente aos correntistas e investidores". Como em toda a instituição financeira, os números de perdas com segurança são proporcionais ao investimento. Relatório da IBM em 2006 (RELATÓRIO ... 2006) prevê a evolução do *Cibercrime*[151] tanto em relação a grandes organizações empresariais como em relação a usuários finais. O lucro faz o cibercrime se estabelecer mundialmente[152].

Só no Brasil, os crimes digitais geraram um prejuízo de R$ 300 milhões a bancos e administradoras de cartões de crédito em 2005. Cerca de 150% a mais que no ano anterior quando contabilizou R$ 100 milhões. Em 2006, o valor das perdas esteve em torno de R$ 350 milhões, de acordo com a pesquisa do IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações) empresa especializada em perícias digitais e apuração de crimes e fraudes no mundo cibernético. Na verdade os números podem ter sido muito superiores, contando com o anonimato. Os especialistas não acreditam que haverá muitas mudanças no tipo de fraude, mas que os fraudadores agirão com mais agilidade: " Já não haverá mais necessidade de os criminosos enviarem e-mails massivos para contaminar novas máquinas".

Sobre os pretendidos “benefícios propostos” sobre a NF-e, o líder empresarial Marcos Cunha Ribeiro, foi vice-presidente da ABRAFORM e Diretor da ABIGRAF ocupou por vários anos a Presidência da RRDonely *Moore*, discorre

---

150 Conforme sua palestra durante o ICCyber 2006 (ww.iccyber.org).

151 Disponível:<http://tecnologia.terra.com.br/interna/0,,OI848630-EI4805,00.html> Acesso maio 2008.

152 Disponível: <www.symantec.com/enterprise/threatreport/index.jsp.> 21 março 2006.

sobre o significado da Nota Fiscal, sob vários ângulos de abordagem: os conteúdos formais, os econômicos, os éticos e também os relacionados à criação de valor. Ao final, ele comenta as perspectivas da adoção, em maior escala, das notas fiscais eletrônicas. Este material foi publicado na Revista Marketing Industrial n° 34 - setembro de 2.006 - páginas 54 a 56: “Este movimento não é voluntário. Na proposta atual da Nota Fiscal Eletrônica, o que mais chama a atenção é ver as escolhas de oferta de valor dos agentes de arrecadação, para atrair voluntários do programa piloto e demais empresas que venham a aderir ao processo, depois de finalmente aprovado e suportado pelo aparato regulatório imprescindível, mas até agora inexistente. A oferta de valor é repleta de sofismas ou até do que se poderia chamar de propaganda enganosa. O público alvo são justamente os empresários e executivos das empresas no ambiente do Marketing Industrial e, não nos iludamos, uma grande parcela deles já toma proveito deste processo, nos mesmos argumentos de oferta de valor para alavancar seus negócios, portanto aderindo aos sofismas e/ou enganos; e outros já se entusiasmam e estudam a oportunidade prometida. Se não vejamos alguns destes pontos:

- Argumento de redução de custo ao contribuinte com base na eliminação de documentos fiscais, que usa dados de pesquisa sobre o custo das empresas como percentual do seu faturamento que não refletem os custos dos documentos, mas o custo total de TI na média das empresas internacionais incluindo infra-estrutura, softwares, todos os dados e suas transações internas e externas, inclusive documentos fiscais ou documentos de comunicação com seus clientes em suas atividades de marketing ou reporte transacional. Ocorre que a implementação do piloto está gerando investimentos em TI que podem variar de R$ 300 mil a mais de R$ 2 milhões, sem nenhum retorno financeiro ou operacional senão para as operações que já poderiam ter adotado o processo de Notas Fiscais por impressão simultânea desde 1995, já o

fizeram ou venham a fazer (Menos de 130 empresas em todo o Brasil após 10 anos e por processo voluntário)

- O argumento de cunho ambiental, com a promessa de redução do corte de árvores – o que tem grande impacto na mídia e na opinião pública, dado o conteúdo emocional que o tema recebe e merece. Ocorre que no Brasil o papel utilizado nas Notas Fiscais, bem como o que será utilizado no documento que a irá substituir para o trânsito de mercadorias e bens ou serviços, no novo sistema proposto, é o resultado de uma indústria brasileira constituída por empresas válidas, certificadas pelos órgãos ambientais, que produzem celulose e papel a partir de reflorestamento em áreas de há muitos séculos desmatadas – nas quais o plantio do eucalipto é suportado por intensa atividade de reflorestamento de espécies naturais – desenvolvem técnicas e tecnologias de ponta no *agribusiness* e geram milhares de empregos formais, além de participarem fortemente da atividade de exportação.
- A última oferta de valor a ser apreciada nesta discussão é a mais emocional e exótica, pois permeia todo o ambiente de negócios da área de TI há anos e infelizmente se baseia na percepção de que o empresariado e os executivos das empresas tomam decisões e implementam mudanças de processo pelo impulso e pela emoção no trato de investimentos de automação transacional, mudanças de processos de controles gerenciais e gerenciamento da base de dados, como se tratasse de uma peça de roupa, uma moda de corte de cabelo ou o mesmo impulso presente na compra de um carro novo. O processo novo exige infra-estrutura de TI para transações eletrônicas entre a empresa e os agentes de arrecadação em tempo real, tanto quanto com os seus clientes em moldes semelhantes ao exigido desde 1995 no convênio COTEPE 058/95 e seus subseqüentes até hoje. O sistema proposto certamente leva em conta que, com seus clientes, grande parte dos relacionamentos transacionais do contribuinte já se faz nas infra-estruturas de hoje, conforme o momento de

> atualização tecnológica de cada empresa. Portanto nada de novo, senão o fato concreto de que no processo proposto o agente arrecadador será um interferente direto no processo crítico de faturamento a cada simples emissão de um documento eletrônico, que será a Nota Fiscal Eletrônica, isto mesmo, um a um, caso a caso. Ele irá se inserir no processo crítico da empresa sem convite e sem boas vindas.

Apesar de ver este Projeto com "bons olhos", está clara a percepção de que as administrações fiscais ainda não estão totalmente preparadas para promover de forma isolada a NF-e e o SPED. Prova disso é que problemas de controles simples fazem parte hoje do custo Brasil. Hoje uma empresa multinacional de escol sofre um elevado "peso" operacional como a simples retirada de uma CND. Inclusive, hoje, na AMCHAM, existe um movimento Nacional sobre o tema e tal a gravidade da questão. O Contribuinte demora meses para baixar seu débito, mesmo depois de ter comprovado a caução ou pagamento do tributo.

A conclusão ainda se apóia na recente manifestação de organismos internacionais como OCDE e OMC, que diante das perdas potencias de receitas tributárias resultantes do desenvolvimento do comércio eletrônico sugeriram uma "Política Fiscal Mundial" para a tributação desse tipo de comércio. A amplitude mundial dessa "política fiscal" se faz necessária, uma vez não há mais limite territoriais às operações comerciais em razão dos avanços tecnológicos, tais como a Internet e a virtualidade das transações[153].Essa mesma política fiscal deverá ser implantada em relação ao Cibercrime.

Uma pesquisa conduzida pela IBM aponta que 100% dos usuários temem o *cibercrime* mais que os delitos físicos[154]. Uma outra pesquisa recente, envolvendo duzentos contabilistas, consultores e profissionais da área financeira de pequenas, médias e grandes empresas foi realizada durante uma palestra de

---

153 Revista Pleafisco, Gramado/RS, Edição n° 3 de agosto de 2.006, página 28 e 29.

154 IDG NOW, Autor Fernanda K. Ângelo, Título, Com cibercrime, síndrome do pânico chega ao mundo virtual, data 07/04/2006

um renomado Centro de Estudos em São Paulo. Por curioso, na oportunidade, foi questionado se alguns dos profissionais presentes acreditavam no projeto NF-e, bem como, foi perguntado se as pesquisas de aceitação da Nota Fiscal Eletrônica traduzem a realidade. Todas as duzentas pessoas presentes informaram que não acreditam na NF-e da forma como o projeto esta sendo veiculado na atualidade.

Infelizmente o combate à corrupção no Brasil não costuma ser enumerado entre as missões da administração pública[155], apenas um lado do tema tem sido enfrentado, mas precisamos trilhar todos os caminhos porque a corrupção e a fraude sempre encontram os seus destinos.

3.4 – A Nota Fiscal Eletrônica e o Atual Cenário dos Crimes de Alta Tecnologia.

Como visto o Projeto NF-e cuida da implantação de um modelo nacional de documento fiscal eletrônico que pretende substituir a sistemática atual de emissão do documento fiscal em papel, o qual, em tese, equivocadamente [156] pretende obter a validade jurídica[157] da Nota Fiscal Eletrônica pela assinatura digital do remetente.

---

155 Este foi o comentário do Agente Fiscal de Rendas da Secretaria da Fazenda do Estado de São Paulo e jornalista especializado em Políticas Públicas pela Faculdade Latin-Americana de Ciências Sociais de Buenos Aires, Hideyo Saito, recomendo o artigo publicado na revista Plenafisco pág 26.

156 Equivocadamente porque todo o sistema de Hardware e de Software precisaria ser auditado. É um sistema de múltiplas funções para emissão da Nota Fiscal. A mercadoria é remetida juntamente com um documento Fiscal desprovido de validade jurídica chamado DANF-e. Trata-se de documento acessório da Nota Fiscal Eletrônica. Os problemas jurídicos e de prova relativos ao uso de assinaturas digitais estão presentes em diversas áreas do Direito. In Casu, aplica-se a regra do Código Civil que determina a perda da Validade Jurídica do documento eletrônico nos casos de impugnação a favor do Contribuinte.

157 Validade jurídica de que trata este tema tem o negócio jurídico, conforme dispõe o artigo 104 do Código Civil: "A validade do negócio jurídico requer I-Agente capaz; II -Objeto lícito, possível, determinado ou determinável; III Forma prescrita ou não defesa em lei. A validade jurídica aqui descrita é típica para validar atos das relações privadas. A Nota Fiscal é documento público e precisa ter fé pública fazendo prova plena. O acesso à Internet se dá através da prestação de dois serviços distintos. Cabe à operadora realizar o transporte do sinal, viabilizando a comunicação, e ao provedor proporcionar a conexão do usuário à Rede. O próprio Código Tributário Nacional, em o art. 110, dispõe que a lei tributária não pode alterar a definição,

Nas palavras de Aires José Rover (2004, p. 238)

> Agora, além das discussões sobre comércio eletrônico, aparece o tema do ”governo eletrônico”, que nesse primeiro momento, será entendido em linhas gerais como a utilização, por parte do setor público, das novas tecnologias de informação e comunicação, em especial a Internet, para prestação de melhores serviços, disseminação de informações, controle as contas públicas, redução de custos administrativos e ampliação das possibilidades de participação dos cidadãos na gestão pública.

Trata-se de um projeto “inovador” [158] que visa gerar maior controle e cruzamento de dados das operações do contribuinte, bem como objetiva simplificar suas obrigações acessórias, permitindo o ineficiente monitoramento, em tempo real, das operações comerciais pelo Fisco. O Projeto da Nota Fiscal Eletrônica carece de infra-estrutura.

O Projeto NF-e, da Administração Fazendária, desenvolvido em conjunto com a Secretária da Receita Federal, está na sua segunda versão, em fase de teste.

---

conteúdo, alcance dos institutos, conceitos e formas de direito privado, pois estará adentrando área de competência de Lei Complementar. Cabe lembrar a regra dos artigos 222, 223, em especial o artigo 225 do Código Civil que determina que as Reproduções eletrônicas de fatos de coisas que fazem prova plena destes, se à parte contra quem forem exibidos, não lhes impugnar o conteúdo. Ou seja, a fiscalização poderá fazer prova face ao Contribuinte, até o momento em que for impugnado o documento. Provada a hipossuficiência do Contribuinte, na hipótese de atos criminosos cometidos por terceiros, deve o Código Tributário Nacional regular estas relações complexas afetas a comunicações e trânsito de documentos públicos. O legislador supremo não cuidou de atingir o conteúdo da comunicação, mas o serviço que a permite, ou seja, o veículo, que, com intuito econômico, objetivo é viabilizar a comunicação entre o fisco e o contribuinte e não se trata da comunicação de massa (social) ou a comunicação privada ou particular. Mas aqui estamos a desvendar qual seria o correto tratamento legislativo para conferir a validade jurídica pretendida para a circulação em larga escala destes documentos públicos. Neste caso o serviço deve estar vinculado ao segmento de comunicação, embora não represente serviço de telecomunicação. Mas como se auferir validade jurídica se “a realidade das redes brasileiras, sem praticamente nenhuma proteção por criptografia, oferece um campo enorme de oportunidades nos segmentos privado e governamental. As redes com criptografia no Brasil ainda utilizam o padrão IPSec/VPN de baixo rendimento e configuração e manutenção onerosas. Para informações completas sobre a linha *SafeNet High-Speed Encryption visite:* http://www.safenet-inc.com/products/encryptors/index.asp.

158 As pesquisas relativas ao projeto-piloto da Nota Fiscal Eletrônica - realizado mediante convênio entre a Secretaria da Receita Federal e Secretaria da Fazenda de vários Estados, dentre eles São Paulo - não representam as reais dimensões do processo de arrecadação de tributos, especialmente se considerados o elevado número de impostos, taxas e área continental do Brasil. Os equívocos começam no modelo adotado, baseado no do Chile, país cujo sistema tributário e geografia são muito diferentes aos do Brasil.

O presente estudo visa demonstrar que o Projeto (NF-e) já nasce em muitos aspectos desamparado, em meio a um crescente sentimento de pânico virtual, o que prenuncia que num segundo momento, quando de sua implantação, vai crescer em sustentação, em meio a códigos brutalmente maliciosos e à esperteza e disfarces de organizações criminosas altamente especializadas no furto qualificado de informações confidenciais. A identidade virtual dos brasileiros corre perigo e o Brasil tem sido consagrado com o título de um dos países mais inseguros do mundo. A Administração Fazendária Nacional deve estar ciente de que seus projetos irão conviver no mesmo ambiente onde reside um vertiginoso e alarmante crescimento de cibercrimes, desde o início do século XXI. Neste contexto a troca de informações entre diversos organismos de Governo e a iniciativa privada é muito importante. A especialidade destes criminosos é não deixar rastros, dificultando a detecção da fraude e criando novos desafios ao estabelecimento de políticas efetivas de gestão de risco para o Encontro Nacional de Coordenadores e Administradores Tributários – ENCAT. Tais fatos são de grande preocupação, não só por parte do contribuinte, mas também diante do temor da população, uma vez que persiste, até então, o anonimato e a sensação de impunidade, como fatores de estímulo dos criminosos, dada à ineficácia legislativa e particularidades do Estado Brasileiro. [159]

As experiências dos Bancos[160] servem como pertinente reflexão[161], alerta e método comparativo. A NF-e trata do trânsito em larga escala de documento

---

159 REBEHY, Marco Wadhy. Gazeta Mercantil, 20 de setembro de 2005.

160 De acordo com estimativas da Febraban de 2.006, as instituições aplicam cerca de US$ 1,2 bilhão por ano no sistema para melhorar a segurança dos clientes, sejam usuários de cartões ou Internet Banking. Cabe notar que os investimentos devem ser proporcionais a possibilidade de perda destas instituições. Nesta vereda, temos um número real para meditar. Vulnerabilidades Web: Nos últimos seis meses de 2005, 69% de todas as vulnerabilidades relatadas foram encontradas em aplicativos Web, um aumento de mais de 15% em relação ao último período analisado. “Roubo de informações” o correto é dizer furto de informações códigos projetados para roubar informações confidenciais continuam a crescer, representando, no último semestre de 2005, 80% dos 50 principais códigos maliciosos reportados. Códigos modulares: os códigos maliciosos modulares, isto é, com componentes iniciais que depois instalam outros módulos, respondem por 88% da lista dos 50 códigos mais reportados no período, um aumento de 14% sobre os 77% anteriormente relatados.Mensagens instantâneas: os softwares de mensagens instantâneas (MSN Messenger, AOL Instant Messenger, Yahoo! Messenger, e outros) estão sendo cada vez mais visados para disseminar códigos maliciosos ou induzir os

público. O método de emissão eletrônica pela Internet significará a quitação das obrigações tributárias de grandes contribuintes em todo o território nacional. Paira o risco ao Estado-Cidadão Arrecadador. O simples armazenamento inadequado de senha ou extravio é de inteira responsabilidade do Contribuinte e coloca em risco o Projeto da Nota Fiscal Eletrônica. É uma corrida. A cada solução surge um problema.

A Legislação que trata do cibercrime[162] não deve ser deficiente e o método de combate pró-ativo. Ao comentar a atuação da Polícia Federal, o perito criminal da Polícia Federal (PF), Paulo Quintiliano da Silva, explicou que a PF trabalha em conjunto com policiais de outros países para resolver crimes praticados na Internet. "No entanto, sua atuação é basicamente reativa e não preventiva, como deveria ser", lamentou o perito.Quintiliano afirmou que, além da inexistência de normas de controle, o Brasil não dispõe de um número de peritos capaz de realizar um trabalho mais expressivo: são apenas 40 agentes.

Atualmente o Estado não tem uma tradição ou legislação preventiva e pró-ativa para promover a defesa do Estado e dos Contribuintes. A falta de uma metodologia e legislação específica, e ainda a inexistência de normatização que

---

usuários a acessarem páginas que exploram vulnerabilidades dos sistemas.Celulares: worms e trojans para dispositivos móveis, especialmente para celulares smartphone, continuam ganhando variantes e adquirindo novas capacidades, como disseminação para computadores rodando Windows e roubo de agendas telefônicas. Phishing Os ataques relacionados a phishing scam continuam crescendo. O número de tentativas de phishing bloqueadas na segunda metade de 2005 pulou de 1,04 bilhão para 1,45 bilhão, um aumento de 44% em relação ao primeiro semestre. Isso significou uma média de 7,92 milhões de tentativas de phishing por dia, contra 5,7 milhões/dia durante o período anterior.
Tendências futuras:
- Aumento dos códigos maliciosos que utilizam capacidades de dissimulação.
- Aumento na comercialização de pesquisas de vulnerabilidades.
- Crescimento de ameaças para plataformas não-convencionais.
- Um ciclo fértil de bots e botnets.
- Aumento das mensagens de phishing e códigos maliciosos distribuídos através de mensagens instantâneas.

161 O relatório completo da Symantec, em inglês, pode ser encontrado na página www.symantec.com/enterprise/threatreport/index.jsp.

162 Disponível: http://www.camara.gov.br/internet/agencia/materias.asp?pk=59220, Reportagem – Patrícia Araújo, Edição - Patricia Roedel. Comenta-se no Website pesquisado que a reprodução foi autorizada mediante citação da Agência Câmara - tel. (61) 216.1851/216.1852 fax. (61) 216.1856 e-mail:agencia@camara.gov.br. A Agência utiliza material jornalístico produzido pela Rádio, Jornal e TV Câmara.

ampare métodos de investigação e auditoria são fatores a serem levados em consideração, uma vez que a Fiscalização não está treinada para coibir fraudes e simulações.

Segundo a Federação Brasileira de Bancos - Febraban, a falta de uma legislação específica para crimes virtuais no Brasil é, hoje, uma forte barreira para o combate desse tipo de fraude; há situações novas que configuram os chamados crimes atípicos, que clamam por uma legislação própria, pois não se enquadram nos tipos penais em vigor. Por conta dessa lacuna, a Polícia Federal e a Justiça tratam esse tipo de delito pela legislação comum, o que levanta as questões: Quais são as garantias ao contribuinte? Qual a segurança ao Estado-Cidadão-Arrecadador? Vamos deixar estas perguntas no ar para reflexão, até por que o projeto NF-e está em fase de testes e, para a adequação deste lamentável quadro, seriam necessárias significativas alterações das antigas e desatualizadas leis Penais e Processuais Brasileiras. Em parte, não é outro, senão o objetivo do amplo Projeto de Lei 89/2003 que, atualmente, tramita no Senado Federal.

Já no início de 2006, imprensa anunciava: “A fraude virtual representa 80% da perda de bancos com roubo”. Face ao grande volume de incidentes e forte impacto das fraudes eletrônicas sobre o setor bancário, a Febraban defende que fraudes na Internet passem a constar na legislação do país como crime inafiançável,[163]pautando-se na premissa de que há falta de uma legislação específica capaz de punir de forma adequada o cibercriminoso no Brasil.

O crime virtual já é mais lucrativo do que o narcotráfico[164].Enquanto as drogas ilegais movimentaram US$ 100 bilhões em 2005, as fraudes *on-line*

---

[163] Disponível: < http://revistaepoca.globo.com/Epoca/0,6993,EPT1111045-1881,00.html> Febraban defende que fraudes na internet virem crime inafiançável” Posted on Wednesday, January 18 @ E. South America Standard Time by davison. A afirmação deve ser consultada no endereço eletrônico: http://www.idgb.com.br/modules.php?name=News&file=article&sid=549. Preocupada com o impacto das fraudes eletrônicas sobre o setor bancário, a Federação Brasileira de Bancos (Febraban) defende que esse tipo de irregularidade passe a constar na legislação do país como crime inafiançável. De acordo com reportagem publicada no jornal Valor Econômico, os bancos acompanham de perto o trâmite do projeto de lei complementar 83/2001 que pode contribuir para que o país tenha legislação específica sobre os crimes eletrônicos, como o roubo de senhas e a violação de contas correntes através da internet.

[164] Os ganhos do crime cibernético, em 2004, excederam os do tráfico de drogas mundial, afirmou a conselheira do Tesouro dos Estados Unidos, Valeri McNiven. Segundo ela, estima-se

totalizaram prejuízos da ordem de US$ 105 bilhões. A Secretaria da Fazenda de São Paulo publicou (Informativo CAT[165] n° 63), que o comércio ilegal se expande na Internet e a pirataria acompanha os mesmos números, já superiores ao do narcotráfico. Portanto, não existe panorama otimista no tocante à utilização de transações de interesse público no ambiente eletrônico. Foi informado, ainda, que o Estado está impotente face ao crime organizado; o crime cibernético cresce e se consolida no mundo todo, tirando proveito do avanço da tecnologia e da vulnerabilidade da comunicação.

Um fisco forte só é possível com a construção democrática de métodos de segurança transparentes na relação com os contribuintes. Um projeto pautado em dados e informações verossímeis. A função do Estado Democrático de Direito é a construção de um método preventivo e simultâneo de combate à corrupção e sonegação. A corrupção abocanha cerca de 32% dos Impostos Arrecadados no Brasil, segundo análise do Instituto Brasileiro de Planejamento Tributário.

---

que os crimes cometidos pela internet - como fraudes, espionagem corporativa, manipulação de ações, pedofilia, extorsões virtuais e diversas formas de pirataria - geraram 105 bilhões de dólares durante 2004. Esta é a primeira vez que o cibercrime desbanca o comércio ilegal de drogas como a atividade criminosa mais lucrativa do planeta."O cibercrime está crescendo tão rapidamente que a lei não consegue acompanhar", disse ela à agência Reuters em uma conferência de segurança bancária em Riad, na Arábia Saudita. Além disso, McNiven aponta o crescimento econômico de países em desenvolvimento, nos quais o policiamento cibernético é ainda precário, como fator decisivo. "Quando você encontra roubo de identidades ou corrupção e manipulação de informação (nos países em desenvolvimento), o problema se torna quase que mais importante porque os sistemas desses países ficam comprometidos desde o seu início", avisou ela. John E Dunn - Techworld, Reino Unido *IDG Now* Publicado neste *Website* por: Equipe Safe Networks
Disponível : <http://www.safenetworks.com >Tão relevante à questão, não bastassem estes dados, há evidências de ligação entre o Cibercrime e o financiamento do terrorismo internacional e o crescimento do tráfico de seres humanos e de drogas. E 2004, foi apontado como o ano em que os crimes cibernéticos passaram a gerar lucros superiores aos do tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004, as perdas totais chegam a US$ 18 bilhões, com taxa de crescimento anual próxima de 35%. Disponível: www.conjur.com.br.

[165] Informativo CAT. Trata-se de informativo mensal da Coordenadoria da Administração Tributária da Secretaria da Fazenda dos Negócios da Fazenda do Estado de São Paulo, que objetiva informar o Auditor Fiscal de Rendas e os Juízes do Egrégio Tribunal de Impostos e Taxas da Secretaria dos Negócios da Fazenda do Estado de São Paulo. O informativo mensal enfatiza importantes artigos de estudiosos para reflexão de dirigentes e funcionários da administração tributária.

Dados oficiais apontam que, só no ano de 2005, os prejuízos com fraudes eletrônicas no mercado nacional ultrapassaram R$ 300 milhões. Contudo estes números são muito superiores e determináveis.

Determináveis por dois motivos: O uso em larga escala dessas ferramentas sofisticadas de segurança dos Bancos envolve custos elevados. Nenhum banco vai investir bilhões de reais em proteção mais do que perde com as fraudes.

Para ilustrar apenas o Banco Itaú mantém investimentos anuais de cerca de R$ 1 bilhão[166] em tecnologia da informação, sempre buscando oferecer ainda mais segurança e modernidade aos clientes. Estes bilionários investimentos existem. A Febraban e as administradoras de cartão de crédito não divulgam o valor das perdas com fraudes por razões de segurança.

Levando-se em consideração a experiência dos bancos, o Estado deveria ter mais cautela com as ferramentas tecnológicas que viabilizarão o trânsito de documentos públicos na rede e adotar grandes investimentos e não baixas aquisições. Órgão de abrangência nacional manifestou que o projeto da NF-e deve oferecer adequada estrutura e robusto suporte tecnológico aos contribuintes.

Segundo Marcia Benedicto Ottoni (2006) [167], a adesão à documentação exclusivamente eletrônica depende de uma base técnica indispensável e legislação que normatize práticas que suportem as transações eletrônicas, bem como falhas no serviço de processamento de dados, com técnicas eficientes de combate à insegurança jurídica, próprias do meio digital – vulnerabilidade dos sistemas, instabilidade, impessoalidade e imateriabilidade dos registros – técnicas capazes de minimizar as fraudes e promover relações mais seguras. Durante esta transição, os advogados serão freqüentemente consultados sobre as conseqüências jurídicas de criar, receber, transmitir, destruir, registrar, guardar e converter cópias materiais em documentos eletrônicos.

---

166 Disponível: <http://www.covergenciadigital.com.br>
Programa “Mais Segurança” tem função social, diz Itaú, Jackeline Carvalho. Acesso 26 julho 2006.

167 Artigo: Certificação Digital e Segurança. In: E-dicas: O Direito na Sociedade da Informação. Marcia Benedicto Ottoni. Gerente Jurídica da CertiSign.

O panorama sistêmico de riscos cibernéticos foi alvo de um amplo estudo realizado pela Deloitte com 150 organizações de um setor com alto grau de dependência tecnológica[168]: as instituições financeiras. Formada em sua maioria (88%) por bancos e seguradoras, a amostra expressa visões e soluções de corporações de todo o mundo, inclusive o Brasil". Nas últimas duas edições da pesquisa, o acesso não autorizado a informações pessoais foi o item mais assinalado entre as preocupações relacionadas à privacidade de dados: 84% em 2006 e 83% em 2005, contra 62% em 2004.

Outro fator que deve ser ponderado pelas Administrações Fazendárias é a "velocidade de processamento, atualizações e a agilidade dos fraudadores que utilizam programas maliciosos que se atualizam automaticamente" [169].

Curiosamente é mister mencionar que na América Latina, o Brasil poderá se integrar em um dos maiores acordos mundiais para desenvolvimento de segurança de ponta na Internet: Acordo de *Wassenaar*, firmado pelos integrantes do G8[170] e diversos paises. Tal tratado tem o objetivo de limitar a exportação da

---

[168] Disponível: <http://www.tiinside.com.br/Filtro.asp?C=265&ID=88899>- Gastos de bancos com TI alcançam US$ 15 bilhões.

[169] O setor bancário brasileiro gastou R$ 15 bilhões em tecnologia da informação no ao passado, cifra 4% maior a registrada em 2006, de acordo com dados divulgados nesta terça-feira (27/5) pela Febraban (Federação Brasileira de Bancos). Deste total, US$ 6,2 bilhões foram investimentos em novas tecnologias, 16% a mais que o total gasto no ano anterior, quando aplicaram US$ 5,3 bilhões. A pesquisa também aponta que o total de usuários de internet banking existentes no país passou de 27,3 milhões em 2006 para 29,8 milhões em 2007. Isso significa um crescimento de 9,2%, sendo 25,3 milhões de clientes pessoas físicas e os outros 4,5 milhões, de pessoas jurídicas.
O mainframe, segundo dados da pesquisa, cresceu 15% em quantidade de Mips (milhões de instruções por segundo) nos *data centers* dos bancos, passando de 349.441 Mips em 2006 para 403.128 Mips em 2007. Isso ocasionou também um aumento nas despesas terceirizadas de manutenção de sistemas legados, que cresceram 27% de um ano para outro. Isso justificou uma queda de 12% nas despesas com contratação de fábrica de software.
Um dado novo da pesquisa foi o crescimento do número de servidores rodando Linux em pontos de atendimentos, que somaram 5.719 unidades, contra 16.698 servidores Windows. Acesso maio 2008.
Disponível:<http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148> Acesso maio 2008

[170] Disponível:< http://www.wassenaar.org/participants/contacts.html#Czech_Republic>
Citam os doutrinadores Brasileiros que na América Latina, e no Brasil inclusive, essa questão não tem merecido maiores preocupações dos setores oficiais, exceto talvez, por parte da Argentina que é signatária do acordo de Wassenaar - firmado entre os integrantes do G8 e mais diversos países, com o objetivo de limitar a exportação das chamadas "tecnologias sensíveis" aos países não signatários (dentre os quais se inclui o Brasil), da qual constam não só armamentos de ponta

chamada tecnologia sensível aos países não signatários como o Brasil. Essa questão, voltada à Segurança Nacional Brasileira, não tem merecido maiores preocupações dos setores oficiais. A Argentina é signatária do acordo que também envolve troca de informações para a construção de criptografia de ponta, com vista a impedir a ação de invasores e a ação de terroristas.

É justamente neste particular que atuação preventiva do governo deve ser efetiva. Viabilizar a sociedade o seu mais amplo desenvolvimento, diminuindo, na medida do possível, as perdas que possam vir a ocorrer. À conta do que se expôs, torna-se imperiosa a necessidade de que se aprofundem os estudos sobre as garantias contra perdas e invasões dos contribuintes e preservação de sua boa fé.

A utilização isolada da Nota Fiscal Eletrônica aponta para o fato de tornar-se um novo alvo de grande geração de riqueza ao cibercriminoso. Para as empresas, um novo fator de risco sistêmico de segurança corporativa. Caso as empresas não atendam à necessidade de armazenamento adequado das informações utilizadas para a geração do documento. Sem dúvida estes custos não são baratos, como tem sido veiculado pela mídia. Para a emissão de cada Nota Fiscal Eletrônica, a legislação exige a utilização de um certificado digital somado a uma chave privada de segurança, que precisam ser guardados, sendo este um dever jurídico do contribuinte ao optar pela nova tecnologia. “Este par de recursos tecnológicos precisa ser guardado em um lugar que não permita acesso

---

como mísseis, submarinos nucleares etc., mas produtos de tecnologia civil que podem ser utilizadas pelo terrorismo (as chamadas “dual-mode technologies”), dentre as quais está a criptografia. Os países citados em 2005 pelos doutrinadores são: Argentina, Austrália, Áustria, Bélgica, Bulgária, Coréia, Dinamarca, Eslováquia, Espanha, Finlândia, Grécia, Holanda, Hungria, Irlanda, Luxemburgo, Noruega, Nova Zelândia, Polônia, Portugal, República Tcheca, Romênia, Rússia, Suécia, Suíça, Turquia e Ucrânia. Lucca, Newwton De e Simão Filho, Adalberto (cordenadores) e outros, Direito&Internet-São Paulo: Quartier Latin, 2ª edição, 2.005. Artigo de Regis Magalhães Soaresde Queiroz&Henrique Azevedo Ferreira França, pág 238. Consultando o Website: verifico a nova lista de membros: Argentina, Australia, *A*ustria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia,Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, *United States.* Acesso maio 2008

indevido, cópia ou qualquer outro tipo de violação" explica Carlos Magno, Sócio - Diretor da *True Access*.

O artigo *CRACKER*[171] informa que redes de computadores são usadas todos os dias por corporações e várias outras organizações, portanto vulneráveis. Para piorar a insegurança do trânsito de documentos públicos no Brasil, não há regulamentação sobre provedores de Internet e suas responsabilidades. Eles atuam segundo seus próprios critérios, em geral movidos por razões apenas econômicas. No Senado, entre outras propostas, tramita o projeto de lei 5.403/01, que regulamenta o acesso às informações na rede. Se aprovado, os provedores de Internet terão de arquivar por um ano o histórico de acesso de seus usuários para ajudar no combate ao uso indevido da rede.

O bem tutelado é o Estado Cidadão Arrecadador e a Segurança do Sistema Fiscal. As formas de tributação serão afetadas pela velocidade do processo tecnológico, base da Nota Fiscal Eletrônica e do Sistema Público de Escrituração Digital.

Para promover o pretendido processo de “revolução fiscal”, as Fazendas Estaduais tem de passar por um processo de fortalecimento interno em vários níveis para depois, colocar em pauta o duvidoso instrumento de integração da gestão tributária nacional em suas diferentes esferas. Neste sentido, para a implantação de um projeto desta magnitude, os Auditores Fiscais de Renda dos Estados, Municípios e da Esfera Federal, devem dominar as novas tecnologias,

---

171 Disponível: < http://www.csu.uem.mz/cracker.htm >

As redes de computadores permitem que os usuários troquem uma vasta quantidade de informações ou dados eficientemente. Usualmente, redes corporativas não são desenvolvidas e implementadas com certa segurança em mente, mas para terem funcionalidade e eficiência máximas. Embora isto seja bom, sob o ponto de vista empresarial, os problemas de segurança certamente aparecerão depois e as empresas gastarão muito dinheiro para resolvê-los na proporção do tamanho de suas redes. Muitas redes corporativas e privadas funcionam baseadas no princípio Cliente-Servidor, onde os usuários utilizam *workstations* para conectarem-se aos servidores e compartilharem as informações. Este documento irá concentrar-se na segurança do servidor, alvo primordial dos *crackers*, pois se ele consegue acesso a este computador que, geralmente, é o mais bem protegido da rede, é muito fácil conseguir acesso ao restante da rede. O elemento vulnerável de um ataque sistêmico em grande escala, normalmente, inclui: instituições financeiras e bancos; ISPs (provedores de internet); companhias farmacêuticas; governo e agências de defesa; empresas multinacionais, embora muitos desses ataques sejam feitos pelos próprios funcionários da empresa que têm senhas de acesso a determinados setores. Acesso maio 2008.

assim como os contribuintes. *Len Hynds*, chefe da luta contra os crimes da *Internet* na Inglaterra, diz que todo policial tem de dominar as novas tecnologias[172].

Do mesmo modo que a Nota Fiscal Eletrônica, quando o Emissor de Cupom Fiscal (ECF) foi criado, anunciava-se o fim das fraudes no varejo, porém, a partir de falhas sistêmicas, equipamentos e pareceres do CONFAZ foram anulados, comprometendo, desta forma, os pilares básicos de tal projeto, tais como os requisitos específicos de segurança da informação e a comprovação eficiente da autenticidade e integridade. Estes pareceres "garantiam" a inviolabilidade das máquinas ECF, mas as armas da fraude e sonegação fiscal sempre encontram os seus caminhos.

Por outro lado, a Polícia Federal concluiu que os meios eletrônicos já são capazes de simular o efeito marca d'água, previsto do Convênio CONFAZ 10/05, este inclusive, ainda mais fácil de ser simulado de forma caseira, com o uso de tintas ou produtos químicos. O estado de São Paulo, de forma excepcional, não aderiu a este Convênio, face à Informação Técnica do Instituto Nacional de Criminalística da Polícia Federal.

Ainda para a fase de implantação, coordenadores e administradores fazendários devem trabalhar com a cooperação de técnicos fazendários especializados com altíssimo nível, bem como se valer da experiência do setor de combate aos crimes cibernéticos do Instituto Nacional de Criminalística da Polícia Federal.

Como exposto, deve-se estudar este projeto, tendo em vista a precariedade atual do cenário brasileiro, no que tange ao trânsito maciço de informações fiscais pela rede mundial de computadores. A inteligência fiscal precisa realizar uma ação que é básica em qualquer tipo de projeto: uma criteriosa análise de riscos. Tratar o projeto como inviolável ou infalível é um completo exagero e demonstra irresponsabilidade por parte de algumas empresas

---

[172] CAPA DA VEJA São Paulo, 3.11.04.

ditas como “provedoras de solução”. Os que “vendem somente facilidade” devem mostrar, de forma isenta e profissional, o terreno em que estamos pisando.

É claro que o monitoramento eletrônico de operações melhorará, e muito, a eficácia da ação fiscal, mas outras janelas de sonegação sempre existirão. A maioria dos contribuintes brasileiros de ICMS que ainda não usam computador.[173]

A Nota Fiscal Eletrônica é uma realidade a ser estudada com cuidado e ponderação pelas autoridades. Este documento digital é uma realidade que precisa ser acompanhada de perto pelo Instituto Nacional de Criminalística da Polícia Federal e Ministério Público, de forma ampla e completa, pois os casos de fraude são alarmantes e preocupantes.

O crime na Internet e a impunidade tornaram-se um círculo vicioso que, sob o ponto de vista tecnológico, parece não ter limites. "Nós criamos uma civilização global em que elementos cruciais - como as comunicações, o comércio, a educação e até a instituição democrática do voto - dependem profundamente da ciência e da tecnologia. Também criamos uma ordem em que quase ninguém compreende a ciência e a tecnologia. É uma receita para o desastre. Podemos escapar ilesos por algum tempo, porém, mais cedo ou mais tarde, essa mistura inflamável de ignorância e poder vai explodir na nossa cara". (Carl Segan, cientista e escritor em "O mundo assombrado pelos demônios",[174]).

---

[173] Segundo informações colhidas no Sebrae, 60% do micro e pequenos empresários não sabem ligar um computador, bem como não têm acesso à Internet.

[174] SAGAN, Carl. O mundo assombrado pelos demônios. São Paulo: Cia das Letras, 1997.

4. Conclusão

Nesta pesquisa procurou-se abordar a utilização da internet e da tecnologia por facções criminosas que cada vez mais tem se utilizado destas ferramentas para suas ações ilícitas contra o Estado. Pretendeu-se remeter o leitor a uma reflexão sistêmica sobre até que ponto esta nova criminalidade acarreta danos a Estados e Governos se estes forem dependentes de um único sistema de comunicação como a Internet e refletir sobre quais seriam os meios de contingência e soluções que poderiam levar estes agentes políticos a um patamar de maior segurança.

Para tanto, analisou-se a possibilidade de se retirar os conceitos de que esses novos projetos são invulneráveis, procurou-se demonstrar que muitos desses conceitos são passados à sociedade por meio de comunicação que se preocupa com a venda de produtos e não com o resultado e efetividade de mecanismos de segurança. Com esse fim, buscaram-se exemplos na história recente no Brasil e em outros países da evolução da criminalidade o modo de comportamento de agentes terroristas e até que ponto é possível aprender com essa análise, uma vez que as facções criminosas adotam a estratégia de grupos terroristas para angariar recursos. Procurou-se analisar na história recente das últimas duas décadas projetos que nasciam sobre a pecha de invulneráveis, mas que depois se verificou a falha das tecnologias frente a sua proposta inicial ser um mecanismo invulnerável de combate à criminalidade. Com exemplos e casos concretos aponta-se que a criminalidade também evolui e encontra novos caminhos.

De um modo mais dedicado, analisou-se o projeto da nota fiscal eletrônica como meio de combate a sonegação fiscal e também a veracidade de

sua plataforma a sociedade. Nesse particular, a pesquisa procurou demonstrar que nos meios de comunicação se propaga a idéia de benefícios ao novo sistema. Nessa linha empresas de tecnologia se preocupam muito mais em vender seus produtos tecnológicos do que em realmente passar um conceito real à sociedade.

Nesse processo de integração e cruzamento de dados, recomenda-se uma maior cooperação preventiva entre os Estados e os órgãos de Criminalística Central da Polícia Federal, seja através de Convênios, seja através de atos governamentais. Aponta-se que no trato do dinheiro público as ações devem ser preventivas e ativas e não apenas repressivas. Em uma visão de futuro desta batalha tecnológica recomenda-se que Estados Contribuintes criem um fundo que certamente será útil para o combate a outras crises mundiais que possam surgir, a exemplo desta que atinge os Estados Unidos (final de 2008).

Foi também verificado que a fatores sociais e políticos são fortes obstáculos à implementação da nota fiscal eletrônica, uma vez que a guerra fiscal é um dos principais fatores ventilados na pesquisa. Nessa nova fronteira, recomenda-se a criação de instrumentos de governo que venham a possibilitar a socialização do risco com a criação de Fundos capazes de gerar a proteção de contribuinte na eventualidade de falhas do sistema gerar danos larga escala a toda a sociedade.

O presente estudo pretendeu demonstrar que o Projeto (NF-E) e outros processos voltados a implantação do Governo Eletrônico nascem desamparados em meio a um crescente sentimento de pânico virtual, o que prenuncia que num segundo momento, quando de sua plena implantação, vai crescer sem sustentação, em meio a códigos brutalmente maliciosos em meio a esperteza e disfarces de organizações criminosas, altamente especializadas no furto qualificado de informações confidenciais. Os brasileiros correm riscos virtuais e o Brasil tem sido consagrado com o título de um dos países mais inseguros do mundo para as questões relacionadas à criminalidade cometida com a utilização da rede mundial de computadores. A Administração Pública Nacional deve estar

ciente de que seus projetos irão conviver no mesmo ambiente onde reside um vertiginoso e alarmante crescimento de cibercrimes, desde o início do século XXI. Nesse contexto, a troca de informações entre diversos organismos de Governo e a iniciativa privada é muito importante.

Considerando a facilidade com que são retirados documentos falsos até mesmo de dentro da Secretaria da Receita Federal recomendou-se à Federação das Indústrias do Estado de São Paulo – FIESP a adoção de uma ação pró-ativa e participativa do Instituto Nacional de Criminalística da Polícia Federal no Projeto Nota Fiscal Eletrônica pois acredita-se que o INC tenha muito a oferecer.

Por outro lado, as experiências dos bancos servem como pertinente reflexão, alerta e também como método comparativo. O Governo Eletrônico trata do trânsito em larga escala de documentos públicos. Sejam cópias de petições junto aos Tribunais, seja o trânsito de notas fiscais e livros fiscais. O método de emissão eletrônica pela Internet significará a quitação das obrigações tributárias de grandes contribuintes em todo o território nacional e o protocolo de prazos e petições. Paira o risco ao Estado-Cidadão Arrecadador se for mantido o sentido de Estado invulnerável e a sensação de super poder do Estado. O simples armazenamento inadequado de senha ou extravio é de inteira responsabilidade do Cidadão, advogados e Contribuintes e coloca em risco Tribunais e Governos. É uma corrida, uma guerra infinita. Nessa pesquisa foram apontadas estimativas de conceituadas organizações que apontam que os usuários da rede temem o cibercrime mais que delitos físicos.

A Legislação que trata do cibercrime não deve ser deficiente e o método de combate precisa ser pró-ativo. As ações de interligação preventivas devem representar o marco e o início de Projetos Governamentais e parcerias público privadas voltadas ao incentivo a pesquisa destas soluções na Sociedade da Informação. Os fatos e as estatísticas demonstram que não existe ambiente totalmente seguro na Internet, na forma como esta sendo divulgado por algumas empresas e apontamos que a Nota Fiscal Eletrônica não será capaz de reduzir a sonegação fiscal se outros métodos de controle forem implantados. Temos como

exemplo desta divulgação o Projeto da Nota Fiscal Eletrônica, divulgado como infalível como muitos outros projetos também o eram no passado e falharam.

Um Estado forte só é possível com a construção democrática de métodos de segurança, cooperação e investigação transparentes na relação com contribuintes e cidadãos. Um projeto pautado em dados e informações verossímeis. A função do Estado Democrático de Direito é a construção de um método preventivo e simultâneo de combate à corrupção e sonegação. Não existe até o momento uma doutrina ou um trabalho que venha a tratar de sistemas de segurança preventivo ativo de combate a crime cibernético organizado capaz de ser implementado para garantir que informações não sejam corrompidas ou "vazadas". Como acontece com os bancos, o cibercriminoso vai atacar o lado mais fraco da relação entre o Estado e o Cidadão.

Infelizmente o combate à corrupção no Brasil não costuma ser enumerado entre as missões da administração pública. O presente trabalho não pretende criticar os processo tecnológicos,mas trazer uma visão de que apenas um lado do tema tem sido enfrentado, sendo necessário percorrer todos os caminhos porque as crises nascem nestes processos. Nesse sentido, a adesão à documentação exclusivamente digital depende de um ponto fulcral técnico vital e uma legislação que normatize práticas que suportem as transações eletrônicas, bem como falhas no serviço de processamento de dados, com técnicas eficientes de combate à falhas e vulnerabilidades próprias do meio digital de ordem mais complexa do que os documentos tradicionais.

Durante esta transição, a comunidade jurídica deverá ser freqüentemente consultada sobre as conseqüências jurídicas de criar, receber, transmitir, destruir, registrar, guardar e converter cópias materiais em documentos eletrônicos.

Outro fator que deve ser ponderado pelas Administrações Fazendárias é a velocidade de processamento, atualizações e a agilidade dos fraudadores que utilizam programas maliciosos que se atualizam automaticamente. Ou seja, demonstrou-se que a criminalidade digital cria programas robôs inteligentes. É justamente neste particular que atuação preventiva o governo deve ser efetiva.

Viabilizar à sociedade o seu mais amplo desenvolvimento, diminuindo, na medida do possível, as perdas que possam vir a ocorrer. À conta do que se expôs, torna-se imperiosa a necessidade de que se aprofundem os estudos sobre as garantias contra perdas e invasões dos contribuintes e preservação de sua boa fé.

A conclusão desta pesquisa se apóia na recente manifestação de organismos internacionais como a Organização para a Cooperação e Desenvolvimento - OCDE e a Organização Mundial do Comércio - OMC, que diante das perdas potencias de receitas tributárias resultantes do desenvolvimento do comércio eletrônico sugeriram uma “Política Fiscal Mundial” para a tributação desse tipo de comércio. A amplitude mundial dessa “política fiscal” se faz necessária, uma vez que não há mais limites territoriais às operações comerciais em razão dos avanços tecnológicos, tais como a internet e a virtualidade das transações.

5. Bibliografia

ALMEIDA FILHO, José Carlos de Araújo. **Processo eletrônico e teoria geral do processo eletrônico**. Rio de Janeiro: Forense, 2007

ALMEIDA FILHO, José Carlos de Araújo. Com a Informatização, a tendência é o aumento de fraudes. Disponível: <http://blog.processoeletronico.com.br/2008/04/13/com-a-informatizacao-a-tendencia-e-o-aumento-de-fraudes/> Acesso 30 maio 2008

AMAZONAS, Marina. O submundo do Crime. Correio Brasiliense 16/11/2004.

ASCENÇÃO,José Carlos de Oliveira. **Direito da Internet e da Sociedade da Informação**. Rio de Janeiro: Forense, 2002.

BALKIN**,** Jack M.; NOVECK, Beth Simone. **The State of Play: law, games, and virtual worlds**. New York: New York University Press, 2006.

BARRETO Júnior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. *In*: PAESANI, Liliana Minardi (Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

BARROS, Marco Antonio de. Tutela punitiva tecnológica. *In*: PAESANI, Liliana Minardi (Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

BOTELHO, Fernando. Para não perder o bonde no combate ao cibercrime. **Convergência Digital**. 06/07/2007. Disponível em <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=8327&sid=15>. Acesso em maio de 2008.

BUENO, Pedro. Cyber Crimes - a trilha do dinheiro. Proceedings of the Second International Conference on Forensic Computer Science Investigation (ICoFCS`2006)/ABEAT(ed.)- Guarujá, Brasil, 2007,124pp.- ISSN-1980-1114.

CAMPOS, André L.N. **Sistema de Segurança da Informação: controlado os riscos.** Florianópolis: Visual Book, 2006.

CARPANEZ, Juliana. Saiba como funcionam os golpes virtuais. Disponível: < http://www1.folha.uol.com.br/folha/informatica/ult124u19456.shtml> Acesso 31 maio 2008.

CORREA, Gustavo Testa. **Aspectos Jurídicos da Internet**. Editora Saraiva, São Paulo/2000.

CASTELLS, Manuel**. A Era da Informação: economia,sociedade e cultura**. 5 ed. São Pulo: Paz e Terra, 2001.v.I.

CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). Cartilha de Segurança para Internet. Disponível: <http://cartilha.cert.br/glossario/> Acesso 30 maio 2008.

Costa Júnior, Paulo José da.**Curso de Direito Penal**. São Paulo: Saraiva, 1º v., Parte Geral, 1991.

DAWEL, George. **A Segurança da Informação nas Empresas.** Rio de Janeiro: Ciência Moderna, 2005.

DE LUCCA, Newton. Aspectos jurídicos da contratação informática telemática. São Paulo:Saraiva, 2003.

DIAS, Virgínia Soprana. **Aspectos da Segurança Jurídica no Âmbito dos Crimes Cibernéticos.** "Proceedings of the Second Internacional Conference of Forensic Computer Science Investigation". (ICoFCS`2007)/ABEAT (ed.)- Guarujá, Brasil, 2007,120 pp.- ISSN-1980-1114

FINKELSTEIN, Maria Eugenia Reis. **Aspectos Jurídicos do Comércio Eletrônico.** Thomson IOB, Editora Síntese, 2004.

FLEURY, André. Criptografia: criptus-graphos - uma questão de Segurança Nacional. Disponível em http://www.radiobras.gov.br/ct/artigos/1998/artigo_271198.htm Acesso em maio de 2008.

FOLHA ONLINE. "Vírus de PC divulga dados sigilosos da polícia japonesa". Disponível: <http://www1.folha.uol.com.br/folha/informatica/ult124u19727.shtml> Acesso 06 março 2006

GRECO, Marco Aurélio. **Internet e Direito**. 2 ed. São Paulo. Editora Dialética, 2000.

GRINOVER Ada Pellegrini; FERNANDES Antonio; GOMES FILHO Antonio Magalhães. **As nulidades no processo penal**. São Paulo: Revista dos Tribunais, 2005.

GUIA do Usuário Conectiva Linux. TCP/IP. Disponível:< http://www.dimap.ufrn.br/~aguiar/Livros/Conectiva9Usuario/glossario.html > Acesso 31 maio 2008.

HOUAISS. **Dicionário da Língua Portuguesa**. Versão online disponível em http://biblioteca.uol.com.br (para assinantes). Último acesso em novembro de 2008.

ICP Brasil. O que é Criptografia? Disponível: <http://www.icpbrasil.gov.br/duvidas/faq/o-que-e-criptografia> Acesso 29 maio 2008.

KAMINSKI, Omar. Retrospectiva 2005 Tecnologia impulsionou acesso à informação jurídica. Disponível: <http://conjur.estadao.com.br/static/text/40300,1 >

Livro Verde da Sociedade da Informação no Brasil. Disponível em: http://www.mct.gov.br/index.php/content/view/18878.html. Grupo de Implantação: Programa Sociedade da Informação e Ministério da Ciência e Tecnologia. Brasília, setembro 2.000.

MACHADO, Hugo de Brito. Proibição do contribuinte inadimplente de imprimir notas fiscais. São Paulo: RDDT - Revista Dialética de Direito Tributário, junho de 2007, artigo página 85 "usque" 95.

MANSO, Bruno Paes; GODOY, Marcelo. MPE usa denúncia multimídia para driblar crise. Cidades/Metrópole. O Estado de São Paulo, 11/03/2007, p. C4.

MARCELO, Antonio; PEREIRA, Marcos. **Engenharia Social: hackeando pessoas.** Rio de Janeiro: Brasport, 2005.

MARTINS, Ives Gandra da Silva. Obtido por meio eletrônico. Revista Consultor Jurídico, dois de janeiro de 2007, artigo “tributos a Brasileira”. http://conjur.estadao.com.br/static/text/51542,1

MICROSOFT Windows Help. O que é encriptação? Disponível: <http://windowshelp.microsoft.com/Windows/pt-PT/Help/f219e5c8-b97b-469a-8dc3-d1791fa6386c2070.mspx> Acesso 31 maio 2008.

MINISTÉRIO PÚBLICO FEDERAL; COMITÊ GESTOR DA INTERNET NO BRASIL. Crimes Cibernéticos. Manual prático de investigação: São Paulo, 2006.

NBSO. Cartilha de Segurança para Internet. O que é criptografia de chaves pública e privada? Disponível: <http://www.htmlstaff.org/cartilhaseguranca/cartilha-03-privacidade.html#subsec1.2> Acesso 31 maio 2008.

NUCCI, Guilherme de Souza, **Código penal comentado**. São Paulo: Revista dos Tribunais, 2007.

NÚCLEO DE INFORMAÇÃO e Coordenação do Ponto Br. Disponível:< http://nic.br/sobre-nic/index.htm> - Acesso 30 maio 2008

O'BRIEN, Natalie. Virtual terrorists - Hunted in reality, jihadists are turning to artificial online worlds such as Second Life to train and recruit members. Disponível: <http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html Acesso em agosto 2007.

OTTONI, Márcia Benedicto. Certificação Digital e Segurança. Disponível em <https://www.certisign.com.br/certinews/artigos/certificacao-digital-e-seguranca/> acesso em junho/2008.

PAESANI, Liliana Minardi *et al*. **O Direito na Sociedade da informação**. São Paulo: Atlas, 2007.

PEOTTA Laerte, Dino Amaral. Honeypot de Baixa Interação como ferramenta para detecção de tráfego com propagação de Botnests. Proceedings of the second international conference on forensic computer science investigation (ICoFCS`2007)/ABEAT(ed.)- Guarujá, Brasil, 2007,120pp.- ISSN-1980-1114.

Policia Federal. Instrução Técnica N°001/GAB/DITEC. Ministério da Justiça, Brasília-DF 10 de outubro de 2.005. Dispõe sobre a padronização de procedimentos e exames no âmbito da perícia e informática.

RAMOS JUNIOR, Hélio Santiago .Crimes contra a Segurança dos Sistemas de Informações da Administração Pública. “Proceedings of the Second Internacional Conference of Forensic Computer Science Investigation”. (ICoFCS`2007)/ABEAT(ed.)- Guarujá, Brasil, 2007,120 pp. p. 65.- ISSN-1980-1114.

REIS Maria Helena Junqueira**. Computer crimes**. Belo Horizonte: Del Rey, 1997.

REZENDE, Pedro Antonio Dourado de. Tipos mais simples de Fraude e Ofuscação do seu Risco. Universidade de Brasília, 2002. Disponível: <http://www.cic.unb.br/docentes/pedro/trabs/SBC.htm> Acesso 30 maio 2008.

ROCHA FILHO, Valdir de Oliveira coordenação. **O Direito e a Internet**. 1. ed. Rio de Janeiro: Editora Forense Universitária, 2002.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2005.

ROVER, José Aires. **Direito e Informática.** Barueri: Manole, 2004.

RULLI JUNIOR, Antonio. "Estrutura e organização judiciária do poder Judiciário do Brasil e universalidade da jurisdição", in Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas, Sede Internacional, São Paulo, ano 10, n. 16, jul./dez. 1996, co-edição APAMAGIS.

RULLI JUNIOR, Antonio, "Estrutura e Organização do Poder Judiciário do Brasil e Universidade de Jurisdição", Revista da Faculdade de Direito dos FMU, Série Internacional VI, Mercosul, ano 10, nº 16,1996.

RULLI JUNIOR, Antonio. "Execução Penal - Visão do TACRIM-SP", São Paulo, Editora Oliveira Mendes, 1998, em colaboração com o título: "Penas Alternativas".

RULLI JUNIOR, Antonio. "Jurisdição e Reforma do Poder Judiciário", Revista da Faculdade de Direito das FMU, Série Nacional, Ano 10, nº 17, 1996.

RULLI JUNIOR, Antonio, "Mercosul: O Direito Comunitário e a Garantia de investimento o Cidadania", Revista da Faculdade de Direito das FMU, Série Nacional, Ano XII, nº 20, 1998 (co-autoria com Francisco Pedro Jucá).

SÊMOLA, Marcos. **Gestão da Segurança da Informação: visão executiva.** Rio de Janeiro: Elevier.2003.

SAGAN, Carl. **O mundo assombrado pelos demônios**. São Paulo: Cia das Letras, 1997.

SCHONOOR, Tatiana. Crimes Digitais geraram prejuízo de R$300 mi em 2005. Disponível:<http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148> Acesso maio 2008

SILVA, Paulo Quintiliano da. dos Crimes Cibernéticos e seus efeitos internacionais. *Procedings of the Firts International Conference on Forensic Computer Science Investigation* (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114

SILVA, Paulo Quintiliano da. A perícia de Informática na Polícia Federal. *Procedings of the Firts International Conference on Forensic Computer Science Investigation* (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114

SOFTWARE LIVRE. É possível violar a urna eletrônica? Disponível: <http://www.softwarelivre.org/news/3163> Acesso em 30 maio 2008.

SPYBOT.INFO Disponível: <http://www.spybot.info> Acesso 30 maio 2008

TOURINHO FILHO, Fernando da Costa. **Processo Penal**. São Paulo: Saraiva, 2007. (2 volumes)

THEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil**. 3 volumes. São Paulo: Forense, 2006.

The International Journal of Forensic Science –V. 1 e V. 2, 2006, 2.007 Brasil. Brazilian Forensic Cyber Crime Unit – Brasilian Federal Police – Brasilia, Brazil. ISSN 1809-9807.

THOMÉ, Clarissa. Perícia de escutas em SP pode levar 4 anos. Caderno Metrópole. Jornal O Estado de São Paulo. 11/03/2007, p. C1.

TIINSIDE <http://tiinside.com.br> acesso em maio 2008.

Ministério da Justiça. Departamento de Polícia Federal. Diretoria Técnica – Científica. Manual de Instruções e Procedimentos. Dispões sobre a padronização de procedimentos e exames no âmbito de perícia. Material de uso Controlado.

VADE MECUM SARAIVA 2008. São Paulo: Saraiva, 2008.

VIEIRA, Eduardo. Por que os mundos virtuais como o *Second Life* podem representar o início de uma nova era na web. Revista Época. Disponível em <http://revistaepoca.globo.com/Revista/Epoca/0,,EDG76738-5990-461,00.html> Acesso 19 março 2007.

VOGT, Peter InternetspieleTummelplatz für Kinderpornografie - Moderation Fritz Frey. Disponível:<http://www.swr.de/report/-/id=233454/nid=233454/did=2060062/1h0wega/index.html> Acesso agosto 2007.

Anexo I

HC 88905 / GO - GOIÁS
HABEAS CORPUS
Relator(a): Min. GILMAR MENDES
Julgamento: 12/09/2006 Órgão Julgador: Segunda Turma

Publicação

DJ 13-10-2006 PP-00067 EMENT VOL-02251-02 PP-00395
LEXSTF v. 28, n. 336, 2006, p. 480-500Parte(s)

PACTE.(S) : DANILO DE OLIVEIRA
IMPTE.(S) : FRANCISCO DAMIÃO DA SILVA
COATOR(A/S)(ES) : SUPERIOR TRIBUNAL DE JUSTIÇA Ementa

EMENTA: Habeas Corpus. 1. Crimes previstos nos arts. 288 e 155, § 4º, incisos II e IV, ambos do Código Penal e art. 10, da Lei Complementar nº 105/2001 (formação de quadrilha, furto qualificado e quebra de sigilo bancário). 2. Alegações: a) ausência de fundamentação do decreto de prisão preventiva; b) excesso de prazo para formação da culpa e conclusão do processo. 3. No caso concreto, a decretação da preventiva baseou-se no fundamento da garantia da ordem pública, nos termos do art. 312 do CPP. O Juiz de 1º grau apresentou elementos concretos suficientes para a caracterização da garantia da ordem pública: a função de "direção" desempenhada pelo paciente na organização, o qual liderava "célula criminosa"; a ramificação das atividades criminosas em diversas unidades da federação; e a alta probabilidade de reiteração delituosa considerando a potencialidade da utilização ampla do meio tecnológico sistematicamente empregado pela quadrilha. Precedentes: HC nº 82.149/SC, 1ª Turma, unânime, Rel. Min. Ellen Gracie, DJ de 13.12.2002; HC nº 82.684/SP, 2ª Turma, unânime, Rel. Min. Maurício Corrêa, DJ de 1º.08.2003 e HC nº 83.157/MT, Pleno, unânime, Rel. Min. Marco Aurélio, DJ de 05.09.2003. 4. Quanto à alegação de excesso de prazo, constata-se a complexidade da causa. No caso concreto, apuram-se diversos delitos cometidos por vários co-réus, denotando razoabilidade na dilação do prazo de instrução processual, sem que a prisão dos envolvidos configure constrangimento ilegal. Dos documentos acostados aos autos, verifica-se também haver contribuição da defesa para a demora processual, não se configurando a ilegalidade alegada por excesso de prazo, por não haver mora injustificada. Precedentes da Corte: HC nº 81.905/PE, 1ª Turma, maioria, Rel. Min. Ellen Gracie, DJ de 16.05.2003; HC nº 82.138/SC, 2ª Turma, unânime, Rel. Min. Maurício Corrêa, DJ de 14.11.2002; e HC nº 71.610/DF, Pleno, unânime, Rel. Min. Sepúlveda Pertence, DJ de 30.03.2001. 5. Decreto de prisão preventiva devidamente fundamentado, nos termos do art. 312 do CPP e art. 93, IX, da CF. Existência de razões suficientes para a manutenção da prisão preventiva. Precedentes. 6. Ordem indeferida

Decisão

A Turma, por votação unânime, indeferiu o pedido de habeas corpus, nos termos do voto do Relator, com recomendação. Ausentes, justificadamente, neste julgamento, os Senhores Ministros Joaquim Barbosa e Eros Grau. 2ª Turma, 12.09.2006.
Indexação(...)

Anexo II

SF PLS 00076 / 2000 de 27/03/2000
Autor SENADOR - Renan Calheiros
Ementa Define e tipifica os delitos informáticos, e dá outras providências.
Indexação REGULAMENTAÇÃO DISPOSITIVOS, DIREITOS E GARANTIAS FUNDAMENTAIS, CONSTITUIÇÃO FEDERAL, DEFINIÇÃO, CRIME CONTRA A LIBERDADE INDIVIDUAL, VIOLAÇÃO, PRIVACIDADE, PESSOA FÍSICA, CIDADÃO, DADOS PESSOAIS, UTILIZAÇÃO, BANCO DE DADOS, INFORMÁTICA, ABUSO, CRIME, SISTEMA, COMUNICAÇÃO, DESTRUIÇÃO, DADOS, COMPUTADOR, TRANSFERÊNCIA FINANCEIRA, VALOR, ATIVO FINANCEIRO, CONTA BANCÁRIA, INEXISTÊNCIA, CONSENTIMENTO, SUPRESSÃO, INFORMAÇÃO, OBJETIVO, PREJUÍZO, DANOS PESSOAIS, DIREITOS, OBRIGAÇÕES, VERDADE, FATO JURÍDICO, CORRELAÇÃO, FALSIFICAÇÃO, INFRATOR, CRIMINOSO POR TENDÊNCIA, APLICAÇÃO, PENA, AMPLIAÇÃO, HIPÓTESE, VÍTIMA, ÓRGÃO PÚBLICO, ADMINISTRAÇÃO DIRETA, ADMINISTRAÇÃO INDIRETA, UNIÃO FEDERAL, ESTADOS, MUNICÍPIOS, ALTERAÇÃO, ATIVAÇÃO, ARTEFATOS, EXPLOSIVOS, DIVULGAÇÃO, MATERIAL, PORNOGRAFIA, RADIODIFUSÃO, IMAGEM VISUAL, CONTESTAÇÃO, ADULTERAÇÃO, DADOS, SEGURANÇA NACIONAL, INTERVENÇÃO, SISTEMA, CONTROLE, AUMENTO, INDUÇÃO, ATO ILÍCITO, ATENTADO, SOBERANIA NACIONAL, TIPICIDADE, CRIME, AUMENTO, PENA DE DETENÇÃO.
Despacho inicial (SF) CE - Comissão de Educação, Cultura e Esporte.
(SF) CCJ - Comissão de Constituição, Justiça e Cidadania.
Comissões CAE - Comissão de Assuntos Econômicos Relatores: Aloizio Mercadante (atual)
CCJ - Comissão de Constituição, Justiça e Cidadania Relatores: José Fogaça (encerrado em 13/01/2003 - redistribuição)
Magno Malta (encerrado em 08/03/2005 - redistribuição)
Garibaldi Alves Filho (encerrado em 11/08/2005 - redistribuição)
CE - Comissão de Educação, Cultura e Esporte Relatores: Bello Parga (encerrado em 09/05/2001 - redistribuição).
José Fogaça (encerrado em 29/10/2001 - redistribuição)
Juvêncio da Fonseca (encerrado em 22/05/2002 - parecer oferecido)
Eduardo Azeredo (encerrado em 23/06/2006 - parecer oferecido)
CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática Relatores: Eduardo Azeredo (encerrado em 05/12/2007 - parecer oferecido)[175].

SF PLS 00137 / 2000 de 11/05/2000
Autor SENADOR - Leomar Quintanilha

[175] Disponível: <http://www.senado.gov.br/sf/atividade/Materia/detalhes.asp?p_cod_mate=43555> Acesso 29 maio 2008

Ementa Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.
Indexação ALTERAÇÃO, DISPOSITIVOS, CÓDIGO PENAL, INCLUSÃO, CRIME, VIOLAÇÃO, PRIVACIDADE, DIREITO, PESSOA FÍSICA, PATRIMÔNIO, PROPRIEDADE IMATERIAL, PROPRIEDADE, INTELECTUAL, COSTUMES, CRIANÇA, ADOLESCENTE, UTILIZAÇÃO, PROCESSO, TECNOLOGIA, INFORMÁTICA, TELECOMUNICAÇÕES, MOTIVO, ABUSO, DIVULGAÇÃO, IMAGEM VISUAL, ESCRITO OBSCENO, PALAVRA, FATO, PESSOAS, FORMAÇÃO, BANCO DE DADOS, FICHÁRIO, ARQUIVO, INFORMAÇÃO CONFIDENCIAL, ALTERAÇÃO, SUPRESSÃO, FORNECIMENTO, TERCEIROS, DADOS, COMPUTADOR, (INTERNET), CORRELAÇÃO, FIXAÇÃO, AUMENTO, PENA, AGENTE INFRATOR.
Despacho inicial (SF) CCJ - Comissão de Constituição, Justiça e Cidadania.
Comissões CAE - Comissão de Assuntos Econômicos Relatores: Aloizio Mercadante (atual)
CCJ - Comissão de Constituição, Justiça e Cidadania Relatores: Roberto Freire (encerrado em 05/10/2000 - redistribuição)
José Fogaça (encerrado em 15/01/2003 - redistribuição)
Magno Malta (encerrado em 08/03/2005 - redistribuição)
Garibaldi Alves Filho (encerrado em 11/08/2005 - redistribuição)
CE - Comissão de Educação, Cultura e Esporte Relatores: Bello Parga (encerrado em 09/05/2001 - redistribuição)
José Fogaça (encerrado em 29/10/2001 - redistribuição)
Juvêncio da Fonseca (encerrado em 17/05/2002 - parecer oferecido)
Eduardo Azeredo (encerrado em 23/06/2006 - parecer oferecido)
CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática Relatores: Eduardo Azeredo (encerrado em 05/12/2007 - parecer oferecido)[176].

SF PLC 00089 / 2003 de 13/11/2003
Outros números CD PL. 00084 / 1999
Autor DEPUTADO - Luiz Piauhylino
Ementa Altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 - Código Penal e a Lei nº 9296, de 24 de julho de 1996, e dá outras providências. (Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial). (PROCESSO ESPECIAL)
Indexação NORMAS, ACESSO, PRESTAÇÃO DE SERVIÇO, REDE DE TRANSMISSÃO, COMPUTADOR, (INTERNET), PRIVACIDADE, DIREITO A INFORMAÇÃO, PESSOAL, BANCO DE DADOS, LIBERDADE, ESTRUTURAÇÃO, RESPONSABILIDADE, CONSUMIDOR, PRESERVAÇÃO, SIGILO, INFORMAÇÃO, ARMAZENAMENTO, DISPONIBILIDADE, UTILIZAÇÃO,

[176] Disponível: <http://www.senado.gov.br/sf/atividade/Materia/detalhes.asp?p_cod_mate=44045> Aceso 29 maio 2008.

USO PRÓPRIO, IDENTIFICAÇÃO, PESSOA FÍSICA, PESSOA JURÍDICA, AUSÊNCIA, OBRIGATORIEDADE, CONHECIMENTO, TERCEIROS, COLETA, PROCESSAMENTO DE DADOS, AUTORIZAÇÃO, INTERESSADO, CADASTRAMENTO, RETIFICAÇÃO, PROIBIÇÃO, DIVULGAÇÃO, INFORMAÇÕES, REVELAÇÃO, OPINIÃO, POLÍTICA, RELIGIÃO, SEXO, PORNOGRAFIA, BANCO DE DADOS. CARACTERIZAÇÃO, CRIME, INFRATOR, INFORMÁTICA, DESTRUIÇÃO, INVASÃO, BANCO DE DADOS, ACESSO, MEIO ELETRÔNICO, PROGRAMA, COMPUTADOR, (INTERNET), FRAUDE, DANOS, ADMINISTRAÇÃO PÚBLICA, VANTAGENS, VIOLAÇÃO, SENHA, DIFUSÃO, VÍRUS, PENA DE DETENÇÃO, MULTA, AGRAVAÇÃO PENAL, CRIMINOSO, EXERCÍCIO PROFISSIONAL.
Comissões CCJ - Comissão de Constituição, Justiça e Cidadania Relatores: Marcelo Crivella (atual)
CE - Comissão de Educação, Cultura e Esporte Relatores: Eduardo Azeredo (encerrado em 23/06/2006 - parecer oferecido).
CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática Relatores: Eduardo Azeredo (encerrado em 05/12/2007 - parecer oferecido)[177].

[177] Disponível: <http://www.senado.gov.br/sf/atividade/Materia/detalhes.asp?p_cod_mate=63967> Acesso 29 maio 2008.

Anexo III

HABEAS CORPUS. ROUBO TENTADO. INTERROGATÓRIO POR VIDEOCONFERÊNCIA. NULIDADE. NÃO-OCORRÊNCIA. ORDEM DENEGADA.
1. A estipulação do sistema de videoconferência para interrogatório do réu não ofende as garantias constitucionais do réu, o qual, na hipótese, conta com o auxílio de dois defensores, um na sala de audiência e outro no presídio.
2. A declaração de nulidade, na presente hipótese, depende da demonstração do efetivo prejuízo, o qual não restou evidenciado.
3. Ordem denegada.

Sustenta o impetrante, em síntese, (a) a inconstitucionalidade formal da lei estadual que prevê a possibilidade do sistema de videoconferência, "consubstanciado na invasão de competência privativa da União para legislar sobre direito processual" (fl. 03), e (b) a existência de constrangimento ilegal, pois que ao paciente "está se impedindo de exercer a plenitude do seu direito de autodefesa, já que teria sido violado seu direito de presença a todos os atos do processo" (fl. 11).

Requer a concessão de liminar, "com a anulação do ato praticado por meio de videoconferência" (fl. 11).

2. Neste exame inicial, de cognição sumária, não vislumbro os requisitos necessários para a concessão da tutela pleiteada.

Com efeito, os fundamentos do julgado impugnado – no sentido de que a "estipulação do sistema de videoconferência para interrogatório do réu não ofende as garantias constitucionais do réu" – mostram-se relevantes e, num primeiro momento, sobrepõem-se àqueles lançados na petição inicial.

Neste aspecto, anoto que, em hipótese análoga a dos presentes autos, esta Corte indeferiu pedido de liminar no HC 90.900, relator o Ministro Gilmar Mendes (DJ 02.04.2007).

Ademais, o pedido liminar formulado na inicial tem nítido caráter satisfativo, o que não recomenda o seu deferimento.

3. Ante o exposto, indefiro a liminar.

Colha-se a manifestação da Procuradoria-Geral da República.

Publique-se.

Brasília, 05 de julho de 2007.

Ministra Ellen Gracie
Presidente