Caderno Jurídico da Escola Superior
do Ministério Público do Estado de São Paulo
Ano 2 - Vol 1- n.º 4 - Julho/2002

DIREITO

E

INTERNET

ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DE SÃO PAULO

Diretor:
Luís Daniel Pereira Cintra

Assessores:
Edgard Moreira da Silva
Maria Amélia Nardy Pereira
Oswaldo Peregrina Rodrigues
Vânia Ferrari Trópia Padilla

Coordenador Editorial:
Edgard Moreira da Silva

Jornalista Responsável:
Rosana Sanches (MTb 17.993)

Capa:
Luís Antônio Alves dos Santos

LOGO
DA IMESP

IMPRENSA OFICIAL DO ESTADO

Diretor Presidente:
Sérgio Kobayashi

Diretor Vice-Presidente:
Luiz Carlos Frigerio

Diretor Industrial:
Carlos Nicolaewsky

Diretor Financeiro e Administrativo:
Richard Vainberg

Coordenador Editorial:
Carlos Taufik Haddad

Escola Superior do Ministério
Público do Estado de São Paulo
R. Minas Gerais, 316 - Higienópolis
CEP 01244-010. Telefones: (11) 3017-7776,
3017-7777; fax: (11) 3017-7754.
e-mail: esmp@mp.sp.gov.br

Imprensa Oficial do Estado
R. da Mooca, 1.921 - Mooca - CEP 03103-902.
Tel. (11) 6099-9446; fax.: (11) 6692-3503.
www.imprensaoficial.com.br
imprensaoficial@imprensaoficial.com.br
SAC 0800-123401

"Caderno Jurídico", co-edição ESMP/Imprensa Oficial do Estado, é trimestral, com tiragem de 3 mil exemplares.

ÍNDICE

APRESENTAÇÃO

Estamos levando aos colegas de Ministério Público e à comunidade jurídica em geral, o primeiro Caderno Jurídico de nossa gestão à frente da diretoria da Escola Superior do Ministério Público do Estado de São Paulo.

Dentro da filosofia que implantamos na direção da ESMP no início do ano, particularmente voltada para a concretização dos objetivos institucionais da Escola Superior, com lastro no profissionalismo e eficiência, procuramos selecionar uma temática nova e ainda não estudada com profundidade no seio de nossa Instituição.

A informática e a internet, na estrutura material, já fazem parte do cotidiano do promotor de Justiça para o desenvolvimento de seu mister institucional.

Todavia, o *cyber* Direito ainda é uma área pouco presente na formação jurídica dos profissionais do Direito e, conseqüentemente, não ocupa o espaço que precisa no campo de conhecimento do Ministério Público.

Recentemente, no dia 10 do mês abril de 2002, a Escola promoveu um seminário sob o título de "Investigação de Crimes pela Internet", com palestra proferida pelo Dr. David Sobel, advogado do Centro de Informações sobre a Privacidade nos Meios Eletrônicos – EPIC/EUA e no National Security Archive, dos Estados Unidos da América, ocasião em que fomos despertados para a urgente necessidade de o Ministério Público, em especial de São Paulo – paradigma para todo o Brasil e para a própria América do Sul –, iniciar discussão sobre os reflexos da internet na seara jurídica e a atuação do Parquet em vista dessa nova realidade.

Assim, é com grande satisfação que apresentamos trabalhos jurídicos elaborados por membros do Ministério Público de São Paulo – Drs. Marco Antonio Zanellato, procurador de Justiça, coordenador do Centro de Apoio das Promotorias de Justiça do Consumidor (CENACON); e Augusto Eduardo de Souza Rossini, promotor de Justiça, coordenador do Centro de Apoio à Execução (CAEx), que são especialistas na temática em testilha.

Além disso, conseguimos trazer à colação estudo elaborado pelo Dr. Ciro Expedito Scheraiber, promotor de Justiça do Consumidor em Curitiba/PR, bem como do Dr. Jean Jacques Eremberg, procurador do Estado de São Paulo.

Também nos brindaram com estudos valiosos e inovadores os Drs. Marcos Costa, Renato M. S. Opice Blum e Juliana Canha Abrusio, advogados em São Paulo, pois não olvidamos o vultoso trabalho desenvolvido pela OAB/SP na elaboração de anteprojeto de lei regulando o comércio eletrônico, a assinatura digital e a validade dos documentos eletrônicos, que se encontra em tramitação no Congresso Nacional.

O tema é relevante para o Ministério Público, que não pode ficar à margem dessa nova realidade, mormente em razão das funções institucionais que lhe foram outorgadas pela Carta Magna de 1988.

Desejamos que os estudos apresentados no presente Caderno Jurídico sejam uma simples chama de um grande incêndio de debates e desenvolvimento da temática do Direito no ambiente virtual em nossa Instituição, que sempre esteve na vanguarda de todas as inovações jurídicas relacionadas ao exercício de suas funções, consoante se verificou na área dos interesses difusos e coletivos; na defesa do consumidor; na proteção do meio ambiente; no combate à improbidade administrativa etc.

No Brasil, o Ministério Público é uma luz no fim do túnel para a nossa sociedade e um cadinho de credibilidade para a população brasileira – confiança que efetivamente fizemos por merecer, pelo trabalho sério e idealista dos integrantes da Instituição.

Com mais esta edição do Caderno Jurídico, esperamos que a Escola Superior do Ministério Público esteja atendendo às expectativas e interesses, e colaborando para o aprimoramento profissional dos membros da Instituição, na busca permanente de uma atuação funcional cada vez mais eficaz.

São Paulo, Julho de 2002

Luís Daniel Pereira Cintra

procurador de Justiça,
diretor do CEAF-ESMP

INTRODUÇÃO

A informática e a internet revolucionaram a sociedade nos últimos trinta anos. Os hábitos e a forma de vida da humanidade mudaram. As transformações provocadas pela informática e pela internet na vida do ser humano são evidentes e se solidificam dia a dia, com interferência em todos os campos sociais: na cultura; na economia; na educação e, por conseguinte, atinge o campo do direito. Estamos diante de uma nova realidade – o mundo virtual convivendo com o mundo real. Hoje, o computador é um equipamento essencial para a própria sobrevivência do homem em sociedade. Aquele que não possui habilidade mínima na utilização da informática e da internet já está sendo considerado um semi-analfabeto.

A informática e a internet estão praticamente em tudo: na telefonia; na escola, na medicina, no consumo em geral, nas comunicações, na segurança pública, no automóvel, nas instituições financeiras para movimentação das contas bancárias; nos semáforos, na grande maioria dos lares do globo terrestre. Vivemos a era dos *chips*, dos *bits* e dos *bytes*.

O ser humano já não consegue mais conviver sem a informática e a internet; elas fazem parte das suas atividades diárias, tanto no campo profissional como na própria vida familiar e no lazer. No mundo hodierno, está se tornando comum a comunicação entre familiares e amigos pela internet. Os empresários realizam reuniões para tratar de questões profissionais pelo ambiente virtual, inclusive com uso, cada vez maior, do notebook. As empresas e os respectivos negócios podem ser facilmente conduzidos à distância, sem a presença física dos executivos na sede da empresa. Em muitos casos, a empresa nem existe fisicamente – ela é virtual, sediada num disco rígido de um microcomputador.

Para o Direito, essa nova realidade não pode ser desprezada, pois as conseqüências da informática e da internet no mundo jurídico são incontestáveis e totalmente diferentes do mundo físico em que nos acostumamos a viver, ou do vulgarmente “ver para crer”.

O Direito, assim, encontra-se diante de um grande desafio, algo totalmente distinto daquelas relações que se buscava regular há cinqüenta anos. O Direito sempre buscou regular relações decorrentes da realidade fática e de âmbito material. Ao

regular a arte, a propriedade intelectual, para protegê-las juridicamente, o Direito partiu do momento em que a idéia, a criação se exteriorizou no mundo concreto, isto é, quando a obra intelectual e artística se materializou no mundo fático.

Agora, principalmente em relação à internet, o Direito se vê diante de um mundo virtual, que não precisa exteriorizar-se materialmente para gerar efeitos jurídicos no mundo fático. Lidamos com *bits* e na dimensão do ciberespaço globalizado.

No mundo virtual nos encontramos diante de idéias não materializadas em átomos, mas sim diante de idéias que se propagam por meio de energia, isto é, por intermédio de impulsos eletroeletrônicos que alcançam todo o planeta Terra.

O comércio eletrônico é uma realidade na vida do ser humano. Compramos produtos sem a necessidade de nos deslocarmos aos supermercados, às livrarias, às farmácias etc. Movimentamos nossas contas bancárias e efetuamos o pagamento de nossas dívidas sem ingressarmos numa agência bancária – que pode até estar situada a milhares de quilômetros da posição física em que realizamos essa operação.

Diante da tela do microcomputador, o ser humano é capaz de concretizar dezenas de negócios jurídicos em pouco espaço de tempo e sem a necessidade de deslocamento do local que escolheu para tal empreitada, tudo isso pelo ciberespaço, plugado na internet.

O desenvolvimento no campo da informática é diário. Neste início de século, os cientistas da computação que trabalham com spintrônica – disciplina que estuda a interação da eletrônica e do magnetismo –, estão pesquisando a montagem de um computador com um só *chip*, que integraria tudo, isto é, memória de acesso randômico (RAM) e disco rígido em um único lugar, o que levaria os atuais computadores, literalmente, para o museu, ou mesmo para a lata do lixo.

O Direito precisa acompanhar essa nova realidade – a ERA DA SOCIEDADE DIGITAL – e estabelecer a regulação pertinente, mas tal empreitada deve vir antes que a informática e a internet se transformem em feras indomáveis, a recriação contemporânea da Hidra de Lerna da mitologia grega, que conseguiu destruir o "invencível" Hércules.

Portanto, antes que a liberdade do homem, sua privacidade e sua paz, bem como o próprio Direito, sejam destruídos, faz-se mister regular e monitorar juridicamente a internet.

Os noticiários dos jornais, praticamente todas as semanas, trazem informações acerca de golpes ou fraudes de ordem econômico-financeiros praticados pela internet, lesando milhares de pessoas. A habilidade dos hackers e crakers no manuseio das ferramentas de informática e de acesso a lugares tidos como intransponíveis por via da internet tem levado as grandes empresas de software e os cientistas da computação a investirem elevados recursos e enorme talento em pesquisas para prevenir as condutas delituosas no mundo virtual.

As grandes corporações bancárias e instituições financeiras investem, anualmente, milhões de dólares na área de segurança, particularmente no desenvolvimento da tecnologia de informática e na criação de instrumentos de criptografia de dados e de acesso à movimentação de recursos financeiros.

Não é admissível que a comunidade jurídica limite-se a correr atrás de soluções paliativas e facilmente suplantadas pelos avanços diários da tecnologia.

O problema decorrente das relações produzidas pela Ciência do Direito e da Informática deve ser amplamente conhecido e avaliado pela comunidade jurídica e pelo legislador nacional. Este, depois da ampla discussão jurídica e legislativa que já seguiu à problemática levantada, precisa apresentar soluções legais aptas a permitirem o reconhecimento e a segurança jurídica que os negócios e as relações jurídicas concretizadas pela internet necessitam para sua eficácia e validade plena no mundo do Direito.

Hoje, não há como negar, o comércio eletrônico já se encontra integrado à vida do consumidor brasileiro, que cada vez mais contrata a aquisição de produtos e a utilização de serviços por meio da internet, quer dentro do nosso país, quer fora dele.

Os clientes e os consumidores dos serviços bancários estão diariamente fazendo uso da internet para o pagamento de contas, transferência de recursos etc.

Os fornecedores vêm ampliando a publicidade e a comercialização de seus produtos e serviços por meio da internet, inclusive, em alguns casos, com o uso indiscriminado de *spammer* e de *cookies*.

As pessoas e as empresas nem se lembram mais da correspondência postal (serviços de cartas pelo correio), pois o *e-mail* é o instrumento ideal para as comunicações e a mantença de correspondência rápida e segura. A sociedade hodierna vivencia a *cyber* cultura, em que uma nova civilização está em criação, na qual os *bits*

constituem a estrutura central das relações humanas. O computador e a internet são praticamente essenciais à vida do homem e à existência da própria sociedade. As relações desatrelam-se do meio físico e passam a ter existência própria no ambiente virtual. Por isso mesmo, os interesses jurídicos e, portanto, os direitos e deveres deles decorrentes passam a ter como objeto a própria mensagem ou informação e não mais o meio físico onde inseridas.

No campo processual, principalmente na esfera criminal, o Poder Judiciário vem, paulatinamente, reconhecendo a validade e a viabilidade do interrogatório à distância de réus presos em outras comarcas e Estados, ou seja, pelo meio eletrônico proporcionado pela internet e pelo desenvolvimento das tecnologias de informática. Além disso, alguns tribunais do país admitem a interposição de recursos por intermédio do correio eletrônico. A grande maioria dos tribunais já possibilita o acesso e a consulta de processos pela internet.

A própria imprensa oficial do Estado de São Paulo, atualmente, fornece e disponibiliza aos advogados, pelo correio eletrônico, serviço de informação da publicação dos atos judiciais que são veiculados pelo Diário Oficial do Poder Judiciário de São Paulo (denominado, antigamente, serviços de recortes) .

Em face da expansão da internet e, particularmente, do uso de *e-mail*, a temática da privacidade está na ordem do dia na doutrina jurídica. O direito à privacidade, como supedâneo da personalidade, deve receber proteção jurídica no ambiente virtual, visto que a Constituição Federal assegura a sua inviolabilidade. Por isso, a legislação futura precisa estabelecer os limites protetivos da privacidade no ambiente cibernético, bem como das comunicações em geral e de dados pessoais, inclusive no ambiente laboral, ainda que se verifique eventual utilização indevida ou contrária às normas e determinações da contratação trabalhista e funcional. O empregador poderia ter acesso ou violar correspondência pessoal de seus empregados em decorrência do abuso no uso da internet pelos computadores da empresa? E o sigilo de informações empresariais, na hipótese de empregados repassá-las a terceiros como se correspondência particular fosse?

Toda essa problemática jurídica e questões decorrentes do uso da informática e internet afligem a comunidade jurídica. No Congresso Nacional tramitam vários projetos de lei a respeito da matéria, mas não se define uma legislação básica, consoante se implementou nos Estados Unidos e nos países da União Européia.

A própria ONU, preocupada com a problemática das relações estabelecidas no ambiente virtual, editou, por intermédio da UNCITRAL, um modelo de legislação padrão para orientar os países na confecção de suas legislações internas e de tratados internacionais.

O Centro de Estudos e Aperfeiçoamento Funcional – Escola Superior do Ministério Público não poderia ficar ausente da discussão dessa relevante temática e, no presente Caderno Jurídico, procura trazer à discussão algumas das questões mais relevantes para a regulação das relações jurídicas no ambiente virtual.

A internet, desde seu surgimento como uma tecnologia militar norte-americana no final dos anos cinqüenta, em plena guerra fria, a denominada ARPANET, vem se desenvolvendo de forma avassaladora e praticamente incontrolável, razão pela qual o Direito precisa estabelecer regras próprias e adequadas para regular os interesses jurídicos dela decorrentes.

Em estudo muito interessante, o ilustre Dr. Marcos Costa (integrante da Comissão da OAB/SP que elaborou o anteprojeto de lei sobre comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital), realiza exame profundo do conceito, da autenticidade, da integridade e da validade jurídica do documento eletrônico em face das disposições estabelecidas pela Medida Provisória nº 2.200-2, de 24 de agosto de 2201, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira. Valiosa a proposta de *lege ferenda* apresentada ao final do aludido estudo, principalmente no que tange à supressão de lacunas constatadas na Medida Provisória 2.200/2001 e de inconstitucionalidades detectadas em seu contexto, mormente falhas legislativas no que tange ao ônus da prova em caso de impugnação do documento eletrônico, da noção de assinatura digital e às formas de certificação dos documentos eletrônicos.

O Direito Autoral Eletrônico, inegavelmente um problema de difícil solução para o Direito, é objeto do trabalho apresentado pelos insignes advogados e professores Renato M. S. Opice Blum e Juliana Cunha Abrusio.

O Dr. Renato Opice Blum é um especialista na área do Direito Eletrônico, com inúmeros artigos acerca da matéria já publicados em revistas jurídicas e obras coletivas, destacando-se o livro “Direito Eletrônico – A Internet e os Tribunais”, São Paulo, EDIPRO, 2001.

No mencionado artigo jurídico, os autores desenvolvem brilhante estudo acerca da inter-relação entre a legislação que proporciona proteção jurídica ao software (Lei

n.º 9.609/98) e a legislação disciplinadora do direitos autorais, artísticos e da propriedade intelectual (Lei n.º 9.610/98). A pirataria de obras intelectuais legalmente protegidas e disponibilizadas na internet é objeto de abordagem doutrinária e prática, trazendo à colação sentença judicial proferida pelo Juízo da 12.ª Vara Cível do Rio de Janeiro sobre a questão, que se constituiu num verdadeiro paradigma em relação à temática da reprodução ou utilização indevida e sem autorização de *softwares* e obras disponibilizadas na internet.

Na seara do Direito, temos verificado que os juristas temem a pirataria ou plágio de seus trabalhos disponibilizados na internet, fato que vem impedindo que doutrinadores de vulto divulguem seus estudos no mundo virtual. Daí a importância do artigo acerca da proteção do direito autoral eletrônico.

Um dos temas mais palpitantes do momento – a publicidade na internet –, é objeto de estudo elaborado pelo Dr. Jean Jacques Erenberg, procurador no Estado de São Paulo e especialista em Interesses Difusos e Coletivos pela Escola Superior do Ministério Público de São Paulo. Após pequeno bosquejo histórico da publicidade na internet, o autor indica e comenta diversas hipóteses de publicidade patológica verificadas na internet, destacando-se os casos de *spamming* – envio de milhões de *e-mails* indiscriminadamente; omissão de informações essenciais em publicidades veiculadas via internet; a obstrução de saída – *sites* que não oferecem opção de retorno à página anterior, obrigando os internautas a se desconectarem ou até mesmo desligar o microcomputador para sair do *site* acessado; publicidade subliminar; desrespeito à privacidade; publicidade em ambiente indevido (salas de *chat* ou *newsgroup*); insinceridade de *link* etc. A expansão da publicidade por meio da internet e a ampliação do comércio eletrônico, embora o Código de Defesa do Consumidor estabeleça regras que alcançam tais condutas, merecem uma regulamentação específica, a fim de prevenir e reprimir condutas antiéticas e ilícitas praticadas no mercado de consumo.

O eminente promotor de Justiça do Consumidor de Curitiba/PR, Dr. Ciro Expedito Scheraiber, sob o título "*Mailing Lists* e Direito do Consumidor", traz à colação estudo inédito e interessante como decorrência do comércio eletrônico. Empresas especializadas – *list brokers* – formam listas de endereços eletrônicos contendo mais de cem milhões de consumidores e as vendem ou alugam a fornecedores de produtos e serviços interessados, cobrando cerca de 120 dólares para cada mil nomes alugados. Essas malas diretas em números e volumes inimagináveis proporcionaram, nos Estados Unidos, no ano de 2000, a arrecadação de mais de 30 bilhões de dólares.

Para os fornecedores de produtos e serviços de consumo, essas listas constituem um instrumento fácil e barato de acesso ao consumidor, pois, em geral, elas informam o perfil do consumidor, suas expectativas, desejos e interesses pessoais de consumo, razão pela qual as ofertas são direcionadas e aptas a proporcionar retorno certo para o empresário. O Direito do Consumidor e o ordenamento jurídico brasileiro não podem ficar à margem desse fato, pois os *mailing lists* constituem um instrumento poderosíssimo de dominação de mercados e de criação de falsas necessidades no mercado de consumo, de modo que as empresas mais fortes economicamente conseguem induzir os consumidores a adquirirem determinados produtos ou a utilizarem certos serviços em vista de dominar informações valiosas do perfil obtido através das listas eletrônicas. Elas podem configurar não só uma prática abusiva, como são aptas a eliminar a própria concorrência em alguns setores da economia.

Em alentado e proeminente trabalho jurídico, o Dr. Marco Antonio Zanellato, procurador de Justiça em São Paulo, brinda-nos com estudo acerca das Condutas Ilícitas na Sociedade Digital. Aludido estudo decorre detalhadamente sobre as variadas espécies de práticas ilícitas mais comuns na intenet, como os *Cookies*; os *Spywares*; os *Spamming*; os *Hoaxes*; os *Sniffers*; os *Trojan Horses*; os *Blackdoors*; o uso perigoso dos *browsers* na internet; a atuação dos *Hackings* e *Crackings*, seus métodos e artimanhas para aproveitar vulnerabilidades da navegação na internet. O trabalho expõe, ainda, acerca da situação atual dessas práticas no Brasil e a necessidade de regulação, oferecendo interessantes propostas no âmbito legislativo, no âmbito deontológico e até formas de auto-proteção para a defesa dos usuários em sua navegação na internet e para a sobrevivência da própria sociedade digital.

Por fim, tratando-se de Ministério Público, não poderia ser olvidada uma abordagem específica acerca dos crimes ou delitos informáticos. Embora denominasse seu tema de Brevíssimas Considerações sobre Delitos Informáticos, o Dr. Augusto Eduardo de Souza Rossini, promotor de Justiça, autoridade na matéria – sua tese de doutorado versa o tema dos delitos informáticos –, apresenta ampla abordagem de condutas criminosas mais comuns no mundo virtual, as quais já são objeto de enfrentamento pelo Ministério Público no dia-a-dia forense. O conceito de delito informático e o bem jurídico tutelado são examinados numa visão diferente daquela estudada no Direito Penal Clássico, evidenciando a necessidade de adaptação dos princípios e regras do direito criminal (penal e processual penal, inclusive no campo da investigação) a essa nova realidade, o mundo sem referências físicas, a sociedade digital.

Os reflexos da internet no Direito são incontestáveis e irreversíveis, já estão no nosso dia-a-dia. A internet constitui um grande desafio para a Ciência Jurídica nesse limiar de século XXI, pois sua influência nas relações jurídicas e os interesses jurídicos que gera são totalmente diferentes do direito tradicional. Estamos diante de um Direito Virtual, ou Direito da Internet, em os aspectos jurídicos exigem soluções inovadoras no campo contratual; na temática da responsabilidade civil; na proteção da privacidade, dos direitos autorais e da propriedade intelectual; no mercado dos valores imobiliários; na punição dos delitos informáticos; na própria segurança jurídica etc.

O jurista contemporâneo precisa se abrir para o mundo virtual, bem como observar e refletir o Direito do século XXI pela tela do computador e da conexão via internet, sob pena de se autocondenar às trevas da seara jurídica.

Assim, a Escola Superior do Ministério Público, a exemplo do que realizou com o seminário “Investigação de Crimes pela Internet”, no mês de abril de 2002, procura levar aos membros do Parquet paulista, bem como de outros Estados da Federação, estudos sobre internet e direito, abrindo a “tela do computador” para a discussão dessa relevante temática no âmbito do Ministério Público.

Edgard Moreira da Silva,

promotor de Justiça,
assessor do CEAF/ESMP

PARTICIPANTES DA OBRA

Augusto Eduardo de Souza Rossini, promotor de Justiça, coordenador do Centro de Apoio à Execução (CAEX), professor de Direito Penal, mestre e doutorando em Direito Penal.

Ciro Expedito Scheraiber, promotor de Justiça de Curitiba, Paraná.

Jean Jacques Erenberg, procurador do Estado de São Paulo, professor de Prática Jurídica na Universidade Cidade de São Paulo, especialista em Interesses Difusos e Coletivos pela ESMP.

Juliana Canha Abrusio: advogada; membro da Associação Brasileira de Direito de Informática e Telecomunicações (ABDI); coordenadora de Grupo de Estudos e Pesquisa em Comércio Eletrônico; palestrante convidada do I Congresso da Comunidade Andina para o Desenvolvimento do Comércio Eletrônico dos Países Membros; autora das Monografias “Aspectos Jurídicos do Comércio Eletrônico” e “Contratos Eletrônicos e a Assinatura Digital”.

Marco Antonio Zanellatto, procurador de Justiça e coordenador do Centro de Apoio Operacional das Promotorias de Justiça do Consumidor; mestre em Direito Civil pela USP, professor de Direito do Consumidor na FAAP-MBA e na ESMP.

Marcos Costa, advogado; conselheiro da OAB-SP; presidente da Comissão Nacional de Informática do Conselho Federal da OAB; presidente da Comissão de Informática Jurídica da OAB-SP.

Renato M. S. Opice Blum: advogado e economista; professor coordenador de pós-graduação em Direito Eletrônico; fundador e conselheiro do Instituto Brasileiro de Política e Direito da Informática (IBDI); presidente do Comitê de Direito da Tecnologia da Câmara Americana de Comércio (AMCHAM); membro da Comissão de Informática Jurídica da OAB/SP e do Conselho de Comércio Eletrônico da Federação do Comércio/SP; autor/colaborador das obras: “Direito Eletrônico - a Internet e os Tribunais”, “Comércio Eletrônico”, “Direito & Internet - aspectos jurídicos relevantes”, “Direito da Informática - temas polêmicos”, “Responsabilidade Civil do Fabricante e Intermediários por Defeitos de Equipamentos e Programas de Informática”, “O Bug do Ano 2000 - aspectos jurídicos e econômicos”.

A ICP-BRASIL E OS DOCUMENTOS ELETRÔNICOS

Marcos Costa

A ICP-BRASIL E OS DOCUMENTOS ELETRÔNICOS

Marcos Costa

I – O DOCUMENTO ELETRÔNICO E A ASSINATURA DIGITAL

1. A informática tem causado quebra de numerosos paradigmas, em todos os ramos da ciência humana, inclusive no direito, dentre os quais, um dos exemplos mais marcantes, é o documento eletrônico, gerado, transmitido, acessado e armazenado em sua forma original, constituída por *bits*, sem necessidade de sua impressão em papel.

2. Os homens há muito têm procurado alternativas ao papel para perenizar suas informações.

Primeiro, pela pouca resistência do papel às ações do tempo, das traças, das intempéries e de sinistros.[1]

Depois, pela dificuldade em recuperar documentos, especialmente se guardados em grande volume.

Um terceiro ponto é o elevado custo para armazenamento de documentos em papel, levando o Estado e o setor privado a manterem enormes espaços para sua

[1] O desembargador paulista Sylvio do Amaral, em nota introdutória de sua obra Falsidade Documental (4ª edição, revisada por Ovídio Rocha Barros Sandoval, Editora Millennium, página 1), transcreve Papini, na afirmação de que "... toda a sociedade – pelo menos nos seus elementos mais delicados e essenciais – está ligada à matéria mais frágil que existe: o papel... nada de resistente e duradouro: um pouco de pasta de madeira e de cola, substâncias deterioráveis e combustíveis, é a que confiam os bens e direitos dos homens, os tesouros da ciência e da arte. A umidade, o fogo, a traça, os ratos, podem desfazer e destruir essa massa imensa de papel sobre que repousa o que há de mais caro no mundo. Símbolo de uma civilização que sabe será efêmera, ou de incurável imbecilidade."

guarda. O custo desse armazenamento, aliás, acaba por ser pago por toda a sociedade, seja através de impostos ou taxas, no caso do Estado, seja por compor preços de produtos e serviços, em se tratando de empresas.

E, finalmente, a própria consciência que a sociedade passou a ter, da necessidade de preservação do meio ambiente, considerando aqui o impacto que sobre ele tem a produção mundial de papel.

3. A tecnologia vinha tentando oferecer alternativas para o documento em papel. Exemplos disto são a microfilmagem e a digitalização de documentos.

O problema é que essas soluções não conseguiam dispensar o papel na emissão de documentos, mas apenas permitir armazenamento mais eficaz de sua cópia eletrônica.

E, pior, sequer conseguiam dispensar a guarda do documento original, já que conseguem apenas produzir cópias, que à evidência não têm o mesmo valor como prova judicial.[2] [3]

---

[2] A propósito da microfilmagem, verifique-se que a Lei nº 5.433, de 8 de maio de 1968, que regula a microfilmagem de documentos oficiais e dá outras providências, a par de dispor, no § 1º, art. 1º, que os microfilmes de que trata a lei (microfilmagem de documentos particulares e oficiais arquivados, estes de órgãos federais, estaduais e municipais – *caput* do art. 1º), estabelece, no § 1º do art. 3º, que "decreto de regulamentação determinará, igualmente, quais os cartórios e órgãos públicos capacitados para efetuarem a microfilmagem de documentos particulares, bem como os requisitos que a microfilmagem realizada por aqueles cartórios e órgãos públicos devem preencher para serem autenticados, a fim de produzirem efeitos jurídicos, em juízo ou fora dêle, quer os microfilmes, quer os seus traslados e certidões originárias." . Daí porque, ou bem as empresas mantêm os documentos físicos, armazenando-os juntamente com as cópias microfilmadas, ou bem, para eliminá-los, devem se servir de serviços notariais ou órgãos públicos correlatos para que as cópias produzam, nos termos da lei, os mesmos efeitos jurídicos, em juízo ou fora dele, do documento original.

Mesmo aqui, porém, há um nítido erro conceitual. Os serviços notariais podem outorgar segurança quanto a ser a cópia fiel ao documento original. Mas o problema pode estar no documento, e não na cópia que o espelha. Imaginemos um documento original que tenha seu conteúdo falsificado, incluindo-se, ou extraindo-se, informações. A cópia apenas reproduzirá essa adulteração que, dependendo da qualidade, só será possível identificar por meio de perícia realizada diretamente sobre o documento original. A cópia, sob esse aspecto, não pode ter o mesmo valor probante do original, ainda que autenticada por notário.

[3] Sobre digitalização de documentos, destaque-se o Projeto de Lei 3173/97, na Câmara dos Deputados (originalmente, Projeto de Lei do Senado 22/96, do Senador Sebastião Rocha, que dispõe sobre os documentos produzidos e arquivados em meio eletrônico e dá outras providências.

O referido PL, na versão aprovada no Senado e encaminhada à Câmara dos Deputados, confunde documentos gerados com os copiados para meio eletrônico, dispondo, o § 2º do art. 1º, inclusive, que "os registros originais, independentemente de seus suportes ou meio onde forem gerados, após serem arquivados eletronicamente poderão, a critério da autoridade competente, ser eliminados ou transferidos para outro suporte e local, observada a legislação pertinente." Ora, não há sentido em facultar-se a eliminação do documento eletrônico pela existência de cópia eletrônica sua. Aliás, uma das características do documento eletrônico é que por se constituir em um conjunto de bits, tem, na sua cópia, as mesmas características do original.

Da mesma forma como ocorre com a Lei de Microfilmagem, na crítica apresentada na nota anterior, também aqui, no PL, se pretende, no § 4º do art 1º, que "terão valor probante, em juízo ou fora dele, as reproduções obtidas do sistema de arquivamento eletrônico, desde que sejam perfeitamente legíveis, e fiéis aos respectivos registros originais e atendam ao decreto regulamentador específico." Ora, como cópia, apenas reproduzem o original. Mas se o próprio original, em papel, sofreu adulteração, a cópia espelhará também a fraude cometida, sem permitir, contudo, com o mesmo alcance e eficácia, sua constatação por perícia.

4. A questão é que qualquer documento, para ter valor de prova, deve atender a pelo menos três requisitos:

a. autenticidade, no sentido de permitir identificar sua autoria;

b. integridade, quanto ao controle de eventuais alterações, depois de gerado o documento;

c. acessibilidade, em relação às informações nele contidas.[4]

Um texto gerado em computador, e mantido em sua forma original, eletrônica, não conseguia cumprir àqueles dois primeiros requisitos. Isto porque não havia como vinculá-lo a alguém, como ocorre, por exemplo, em textos lançados em papel, que contenham assinatura física e, em sendo uma seqüência binária, poderia sofrer a qualquer momento modificação, sem que se saiba que sua integridade foi comprometida.

Em 1975, dois professores da Universidade de Stanford, Martin Hellman e Whitfield Diffie[5], no entanto, procurando resolver um dos mais difíceis problemas da criptografia, qual seja, a distribuição da chave criptográfica, sem que pessoas desautorizadas pudessem ter conhecimento dela, descobriram uma solução que iria modificar a estrutura e os paradigmas do documento: a criptografia assimétrica.

5. A criptografia tradicional, milenar, é a ciência de encriptar informações, de forma que somente seu autor e o destinatário por ele definido tenham acesso ao seu conteúdo.

Exemplo tradicional é o de Júlio César, que codificava as mensagens que enviava aos seus comandados, atribuindo a cada letra, a sua correspondente três casas acima na ordem alfabética.[6]

A criptografia tradicional permite sigilo de informações, mas não serve para gerar documentos para efeito de provas, já que tanto o signatário quanto o destinatário

---

[4] Não é comum a doutrina mencionar esse terceiro requisito, mas é importante notar que um documento que não permita conhecer seu conteúdo não pode ter valor judicial. Verifique-se, por exemplo, a regra constante do art. 157 do Código de Processo Civil, que determina que um documento escrito em língua estrangeira só pode ser junto aos autos quando acompanhado de versão em vernáculo, firmada por tradutor juramentado. No documento eletrônico, onde o uso da criptografia se torna cada vez mais comum, e essencial, é possível criptografar documentos com chaves de sigilo impedindo que terceiros, mesmo um juiz, possam ter acesso ao seu conteúdo. Verifique-se, nesse sentido, o disposto no art. 166, 2, do Código de Processo Penal de Portugal, que determina: "Artigo 166.º (Tradução, decifração e transcrição de documentos) 2 - Se o documento for dificilmente legível, é feito acompanhar de transcrição que o esclareça, e se for cifrado, é submetido a perícia destinada a obter a sua decifração."

[5] Sobre a história da descoberta da criptografia assimétrica, ver "O Livro dos Códigos: A Ciência do Sigilo – do antigo Egito à Criptografia Quântica" (The Code Book, no original), de Simon Singh, importante estudo sobre a evolução da criptografia até os dias atuais (Editora Record, Tradução de Jorge Calife).

[6] Essa cifragem é conhecida como *Cifra de César*.

precisam conhecer em conjunto os segredos para encriptação e decriptação da mensagem. E, se dois compartilham o segredo, um terceiro que receba a mensagem já não saberá, com segurança, qual deles a encaminhou.

Já a criptografia de chaves públicas se diferencia da tradicional porque agrega a possibilidade de geração de assinaturas digitais, pelo fato de operar com duas chaves, uma privada, e outra pública. A denominação privada tem o significado de confidencial; a pública, de conhecimento público.

6. Assinatura digital é o resultado do emprego do sistema criptográfico de chaves públicas, gerando um conjunto de *bits* que, dependendo do sistema empregado, pode constituir um arquivo em separado ou ser integrante do próprio corpo do documento eletrônico, e que é inter-relacionado ao documento de tal forma que se ele sofrer qualquer alteração a assinatura será invalidada. A assinatura digital é gerada usando de determinada chave privada. Essa assinatura só poderá ser conferida pela chave pública a ela correspondente.

7. É de se notar que a assinatura digital não é única por pessoa, como o é a assinatura física. Ela é única por documento, porque é gerada a partir de seu conteúdo. No caso, será único por pessoa o par de chaves criptográficas que gerará e conferirá a assinatura.

Se uma assinatura digital for validada por determinada chave pública é porque foi gerada pela chave privada a ela inter-relacionada. Isto porque os sistemas criptográficos partem de cálculos algorítmicos extremamente complexos, de forma, de um lado, a confirmar o inter-relacionado das duas chaves, ou seja, só a chave pública gerada simultaneamente com a privada pode validar uma assinatura e, de outro, a impedir que, a partir da chave pública, se possa calcular a chave privada correspondente.

A literatura, a propósito, afirma que se todos os computadores do mundo pudessem ser usados para processar simultaneamente uma informação, demorariam séculos para conseguir descobrir a chave privada, sigilosa, a partir da pública.

8. O surgimento, pois, da assinatura digital, passou a permitir que arquivos gerados em computador pudessem ser reconhecidos como documentos em sua forma original, eletrônica, sem necessidade de impressão no papel. [7]

---

[7] Augusto Tavares Rosa Marcacini, que no país foi provavelmente quem primeiro se interessou pela questão, dentro de sua formação acadêmica de mestre e doutor em processo civil, assim define, com precisão, o conceito de documento eletrônico: "Uma seqüência de *bits* que, traduzida por meio de determinado programa de computador, seja representativa de um fato" (em "Direito e Informática – Uma Abordagem Jurídica sobre Criptografia", Editora Forense, página 66).

II – A CERTIFICAÇÃO ELETRÔNICA

9. Como antes mencionado, se uma assinatura digital for validada por determinada chave pública é porque foi gerada a partir da chave privada a ela correspondente: sabendo-se a quem pertence determinada chave pública, saber-se-á quem é o titular da chave privada que assinou digitalmente o documento.

10. É preciso considerar, porém, que o mundo digital é um mundo globalizado, em que contratos são firmados entre pessoas que não raras vezes nunca se viram e que podem, inclusive, morar em cidades, estados, países ou continentes diferentes.

Assim, é comum a situação de alguém receber um documento assinado digitalmente, mas não ter como conferir se o emissor é realmente quem se apresenta ser.

11. As comparações com o meio físico são sempre imperfeitas, já que as premissas são diferentes, mas servem, ao menos, para ilustrar alguns preceitos do meio eletrônico.

No caso da titularidade da chave pública, a comparação possível é a de uma assinatura física, da qual não se conhece o autor, ou a assinatura dele.

No documento tradicional, em papel, é possível recorrer-se a alguém em quem se confia para atestar a titularidade da assinatura. Requer-se, por exemplo, seu reconhecimento por notário, ou o abono dela por um banco.

Confia-se no notário porque ele tem fé pública. Confia-se no abono bancário porque o banco tem fé privada.

A fé pública decorre da condição de agente estatal do subscritor da declaração e é pautada em processos burocráticos, que reclamam preciso controle sobre o fato a ser atestado; arquivamento de documentos que comprovam esses fatos; continuidade das atividades; e responsabilidade, civil e penal do agente.

Já a fé privada decorre da capacidade da pessoa física ou jurídica de direito privado em conquistar a confiança da sociedade. É pautada, basicamente, na adoção de procedimentos seguros para atestar o fato em questão, e na possibilidade de reparação de danos que a mesma vier a causar. Confia-se tradicionalmente no abono bancário, pela presunção de que o banco adota procedimentos corretos para identificação de seu cliente, e da assinatura dele, e na capacidade financeira que tem o banco em arcar com prejuízo que eventual declaração incorreta venha a causar.

12. No caso das certificações digitais, também é possível socorrer-se a um terceiro de confiança para atestar a titularidade de determinada chave pública. A esse terceiro de confiança dá-se o nome de Entidade Certificadora ou Autoridade Certificadora.

A certificação, é importante notar, não recai sobre a assinatura, mas sim sobre a chave pública. Novamente buscando similaridade com o mundo real, seria como se a certificação recaísse sobre a caneta, e não sobre a assinatura. Por essa razão, toda a vez que alguém com certificado assinar digitalmente um documento, ele já estará automaticamente certificado, sem necessidade de requerer um novo certificado a cada assinatura – algo como se toda a assinatura que saísse de determinada caneta já contivesse reconhecimento de firma.

13. As certificadoras utilizam um conjunto de equipamentos, sistemas e profissionais qualificados, estruturados por procedimentos de segurança, para emissão e controle de validade dos certificados. Esse conjunto se denomina Infra-Estrutura de Chave Pública, ou simplesmente ICP. [8]

Uma infra-estrutura tecnológica é constituída por um conjunto de equipamentos, *softwares* e mão-de-obra especializada, estruturado a partir de procedimentos lógicos adequados, para assegurar confidencialidade, integridade e acessibilidade a informações. Existem diversos exemplos de infra-estruturas tecnológicas.

Uma infra-estrutura de uma pequena empresa, para colher armazenar e processar seus dados financeiros, assegurando-lhe confidencialidade e integralidade, é um exemplo de infra-estrutura tecnológica.

Outro exemplo: uma infra-estrutura para repositório de acórdãos de determinado tribunal, para assegurar integridade e acessibilidade pelos magistrados e por advogados.

Outro ainda: aquela destinada à arrecadação tributária, que envolve geração, transmissão, tratamento e armazenamento adequados de arquivos com recolhimentos de tributos.

A implantação de uma infra-estrutura tecnológica tem natureza administrativa e considera fatores e especificações próprios de sua finalidade, bem como quem irá constituí-la e acessar suas informações. A maior ou menor dimensão e complexidade delas estão interligadas a aspectos individuais, como o nível crítico das informações,

---

[8] A expressão Infra-Estrutura de Chave Pública tem origem na expressão inglesa *Public Key Infrastructure – PKI.*

se são mais ou menos sensíveis, tempo de armazenamento, acessibilidade, capacidade de investimento etc.

Uma infra-estrutura de chaves públicas não foge a essa regra, tendo por objetivo a correta emissão e distribuição dos certificados, e controle de validade.

Basicamente, a ICP tem por objetivo assegurar que os certificados sejam emitidos de forma adequada, dentro dos parâmetros a que se propõem. Para tanto, são adotadas medidas de segurança visando assegurar confidencialidade da chave privada da certificadora, que assinará os certificados, para impedir que terceiros o façam em nome dela.

14. As certificadoras empregam diferentes tipos de procedimentos para identificação de titularidade de chaves públicas, que geram diferentes níveis de certificados.

Esses níveis diferentes de certificados acabam por diferenciar a responsabilidade das certificadoras, no caso de o titular da chave não ser realmente quem o certificado indicar.

Existem certificados emitidos por mera solicitação realizada por mensagem eletrônica, sem qualquer contato pessoal do solicitante com a certificadora. Não raras vezes, os solicitantes se encontram, inclusive, em países diferentes das próprias certificadoras. Do ângulo da qualidade para efeito de comprovação da titularidade da chave pública, esse tipo de certificado não agrega eficácia alguma, já que qualquer um pode configurar seu sistema de transmissão de mensagens eletrônicas em nome de outrem.

Outros certificados são emitidos mediante confronto de informações fornecidas pelo solicitante, com informações que sobre ele detém a certificadora. As certificadoras que trabalham com esse tipo de certificados adquirem no mercado informações privadas de pessoas. Depois, confrontam essas informações com aquelas que o pretendente de um certificado apresenta. Se essas informações coincidirem, o certificado será emitido. Naturalmente, esse tipo de certificado agrega segurança um pouco maior do que o nível anterior, onde sequer esse confronto existe. Mas não tem qualidade suficiente para gerar eficácia jurídica perante terceiros, já que também o solicitante pode apresentar-se em nome de terceiro, apontando dados que dele detenha.

Existem, ainda, certificados que são emitidos com o comparecimento pessoal do solicitante perante a certificadora, que faz a sua identificação, extrai cópia de seus documentos para arquivamento, e requer a assinatura física dele, em um termo no

qual declara ser titular de sua chave pública. Esse certificado, por representar uma identificação mais precisa do solicitante, é o único que pode representar algum tipo de eficácia para efeito jurídico. [9]

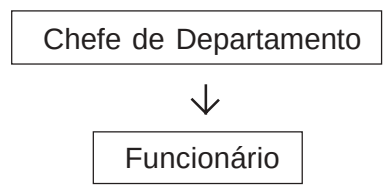
15. Considerando que as certificadoras têm, muitas vezes atuação global, para que pudessem emitir esse tipo de certificado, com identificação pessoal, em todo o mundo, foram criadas as figuras das entidades de registro, ou autoridades de registro, que têm exatamente a finalidade conferir os dados do solicitante, permitindo, assim, ampliação da área territorial de autuação das próprias certificadoras.

Além disto, existem certificadoras que, para maior segurança, socorrem-se de declarações emitidas por notários ou, nos países em que eles não existem, de entidades com o mesmo perfil, no sentido de que o solicitante compareceu pessoalmente a um desses órgãos e declarou-se titular de determinada chave pública. Os certificados assim emitidos têm a vantagem de estar baseados em declarações de titularidade com fé pública, com as presunções jurídicas a ela inerentes.

16. Esses diferentes níveis de certificados, e os procedimentos adotados pela sua emissão, são declarados ao público em geral, pelas certificadoras, através de sua "Declaração de Práticas de Certificação". Nela, a certificadora informa ainda a responsabilidade que se dispõe a assumir perante aqueles que aceitarem seus certificados, em caso de emissão incorreta dos mesmos.

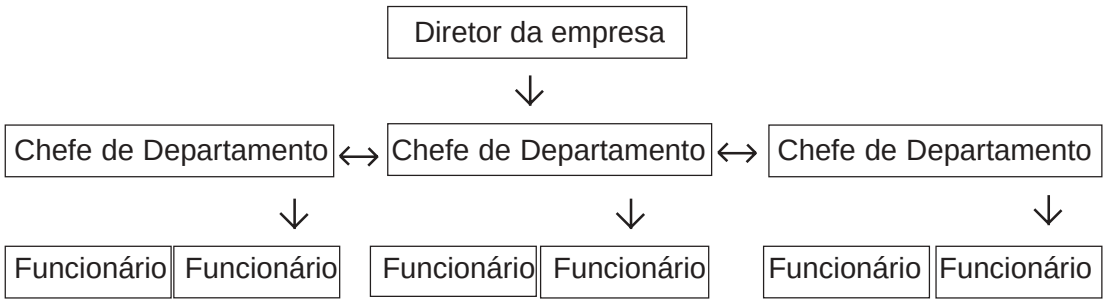
17. Outro dado importante a ser exposto, no contexto das certificações eletrônicas, é que, por basearem-se em sistemas de confiança, podem, a partir de uma estrutura hierárquica, contar com um número maior de usuários que aceitem os certificados.

Como exemplo, podemos citar uma estrutura administrativa de uma empresa, onde funcionários de determinado departamento confiam, por dever de subordinação, em seu chefe. Os certificados por ele emitidos, assim, são aceitos pelos funcionários daquele departamento.



[9] Usando, mais uma vez, de comparação, sempre imperfeita, com a assinatura física, mas apenas para efeito ilustrativo, esse nível diferente de certificado corresponde ao reconhecimento de assinatura por verossimilhança e ao reconhecimento presencial, sendo que apenas este último gera eficácia jurídica probante.

Outros departamentos da empresa, no entanto, sobre os quais aquele chefe não tem poder de subordinação, podem não aceitar seus certificados. Para superar isto, o mencionado chefe de departamento é certificado pelo Diretor da empresa que comanda diversos departamentos, inclusive aquele inicialmente mencionado.



Assim, todos os funcionários, de quaisquer departamentos, irão acolher certificados da estrutura, ainda que emitidos por chefe de departamento no qual não atuem, pois esse chefe, na cadeia de certificação, estará por sua vez certificado por Diretor que abrange todos aqueles departamentos.

Este exemplo, apesar de bastante simplista, visa a melhor identificar o sentido de *hierarquia de confiança*, onde a confiança do *topo da pirâmide* se transfere para todos os que estão abaixo dela.

III – A INSTITUIÇÃO DA ICP-BRASIL[10]

18. A Medida Provisória 2.200-2, de 24 de agosto de 2001, instituiu Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, com a finalidade, segundo seu art. 1º, de 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.[11]

---

[10] Existem numerosas questões técnicas envolvidas no uso da criptografia. Existem também questões de natureza política, como da confidencialidade de informações, próprias de sistemas de informação que utilizam criptografia. No âmbito deste estudo, porém, e pelas suas dimensões, não há como pretender encerrar todos os aspectos envolvidos na criação e desenvolvimento da ICP-Brasil. Por essa razão, será ele limitado àqueles pontos que me parecem mais relevantes, quais sejam, alcance e eficácia jurídica dos certificados emitidos no âmbito da ICP-Brasil.

[11] A primeira versão dessa Medida Provisória foi publicada em 27 de junho de 2001, tendo sofrido diversas modificações, sendo que, para efeito deste estudo, os comentários ficarão restritos à sua versão final.

19. Estabeleceu aquela Medida Provisória uma Chave Raiz da ICP-Brasil, o Instituto de Tecnologia da Informação[12], que passou a constituir-se em autarquia federal, com sede e foro em Brasília[13].

20. Foi criado, ainda, um Comitê Gestor, com atribuições definidas no artigo 4º da Medida Provisória 2.200-2.[14]

21. Dispõe o art. 10 daquela Medida Provisória: "Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória."

Na forma de seu parágrafo primeiro, "as declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil."

E, de acordo com seu parágrafo segundo, o disposto naquela Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

IV – ICP-BRASIL: AUTENTICIDADE E INTEGRIDADE DOS DOCUMENTOS ELETRÔNICOS

22. Dispõe a parte primeira do art. 1º da Medida Provisória nº 2.200-2, que a

---

[12] Art. 13 da Medida Provisória 2.200-2.

[13] Art. 12 da Medida Provisória 2.200-2.

[14] Art. 4º da Medida Provisória nº 2.200-2: "Art. 4º Compete ao Comitê Gestor da ICP-Brasil: I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil; II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação; III - estabelecer a política de certificação e as regras operacionais da AC Raiz; IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço; V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação; VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado; VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança."

ICP-Brasil foi criada para assegurar autenticidade, integridade e validade jurídica aos documentos eletrônicos, bem como das transações eletrônicas seguras.

23. Autenticidade, conforme antes mencionado, está relacionada à possibilidade de conhecer-se o autor de um documento. Integridade, por sua, vez, é a condição de não-alteração de um documento depois de ter sido emitido.

Tratando-se de documentos eletrônicos, autenticidade e integridade são atributos do sistema criptográficos de chaves públicas.

No plano teórico e acadêmico, a autenticidade resulta da presunção de que, considerando que as chaves criptográficas são geradas simultaneamente e que não é possível fatorar a chave pública, de forma a descobrir a chave privada, uma assinatura digital conferida por uma chave pública foi gerada obrigatoriamente pela chave privada correspondente.

Também no plano teórico e acadêmico, considerando que a assinatura digital é aplicada sobre um resumo do documento original, se ela, ao ser conferida pela chave pública, continuar a corresponder àquele resumo é porque o documento original não foi alterado.

24. Esses atributos são válidos no plano teórico, mas não o são, necessária e obrigatoriamente, efetivos no plano real.

Isto porque a validade deles está condicionada ao sistema criptográfico que irá gerar o par de chaves. Temos, atualmente, numerosos sistemas criptográficos. Alguns desenvolvidos por empresas, outros, por governos, e outros, no meio acadêmico.

Não é possível pressupor que todos esses sistemas foram escritos adequadamente, nem que nenhum deles contenha um *bug* [15]. Também não é crível que todos os sistemas observem todos os parâmetros matemáticos com precisão, e empreguem técnicas adequadas de segurança, como por exemplo, números primos em tamanho adequado para evitar fatoração, e escolhidos de forma aleatória o suficiente para evitar identificação posterior [16]. Isto, fora o risco de sistemas *maliciosos*, que possam extrair

---

[15] Jargão técnico que representa erro de programação.

[16] Daniel Balparda de Carvalho esclarece: "A geração de números aleatórios é central na prática criptográfica moderna. Isto porque, por um lado, eles são necessários como ferramentas para várias tarefas na criptografia e por outro, bons números aleatórios são relativamente difíceis de conseguir." E em seguida, afirma: "Na criptografia precisa-se dos chamados *números aleatórios criptograficamente fortes*. É impressionante como se pode facilmente ser enganado quando se trata de gerar este tipo de número. Normalmente, quando se precisa de um número aleatório na criptografia, o inimigo não pode, nem de perto, desconfiar qual o número escolhido. Se ele possuir um meio de reproduzir o processo de geração de números e/ou limitar o espaço de procura, então o número não é adequado para usos criptográficos." (em "Criptografia: Métodos e Algoritmos", Editora Express Book, página 59).

cópia da chave privada quando gerar o par de chaves, e transmiti-la ao autor do sistema, sem conhecimento do usuário.

25. Na forma do § único do art. 6º da Medida Provisória 2.200-1, "O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento."

Ora, se compete ao usuário gerar seu par de chaves, compete-lhe, também, por conseqüência, definir qual sistema irá utilizar para tanto. E, ao escolhê-lo, poderá, em tese, até por desconhecimento, optar por algum que não atenda com precisão aos parâmetros matemáticos da criptografia de chaves públicas, contenha erros de programação, ou mesmo uma função oculta que prejudique o sigilo da chave privada.

Nestas situações, os atributos de autenticidade e integridade não serão tecnicamente atendidos.

Daí a razão de nenhuma lei ter o poder assegurar, salvo se competir à autoridade definir o sistema criptográfico a ser utilizado, o cumprimento de requisitos de autenticidade e integridade de um documento eletrônico: não pode porque depende do sistema que será usado para emissão do par de chaves criptográficas, escolhido pelo usuário.

Pedro Rezende, uma das maiores autoridades civis em criptografia do país, nessa mesma linha de raciocínio, assim expôs, em artigo denominado Sistema de Pagamentos Brasileiro e ICP-Brasil: "Ora, quem pode garantir a autenticidade e a integridade de documentos em forma eletrônica são sistemas criptográficos apropriados (os de pares de chaves assimétricas – pública e privada) operando em condições adequadas, e não a norma jurídica. Em linguagem técnica, o uso do termo "Infra-Estrutura de Chaves Públicas" se refere a um conjunto desses sistemas e dos meios adequados para sua operação. Tais sistemas são propriedade de certas formas matemáticas do mundo platônico, de conhecimento público há mais de 24 anos e de domínio público há mais de dois. São sistemas de manipulação de símbolos que obedecem a certas leis semiológicas, mensuráveis enquanto os sistemas operam em condições adequadas. Tendo sido já descobertas e não sendo criação ou propriedade intelectual ou material do legislador, ou de quem quer que seja, esses sistemas não estão em poder do legislador para serem por ele instituídos no sistema jurídico brasileiro. Estão na bagagem cultural da sociedade, na forma como esta os disponha. O que caberia a uma norma jurídica instituir sobre uma tal infra-estrutura seria, apenas, a regulação dos efeitos jurídicos do uso de tais sistemas sob condições adequadas. A norma jurídica não

pode, por si só, garantir integridade e autenticidade digital alguma. São leis semiológicas que garantem. Da mesma forma que não faz sentido uma norma jurídica decretar ou revogar uma lei física, como a lei da gravidade, a lei da relatividade ou as leis da termodinâmica, estas as que mais se assemelham a leis semiológicas."[17]

26. Esclareça-se que na primeira versão da Medida Provisória 2.200, o par de chaves criptográficas do usuário seria gerado pela própria ICP-Brasil. Nesse caso, poderia ela assegurar autenticidade e integridade, já que definiria o sistema criptográfico que empregaria.

Mas isto seria inadmissível do ângulo da privacidade, posto que, uma outra função da criptografia, mesmo de chaves públicas, é assegurar a confidencialidade de informações. Nesse caso, o processo é inverso daquele da assinatura digital. Como o que uma chave faz, a outra desfaz, o autor de uma mensagem eletrônica pode criptografá-la por meio da chave pública do destinatário, e só destinatário dela, titular também da chave privada, poderá decriptá-la.

Logo, a possibilidade de uma estrutura pública governamental emitir o par de chaves seria inadmissível, posto que, em tese, o governo poderia extrair uma cópia da chave privada para posteriormente ter acesso ao conteúdo das mensagens do cidadão.[18]

Pela mesma razão, a emissão do par de chaves pelas estruturas do Governo Federal seria inadmissível para a função de assinatura digital, pelo risco de alguém que ficasse com cópia da chave privada pudesse vir a firmar uma manifestação de vontade de determinado cidadão, em nome dele.

---

[17] Ver em http://www.observatoriodaimprensa.com.br/artigos/eno130320021.htm

[18] Bruce Schneier, um dos criptógrafos de maior relevo na atualidade, em "Segredos e Mentiras sobre a Proteção na Vida Digital" (*Secrets & Lies*, no original), Editora Campus, páginas 76 e 77, a propósito de tentativas governamentais norte-americanas em ter acesso às chaves criptográficas dos cidadãos, alerta: "O governo, particularmente o FBI, gosta de pintar a privacidade (e os sistemas que a completam) como ferramenta de terror dos Quatro Cavaleiros da Informação do Apocalipse: terroristas, traficantes de drogas, dinheiro sujo e pedófilos pornográficos. Em 1994, o FBI pressionou o *Digital Telephoy Bill* via Congresso, que tentou forçar companhias telefônicas a instalar equipamento em centrais para tornar mais fácil grampear pessoas. No final do bombear do World Trade Center (sic, menção ao atentado anterior ao de 11 de setembro), pressionaram o *Omnibus Counterterorism Bill*, que lhes dava o poder de fazerem grampos e ao Presidente o poder de classificar unilateralmente e secretamente grupos políticos como organizações terroristas. Felizmente, não passou. Depois que o vôo 800 da TWA caiu do céu em 1996, devido à explosão de combustível, o FBI espalhou rumores de que foi um ataque de míssil e passou a outras séries de medidas que posteriormente atingiram a privacidade. Eles prosseguem fazendo *lobby* para dar acesso ao governo a todas as chaves criptográficas que protege a privacidade ou para enfraquecer a segurança de modo que não seja importante."

Assim é que a Ordem dos Advogados do Brasil, pelos presidentes de seu Conselho Federal e de sua Seccional Paulista repudiaram a primeira edição da MP 2.200.[19] [20]

O próprio Governo Federal entendeu esta crítica e suprimiu, já na segunda versão daquela Medida Provisória, 2.200-1, a emissão do par de chaves pela ICP-Brasil.

Porém, ao suprimi-la, deveria ter adaptado seu art. 1º, posto que, como compete ao usuário definir o sistema criptográfico que utilizará, e como esse sistema é que poderá atender ou não aos atributos de autenticidade e integridade, não pode, à evidência, a ICP-Brasil, assegurá-los.

V – ICP-BRASIL : *TRANSAÇÕES ELETRÔNICAS SEGURAS*

27. Na forma do mesmo art. 1º, informa a MP 2.200 que a ICP-Brasil foi criada também para assegurar transações eletrônicas seguras.

Transação é expressão de significado jurídico muito claro: é acordo entre as partes para pôr fim a uma demanda. Parece evidente que não foi nesse significado que a MP 2.200 se utilizou da expressão transação, salvo se a ICP-Brasil comparecesse a cada acordo para conferir o fim do litígio...

Em um esforço de vontade, poder-se-ia entender que a transação é usada em seu sentido leigo, de negócio. Mas, ainda assim, a ICP-Brasil não poderia assegurá-lo. Negócio jurídico seguro é aquele reconhecido como lícito pelo direito, realizado entre partes capazes, com objeto lícito, e forma defesa ou não prescrita em lei. Assim, entender

---

[19] O presidente do Conselho Federal da Ordem se manifestou através de nota oficial, cuja íntegra é a seguinte: "A Ordem dos Advogados do Brasil vem a público manifestar o seu repúdio à nova Medida Provisória nº 2.200, de 29/06/2001, que trata da segurança no comércio eletrônico no País. A MP, editada às vésperas do recesso dos Poderes Legislativo e Judiciário, desprezou os debates que vêm sendo realizados há mais de um ano no Congresso Nacional sobre três projetos a esse respeito, um dos quais oferecido pela OAB-SP. Ao estabelecer exigência de certificações para validade dos documentos eletrônicos públicos e privados, a MP não apenas burocratiza e onera o comércio eletrônico, como distancia o Brasil das legislações promulgadas em todo o mundo. Pior: ao outorgar poderes a um Comitê Gestor, nomeado internamente pelo Executivo e assessorado por órgão ligado ao serviço de segurança nacional, o governo subtrai a participação direta da sociedade civil na definição de normas jurídicas inerentes ao conteúdo, procedimentos e responsabilidades daquelas certificações. Tudo isso é motivo de extrema preocupação no que tange à preservação do sigilo de comunicação eletrônica e da privacidade dos cidadãos, num momento em que grampos telefônicos têm se proliferado país afora, afrontando, inclusive, o livre exercício da advocacia. Brasília, 03 de julho de 2001. Rubens Approbato Machado. Presidente nacional da OAB.

[20] O presidente da Seccional Paulista da OAB, Carlos Miguel Castex Aidar, se manifestou em artigo que escrevemos em co-autoria, publicado no Jornal Folha de São Paulo, denominado "A velha burocracia e os novos arapongas no mundo virtual" em 17.07.2001, Painel Tendências/Debates, cuja íntegra pode ser acessada em: http://www.oabsp.org.br/main3.asp?pg=3.1&pgv=a&id_pres=40

que a ICP-Brasil assegura realização de negócios eletrônicos seguros implicaria em sua participação em cada realização negocial, verificação se as partes são capazes, se o objeto é lícito, se a forma está de acordo com as disposições legais...

Parece-me, ao revés, que aqui a norma está se referindo aos denominados certificados de servidor remoto, que são utilizados para assegurar a titularidade do servidor do *site*, bem como para criptografar as informações que saem do computador do visitante até sua chegada ao servidor que está hospedando o *site*. Mas isto não implica em segurança negocial, nem significa que as informações que saírem do computador do visitante do *site* sejam verdadeiras, nem que serão devidamente tratadas e armazenadas no servidor ao qual foram transferidas, nem que o negócio será efetivamente firmado, nem que o bem ou serviço será entregue ou prestado, nem outra qualquer implicação relativa a um negócio realizado de forma eletrônica, a não ser a criptografia usada na transmissão de dados.

Mas, se aquela expressão estiver sendo usada apenas para criptografia de servidores, não poderia falar em transação segura, mas apenas em transmissão segura.

E, nesse sentido estreito de uso de certificados eletrônicos de servidores remotos, a expressão é representativa de um famoso produto patenteado, de titularidade de uma empresa mundial de cartões de crédito, a Visa: a SET – *Security Eletronic Transacion.*

Portanto, também em relação às chamadas transações eletrônicas seguras, o art. 1º da Medida Provisória não tem significado jurídico algum, constituindo-se verdadeira *aberração* jurídica.

VI – ICP-BRASIL: *VALIDADE JURÍDICA* DOS DOCUMENTOS ELETRÔNICOS

28. Diz ainda o artigo 1º que a ICP-Brasil foi também instituída para assegurar validade jurídica aos documentos eletrônicos. E o art. 10, *caput*, informa que a Medida Provisória trata de todos os documentos eletrônicos, públicos e privados.

Estou convencido, entretanto, de que errou a Medida Provisória 2.200, ao pretender tratar, como se fossem estruturas iguais, documentos públicos, da administração pública; documentos privados; e documentos públicos de natureza privada,

com intervenção notarial, pois suas peculiaridades reclamam tratamentos jurídicos diferenciados.

VI.A. *VALIDADE JURÍDICA* DOS DOCUMENTOS ELETRÔNICOS PRIVADOS

29. Referir-se à *validade jurídica* de um documento é ingressar na validade da própria manifestação de vontade.

Tratando-se de atos jurídicos privados, no mais das vezes a validade dessa manifestação independe de forma[21] [22]. Raros são os documentos privados que têm forma definida em lei. Um exemplo é a escritura de venda e compra de imóvel. Nesses casos de exceção, a inobservância da forma pode representar a nulidade do próprio ato[23].

Para documentos privados, o importante é reconhecer seu valor de prova e não sua validade jurídica – salvo naquelas exceções legais em que se requer forma própria. Mas de valor de prova não trata a Medida Provisória 2.200.

Assim, ou bem a Medida Provisória passou a exigir, para todos os documentos privados, pelo só fato de serem emitidos eletronicamente, forma especial, sem o que o próprio ato poderia padecer de nulidade, ou bem a expressão validade jurídica se refere exclusivamente àquelas hipóteses em que a lei reclama forma própria para realização do ato jurídico.

A primeira hipótese, que estabeleceria forma especial para todos os documentos privados, parece-me afastada pelo disposto no art. 10, § 2º, que autoriza outras formas de prova de integridade e autenticidade dos documentos eletrônicos, inclusive certificados não gerados pela ICP-Brasil. Se as partes podem definir a forma, ela não é obrigatória. Além do que seria disparatado exigir, em negócios que podem ser realizados até verbalmente, forma especial para consumação por meio eletrônico.

---

[21] Artigo 82 do Código Civil: A validade do ato jurídico requer agente capaz, objeto lícito e forma prescrita ou não defesa em lei.

[22] Artigo 129 do Código Civil: A validade das declarações de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.

[23] Artigo 130 do Código Civil: Não vale o ato, que deixar de revestir a forma especial, determinada em lei, salvo quando esta comine sanção diferente contra a preterição da forma exigida.

Resta, pois, a segunda hipótese, de que ao se referir à validade jurídica de documentos, o dispositivo em comento está, na verdade, reportando-se exclusivamente a documentos públicos, que precisam adotar forma especial, consagrando-a no meio eletrônico. Neste caso, porém, existirão questões constitucionais que serão expostas, em capítulos próprios deste estudo, que tratam de documentos públicos de atos jurídicos civis, e documentos públicos, geridos pela própria administração pública.

30. Existem, por outro, manifestações proferidas em seminários e congressos, e divulgadas na imprensa, no sentido de que o art. 1º, na parte em que trata dos documentos eletrônicos, deverá ser interpretado à luz do disposto no art. 10, parágrafo primeiro, da mesma Medida Provisória, que dispõe:

> "§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei n.º 3.071, de 1.º de janeiro de 1916 - Código Civil."

Essas manifestações vêm pretendendo extrair do transcrito § 1º do art. 10 a consagração, na Medida Provisória 2.200-2, o preceito de *não-repúdio*. Daí, a expressão *validade jurídica* teria, para documentos eletrônicos, significação de não-recusa de autoria.

Porém, validade jurídica não tem relação com impugnação de autoria. É conceito bem mais amplo, que envolve capacidade de assumir direitos e obrigações, objeto lícito, e forma prescrita ou não defesa em lei.

31. *Não-repúdio*, ademais, é uma expressão técnica, que parte da presunção de inter-relacionamento das chaves criptográficas. Se a chave pública de alguém validar a assinatura digital é porque ela foi obrigatoriamente gerada pela chave privada a ela correspondente.

Mesmo em seu significado técnico, o conceito de *não-repúdio* é aceito no plano teórico e abstrato, mas não necessariamente no plano real.

Tal qual ocorre em relação à autenticidade e integridade, dependerá também da qualidade do *software* escolhido para geração do par de chaves.

Mas, no conceito de *não-repúdio*, também estão envolvidas questões relacionadas ao sigilo da chave privada, e à correta identificação do titular da chave pública.

Quanto ao sigilo da chave privada, é de se indagar, e ainda considerando apenas o conceito do *não*-repúdio, se a tecnologia oferece, de fato, sistemas, equipamentos, e procedimentos que efetivamente impeçam alguém de, sem consentimento do titular, acessar a chave privada dele.

Mais ainda: é preciso saber se essa tecnologia, que deve, no plano abstrato e prático, realmente impede, sem qualquer possibilidade de falhas, aquele acesso indevido, e é disponível ao cidadão comum, quer na sua disponibilidade no mercado, quer em preço acessível ao consumidor.

Ainda mais: o *não-repúdio* dependerá, também em seu conceito técnico, da perfeita distribuição da chave pública. De nada adiantará um sistema perfeito de emissão de chaves, o ambiente adequado para guarda em sigilo da chave privada, se for possível a alguém atribuir a si, ou a outrem, a titularidade de chave pública de terceiros.

Assim, e reiterando, sempre no plano técnico, sem ingressar, ainda, nas suas implicações jurídicas, o próprio *não-repúdio*, que academicamente pode ser considerado correto, na prática dependerá de uma tal sorte de fatores, internos e externos, físicos e lógicos, que não pode ser considerado uma verdade absoluta.

32. Ora, se ele, mesmo no plano técnico, não pode ser considerado como conceito absoluto, no plano legal, pretender estabelecer a impossibilidade de impugnação a uma assinatura digital e, assim, à própria manifestação de vontade consagrada em um documento eletrônico, constitui nítida aberração jurídica. [24]

Ninguém pode ser privado da liberdade e de seus bens sem o devido processo legal, conforme consagrado no art. 5º, LIV, da Constituição do Brasil. E se fosse impossível impugnar uma assinatura digital, simplesmente não precisaria existir processo legal. Bastaria apresentar um documento eletrônico para condenar alguém, seja no âmbito penal, seja no cível, pela declaração ali contida.

---

[24] A possível justificativa para tentativa de seu enquadramento jurídico é dada por Bruce Shneier, ao observar que "Isso importa principalmente por causa do termo *não-repúdio*. Assim como 'confiável', esse termo é tomado da literatura da criptografia acadêmica. Lá, ele possui um significado especial: que o algoritmo de assinatura digital é impenetrável, de modo que um terceiro não poderá forjar sua assinatura. Os fornecedores de PKI se apoderaram do termo e o usaram em um sentido legal, fazendo lobby para leis com o efeito de que, se alguém usa sua chave de assinatura privada, então você não pode repudiar a assinatura. Em outras palavras, sob algumas leis de assinatura digital (por exemplo, as de Utah e Washington), se a sua chave de assinatura tiver sido certificada por uma CA aprovada, então você é responsável por qualquer coisa que a chave privada faça. Não importa quem estava no teclado do computador ou qual vírus fez a assinatura; você é legalmente responsável" (obra citada, página 236).

Aos litigantes, em processo judicial e administrativo, e aos acusados em geral, são assegurados, pelo art. 5º, LV, da Constituição Brasileira, o contraditório e a ampla defesa, com os meios e recursos a eles inerentes. Mas inexistiria contraditório e ampla defesa se aquele contra quem fosse produzida uma prova documental simplesmente fosse impedido de negar sua autoria.

A lei não excluirá do Poder Judiciário lesão ou ameaça de lesão a direito, segundo dispõe o art. 5º, XXXV, de nossa Lei Maior. Mas, na interpretação que se vem pretendendo emprestar ao antes transcrito parágrafo 1º do art. 10 da Medida Provisória, teria ele o efeito de impedir alguém de se socorrer ao Poder Judiciário para evitar lesão, ou ameaça de lesão a direito, consubstanciada em documento eletrônico cuja titularidade lhe é, indevidamente, atribuída.

33. Por outro lado, parece-me haver confusão entre a obrigação de guarda de uma chave privada e a responsabilização pelo descumprimento dessa obrigação.

A obrigação de sigilo da chave privada é aceitável, desde que transmitidas aos usuários de certificados plenas informações sobre os riscos que estão assumindo ao utilizar assinaturas digitais [25] e estejam disponíveis os elementos tecnológicos necessários à sua preservação. Ainda assim, porém, não pode ser uma obrigação absoluta, já que a quebra de sigilo pode ocorrer por força maior ou caso fortuito, excludentes de responsabilidade – o que, por si só, já justifica repúdio ao *não-repúdio*.

O descumprimento da obrigação de guarda da chave privada pode gerar, contra seu titular, responsabilidade pelos danos que venha a causar a terceiros. Mesmo isto, porém, não significa que tudo o que for assinado deva ser cumprido.

34. Sabemos, por outro lado, que o sistema adotado para emissão do par de chaves pode conter, em teoria, uma *porta traseira*, e transmitir, para outrem, sem conhecimento do titular das chaves, uma cópia da chave privada. Ou ainda, que existe possibilidade de um *hacker* ingressar no computador de determinada pessoa e extrair cópia de sua chave privada.

Assim, não me parece que um magistrado viria a recusar a possibilidade de alguém negar a assinatura digital de um documento por quebra do sigilo da chave

---

[25] Art. 6º, III, da Lei nº 8078/90 (Código de Defesa do Consumidor): "São direitos básicos do consumidor: III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características composição, qualidade e preço, bem como sobre os riscos que representem."

privada. Poderá exigir a prova disto. Ainda que a quebra seja provada, poderá responsabilizar o titular da chave privada pelo prejuízo que vier a causar. Mas daí a simplesmente recusar a própria possibilidade de alguém impugnar uma assinatura digital há uma enorme distância.

Só para exemplificar. Imaginem um contrato de cessão gratuita de cotas de uma sociedade limitada, em que se impeça o empresário, titular das quotas, de negar a autoria da assinatura digital, ainda que de fato ele não tenha feito uso de sua chave privada. Uma coisa é entender que, por não ter mantido em sigilo a chave privada, deva reparar o dano eventualmente causado a quem confiou na assinatura digital dela decorrente. Outra, porém, é simplesmente obrigá-lo a entregar a chave (física) do estabelecimento a quem se disse beneficiário daquela doação.

35. Além disto, a impugnação de uma assinatura digital pode não recair sobre o uso da chave privada, mas sobre a titularidade da chave pública. Não é porque um certificado atribua a alguém a titularidade de uma chave pública que isto constitui uma verdade inafastável. Pode a certificadora ter errado na designação. Pode ser caso de homonímia. O funcionário da certificadora pode ter se enganado e escrito o nome incorreto. Ou pode tê-lo feito de má-fé. Pode, ainda, ter alguém se apresentado àquele funcionário com documentos falsos.

36. Outra afirmação cada vez mais comum é de que não-repúdio e irretratabilidade seriam expressões sinônimas.[26] Irretratabilidade é cláusula que impede aquele que assumiu uma obrigação jurídica de, posteriormente, pretender desfazer unilateralmente o compromisso. Nada tem nenhuma relação com o conceito jurídico que querem dar ao *não-repúdio*, de impossibilidade de negar-se a autoria de um documento, já que, na irretratabilidade, não está em causa a autoria, e sim a possibilidade de, sem concordância da outra parte, desfazer-se da obrigação anteriormente assumida.

37. O mais curioso, porém, é que o parágrafo primeiro do art. 10, no qual pretendem sustentar o *não-repúdio*, sequer trata de presunção de autoria.

Sua redação é claríssima. Dispõe sobre a declaração, o conteúdo do documento eletrônico, e não sobre sua autoria. A presunção que gera, e que, conforme referência

---

[26] Como exemplo, verifique-se glossário constante do "Projeto Básico", anexo I, do Edital de Licitação de Empresa Brasileira de Correios e Telégrafos nº 003/2002, que, às fls. 66, afirmou: "Irretratabilidade (não-repúdio) – Garantia de que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou a participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gerar".

que faz, consta de nosso Código Civil, é a da veracidade dos fatos constantes da declaração, contra quem a assinou, e não sobre quem assinou o documento.

Daí porque entendo que, em relação a documentos particulares, sem forma definida ou defesa em lei, a expressão *validade jurídica* é vazia de significado jurídico. Não corresponde a valor de prova, pois lhe faltam definições processuais importantes. Não diz respeito à validade do ato jurídico, pois representaria que manifestações de vontade que podem ser proferidas até de forma verbal dependeriam, quando emitidas por meio eletrônico, para ter validade, de forma própria. E porque, ao contrário do que tem sido divulgado, em nenhum momento a Medida Provisória trata de *não-repúdio*, no significado jurídico que alguns pretendem lhe emprestar, de impossibilidade, *jure et de jure*, de alguém negar a assinatura digital em um documento eletrônico.

VI.B. *VALIDADE JURÍDICA* DOS DOCUMENTOS ELETRÔNICOS PÚBLICOS, DE NATUREZA PRIVADA

38. O art. 236 da Constituição do Brasil determina que "os serviços notariais e de registro são exercidos em caráter privado, por delegação do poder público", e que a "lei regulará as atividades, disciplinará a responsabilidade civil e penal dos notários, dos oficiais de registro e de seus prepostos, e definirá a fiscalização de seus atos pelo Poder Judiciário."

Já se disse que ao príncipe tudo é permitido, exceto mudar a natureza das coisas. E a natureza dos serviços notariais e de registros é absolutamente tranqüila no mundo jurídico, bem espelhada, aliás, no disposto no art. 1º da Lei nº 8.935/94, ao informar que "*são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos*".

Ora, em se tratando de declarações que visem a outorgar segurança jurídica a atos privados, com presunções legais inerentes à fé pública, só por via de serviços notariais e de registro podem ser efetivadas.

39. É preciso distinguir entre certificações eletrônicas expedidas como atividade-meio e como atividade-fim.

Como atividade-meio, pode o Estado promover suas próprias certificações, atestando titularidade de chaves públicas dos servidores públicos, ou de autoridades

públicas, ou ainda, para validar fluxo de documentos entre o Estado e os administrados. Essas certificações, desde que emitidas no exercício de função pública, terão fé pública.

Porém, como atividade-fim, de intervenção estatal em negócios de natureza privada, a Constituição do Brasil consagrou como competentes os serviços notariais e de registro para dar segurança jurídica às contratações.

40. Por outro lado, empresas privadas podem, conforme antes mencionado, emitir certificados como atividade-meio, para validar, por exemplo, o fluxo de documentos internos, ou como atividade-fim, prestando serviços de certificação à população em geral.

A diferença entre esses certificados e aqueles emitidos pelo Poder Público é a presença da fé pública, com os efeitos a ela inerentes.

41. A Medida Provisória 2.200-2, ao se referir à validade jurídica de documentos eletrônicos públicos (art. 1º, primeira parte, e art. 10, § 1º), condicionando-a à certificação eletrônica da ICP-Brasil, parece transferir para o Poder Executivo, e sua ICP-Brasil, função de confiança que a sociedade civil sempre outorgou aos serviços notariais e de registrado, e que foi consagrada no art. 236 da Constituição do Brasil.

42. É de se ressaltar que as presunções dos atos notariais e dos registradores são lastreadas em sua responsabilidade civil e penal. A Medida Provisória não trata de responsabilidade pela emissão incorreta de certificados, deixando isto para ser definido pelas próprias certificadoras.

Não se preocupou também em definir quem arcará com o prejuízo causado por um certificado incorretamente emitido: se a AC ou se a AR[27]. Os notários são responsáveis por atos de seus prepostos.

O serviço notarial não sofre solução de continuidade. A Medida Provisória 2.200 nada fala sobre como ficarão os certificados de uma AC, ou a documentação de uma AR, caso encerrem suas atividades.

As taxas notariais são tabeladas. A ICP-Brasil não trata disto, e cada certificadora determinará seu preço.

---

[27] A Resolução nº 8, do Comitê Gestor, no item 2.2.2. definiu que "a AC responsável pela DPC responderá solidariamente pelos atos das AR a ela vinculadas." o que nem faz parte de suas atribuições, que se limitam a adotar critérios técnicos, e não jurídicos, da ICP-Brasil (art. 4º, II, da Medida Provisória 2.200-2), nem poderia ser feito por mera norma administrativa, já que responsabilidade é matéria reservada à lei.

São milhares de notários em todo o Brasil. A ICP-Brasil é monopolizante, pelas exigências que faz para constituição de uma AC, agora agravada por uma cobrança de duvidosa constitucionalidade, de tarifa de certificação da Acs, pela AC-Raiz e que poucas empresas conseguirão cumprir.[28]

O Código de Processo Civil expõe, com precisão, todas as conseqüências legais resultantes de assinaturas conferidas por notários, ou documentos registrados por registradores. A ICP-Brasil não tem uma única disposição de natureza processual.

Mais uma vez, portanto, sofre de imperfeições a Medida Provisória 2.200, inclusive de ordem constitucional, que tornam sem conteúdo efetivo os certificados emitidos pela ICP-Brasil.

VI.C. *VALIDADE JURÍDICA* DOS DOCUMENTOS ELETRÔNICOS PÚBLICOS, DA ADMINISTRAÇÃO PÚBLICA

43. No caso de documentos eletrônicos da administração pública federal, pode a União Federal dispor sobre a forma com que devam ser emitidos. Mas não parece possível que a União Federal condicione a validade jurídica de todos os documentos eletrônicos públicos, à sua certificação de chaves públicas, incluindo aqueles emitidos por autoridades e serventuários dos estados, municípios e do Distrito Federal, bem como dos demais Poderes, Legislativo e Judiciário.

A MP 2.200-2, não dispõe de forma explícita dos documentos eletrônicos das demais esferas político-administrativas, nem dos demais poderes da República.

Porém, também não faz distinção ao dispor, no *caput* de seu art. 10, quando se refere a documentos eletrônicos públicos e privados, para todos os fins legais.

---

[28] A Resolução nº 10, do Comitê Gestor, que, sem nenhum critério econômico aparente, ou embasamento legal, definiu que a emissão do certificado raiz às autoridades certificadoras constitui serviço, tarifado entre R$ 100.000,00 (cem mil reais) a R$ 500.000,00 (quinhentos mil reais). A Portaria 12 da Chave-Raiz da ICP-Brasil, o ITI, a pretexto de regular essa Resolução, fez ainda pior: desconsiderou o escalonamento previsto na própria Resolução e fixou a taxa em R$ 500.000,00. Só posteriormente o Governo Federal encaminhou Projeto de Lei ao Congresso Nacional (PL nº 6825, de 2002), pretendendo estabelecer duas taxas: uma de credenciamento, que denominou "Taxa de Credenciamento – TCD", e outra, de fiscalização, chamada "Taxa de Fiscalização e de Manutenção de Credenciamento – TFM". Ambas estipulando taxas astronômicas: A TCD, R$ 500.000,00 (quinhentos mil reais) no caso de AC de nível imediatamente subseqüente ao da AC Raiz; R$ 200.000,00 (duzentos mil reais) no caso das demais AC; R$ 10.000,00 (dez mil reais) no caso das AR; e R$ 5.000,00 (cinco mil reais) no caso dos demais prestadores de serviço de suporte à ICP-Brasil; a TFM, em R$ 20.000,00 (vinte mil reais) no caso de AC de nível imediatamente subseqüente ao da AC Raiz; R$ 5.000,00 (cinco mil reais) no caso das demais AC; e R$ 1,00 (um real) para as AC que emitam certificados para o usuário final.

Em sua justificativa, afirma a Medida Provisória:

> "Das sugestões acolhidas[29] referentes à autenticidade e à integridade do documento eletrônico, a maior parte diz respeito à abrangência da norma basicamente para incluir a administração indireta, especialmente as autarquias, fundações e sociedades de economia mista, o Distrito Federal, os demais poderes, as serventias extrajudiciais, pessoas jurídicas de direito privado, em geral, inclusive empresas e bancos."

Além disto, mais recentemente, foi vetado pela Presidência da República um parágrafo único, que o art. 1º do projeto que resultou na Lei nº 10358/01 pretendia acrescer ao art. 154 do Código de Processo Civil.

Dizia aquele parágrafo:

> "Art. 154 .....
>
> Parágrafo único. Atendidos os requisitos de segurança e autenticidade, poderão os tribunais disciplinar, no âmbito da sua jurisdição, a prática de atos processuais e sua comunicação às partes, mediante a utilização de meios eletrônicos." (NR)

E estas foram as razões do veto:

> "A superveniente edição da Medida Provisória no 2.200, de 2001, que institui a Infra-Estrutura de Chaves Públicas Brasileira - 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, que, aliás, já está em funcionamento[30], conduz à inconveniência da adoção da medida projetada, que deve ser tratada de forma uniforme em prol da segurança jurídica."

Logo, embora não conste explicitamente daquela Medida Provisória, parece ser intenção dela que documentos eletrônicos emitidos por Estados, Municípios, Distrito Federal, e pelos Poderes Legislativo e Judiciário, dependem, aí sim, para ter sua validade jurídica reconhecida, de certificação da ICP-Brasil.

---

[29] A referência às sugestões acolhidas diz respeito ao anteprojeto de lei que originou a Medida Provisória 2.200, e que instituía a ICP-Gov (Infra-Estrutura de Chaves Públicas Governamental.

[30] Na verdade, na data do veto a ICP-Brasil não estava em funcionamento, sendo que nenhuma empresa ou entidade pública havia sido credenciada para operar como Autoridade Certificadora.

44. Tal exigência, entretanto, nitidamente viola preceitos constitucionais.

O primeiro deles é o da eficiência, consagrado no art. 37, caput, da Constituição Brasileira. Não existe um sapato único para todos os pés do Brasil. Não existe uma única certificação, padrão, para atender a todos os fluxos de informações brasileiros.

O segundo preceito violado é o da autonomia dos entes político-administrativos da República Brasileira, insculpido no art. 18, *caput*, de nossa Constituição. Não pode a União pretender impor seu certificado aos Estados, Municípios e Distrito Federal.

O terceiro, e na mesma linha de raciocínio, é o da independência dos Poderes, uma das maiores conquistas do Estado Democrático de Direito, e declarado já no artigo 2º da Constituição Brasileira.

Imagine-se, por exemplo, uma lei, após aprovada pela Assembléia Legislativa, ser sancionada por meio de assinatura digital do Governador do Estado, mas não ter *validade jurídica* porque, embora atendesse a todos os preceitos constitucionais formais e materiais de uma lei estadual, não contivesse, a chave pública do Governador do Estado, a certificação eletrônica do Governo Federal. Não pode a assinatura digital de um magistrado, ou de um parlamentar, ter sua validade condicionada à certificação da chave pública pelo Poder Executivo Federal.

Da mesma forma, o presidente de uma Corte Estadual, ou mesmo do Supremo Tribunal Federal, ao assinar um ato – de natureza judicante ou administrativa, estaria sujeito a ter questionada sua validade, não por descumprimento de algum preceito legal ou constitucional, mas porque sua chave pública não fora certificada pelo Governo Federal.

45. A tecnologia, esclareça-se, não exige uma chave raiz única. Nenhum país a adotou. E ainda que exigisse, que se mudasse a tecnologia, mas jamais se pretenda mudar o próprio Estado Democrático de Direito, e suas conquistas sociais, para ajustá-lo a ela, condicionando a validade de um ato de um Estado ou de um Município autônomo, ou de um Poder independente, à certificação da União Federal.[31]

---

[31] O filósofo francês Paul Virilio, na obra *"A Bomba Informática"* (Estação Liberdade Editora, pág. 11), alerta, quanto aos riscos que a tecnologia tem trazido às ciências, por conta de interesses comerciais e publicitários: "De fato, o único horizonte científico é a autenticidade, o rigor experimental dos pesquisadores e todos conhecemos, infelizmente, os abusos midiáticos que envolvem certas "descobertas", o caráter publicitário da divulgação prematura dos resultados desta ou de outra experiência; esses abusos não passam de uma maneira de condicionar a opinião pública por meio de uma ciência de extremos, menos preocupada com a verdade que com o impacto do anúncio de um achado e não mais, como outrora, de uma descoberta autêntica, útil ao homem comum". Isto não difere com o que está ocorrendo em relação à ciência jurídica, quanto à assinatura digital. É ela, inegavelmente, um importante instrumento, que pode ser usado pelo Estado e pela sociedade para superar as dificuldades inerentes ao uso do papel para emissão de documentos. Mas isto não pode implicar em desconsiderar preceitos básicos da ciência jurídica, *vendendo* a tecnologia de assinatura digital como se fosse uma solução mágica, sem riscos, e de tal ordem que pudesse derrogar preceitos basilares do Estado Democrático de Direito.

VII. DE *LEGE FERENDA*

46. É preciso, por todo o exposto, ajustar rapidamente a legislação sobre documento eletrônico, assinatura digital e certificação eletrônica, sob pena de criar-se maior insegurança jurídica, por leituras apressadas e por manifestações contínuas do Governo Federal, daquela que havia quando não existia, no Brasil, legislação alguma sobre aqueles importantes instrumentos.

Destaco, a seguir, os pontos que me parecem principais, e que merecem ser objeto da nova lei, seja para suprimir inconstitucionalidades da Medida Provisória 2.200-2, seja para suprir as lacunas que permaneceram sem disciplina legal com a sua adoção.

47. O primeiro deles diz respeito ao ônus da prova, em caso de impugnação de um documento eletrônico.

A expressão “assinatura digital” só pode ser equiparada à assinatura física no que tange à sua eficácia. Mas são diferentes quanto às suas estruturas de emissão.

Uma assinatura física é um ato único.

A assinatura digital é um processo que se inicia na escolha do par de chaves, passa pela guarda em sigilo da chave privada e pela correta distribuição da chave pública, e chega ao sistema do destinatário, encarregado de fazer a correta identificação da assinatura.

Negar uma assinatura física representa apenas afirmar que a assinatura não pertence a quem é atribuída.

Negar uma assinatura digital não é tão simples.

Os dois exemplos antes mencionados dão dimensão disto: alguém pode impugnar uma assinatura digital sob o pretexto de que outra pessoa teve acesso à sua chave privada. Outro, ao revés, pode impugná-la alegando simplesmente não ser titular da chave pública. Verifique-se: são duas situações extremas, mas que bem demonstram a necessidade de ajuste do nosso Código de Processo Civil. Na primeira situação, não há negação de titularidade do par de chaves, mas sim de seu uso. Na segunda, a própria titularidade do par de chaves está em questão.

No projeto de lei da OAB-SP, que hoje tramita no Congresso Nacional na forma do PL 1.589/99, houve a preocupação de que isto estivesse ajustado, atribuindo-se, a cada possível impugnação, diferentes ônus de prova.[32]

48. Outro ponto omisso na Medida Provisória 2.200, e que precisa ser tratado em lei, diz respeito às obrigações das certificadoras.

O projeto da Seccional Paulista da OAB prevê diferentes tipos de certificados, tratando-os de formas diferentes.

Trata dos certificados privados, emitidos por certificadoras privadas. Nesse caso, diz o projeto da Ordem-SP, o certificado tem caráter comercial, e suas condições serão definidas em contrato. Quando digo condições, refiro-me às diferentes classes de certificados, que no mundo inteiro são definidas de acordo com os procedimentos adotados para reconhecimento da chave pública, bem como sobre as diferentes responsabilidades, que cada nível de certificado gera.

Os certificados privados, emitidos como atividade-meio ou atividade-fim, não geram, pelo projeto da OAB-SP, presunções jurídicas próprias da fé pública, exatamente porque não espelham declarações de agentes públicos, mas de empresas privadas. Daí porque permite essa flexibilidade nas práticas de certificação, e níveis diferentes de responsabilidade.[33]

A Medida Provisória 2.200 confundiu isto ao pretender que todos os certificados emitidos abaixo de sua chave-raiz, por entidades públicas e também por empresas privadas, gerassem "presunções jurídicas" de autenticidade, integridade, e validade jurídica de documentos eletrônicos, mas não tratou, como mencionei, nem de processos, nem de continuidade dos certificados, em caso da empresa certificadora encerrar suas atividades, nem da responsabilidade civil e penal por emissões incorretas de certificados.

---

[32] Arts. 22 e 23 do Projeto de Lei 1.589/99: "Art. 22 - O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura. Art. 23 - Havendo impugnação do documento eletrônico, incumbe o ônus da prova: I - à parte que produziu o documento, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado;II - à parte contrária à que produziu o documento, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves. Parágrafo único - Não sendo alegada questão técnica relevante, a ser dirimida por meio de perícia, poderá o juiz, ao apreciar a segurança do sistema criptográfico utilizado, valer-se de conhecimentos próprios, da experiência comum, ou de fatos notórios."

[33] Art. 24 do Projeto de Lei 1.589/99: "Art. 24 - Os serviços prestados por entidades certificadoras privadas são de caráter comercial, essencialmente privados e não se confundem em seus efeitos com a atividade de certificação eletrônica por tabelião, prevista no Capítulo II deste Título."

Isto, plenamente admissível em contratos privados, não pode ser aceito em se tratando de certificados que pretendam conter alguma presunção jurídica.

Tratou ainda aquele projeto de lei sobre certificados emitidos pelos notários, por conta, como antes exposto, do disposto no art. 236 da Constituição brasileira, com as presunções decorrentes da fé pública de sua atividade; mas, para tanto, dispunha minuciosamente sobre procedimentos, sistemas, continuidade de atividades, fiscalização, e responsabilidade civil e penal, para emissão de certificados.[34]

49. É preciso também ajustar as normas penais que tipificam falsidades documentais às novas realidades tecnológicas.

A norma penal deve definir, com absoluta precisão, o tipo que pretende punir. É preciso, assim, ajustar a norma às peculiaridades próprias dos documentos eletrônicos, assinaturas digitais e certificações eletrônicas, sob pena de não serem aplicáveis a elas. O Projeto da OAB-SP apresenta novos tipos penais para suprir essa lacuna.[35]

A Medida Provisória 2.200-2 não os apresenta[36], nem poderia apresentá-los, na medida em que esse veículo legislativo não pode tratar de matéria penal.

50. Finalmente, observe-se que o projeto da OAB-SP não tratou de certificados emitidos pelo Estado, para efeito de fluxo de informações da administração pública. Isto por entender, primeiro, que cada esfera político-administrativa tem o direito de definir sua própria política de certificação e, depois, que sua regulação independe de lei, bastando mero decreto para implementá-los.

Neste contexto, será fundamental, inclusive para sanar inconstitucionalidades da Medida Provisória 2.200-2, antes apontadas, que a ICP-Brasil seja transformada, conforme sua própria proposta inicial, em ICP-Gov, limitada a documentos eletrônicos emitidos e recebidos pela administração pública federal, resgatando-se a autonomia das esferas político-administrativas da Nação, e independência e harmonia dos Poderes da República brasileira.

Marcos Costa,

advogado

---

[34] Arts. 25 a 42 do Projeto de Lei 1.589/99.

[35] Arts. 43 a 49 do Projeto de Lei 1.589/99.

[36] Muito embora a sua justificativa afirme que a expressão “para todos os fins legais”, constante do *caput* do art. 10, tenha exatamente a finalidade de incluir efeitos penais.

DIREITO AUTORAL ELETRÔNICO

Renato M. S. Opice Blum e
Juliana Canha Abrusio

DIREITO AUTORAL ELETRÔNICO

Renato M. S. Opice Blum e
Juliana Canha Abrusio

A internet já faz parte do cotidiano das empresas, bem como do cidadão comum. A tecnologia trazida pelo avanço das telecomunicações já se consagrou, de sorte que é inconcebível pensar nas relações interpessoais e comerciais sem esta ferramenta virtual.

Assinale-se, porém, que além das várias vantagens trazidas pela internet, surgiram também os conflitos, que antes da criação da grande rede mundial não causavam tanta preocupação. Com efeito, uma questão que tem causado muitos debates é o Direito Autoral na Internet. A Constituição Federal brasileira, em seu artigo 5º, inciso XXVII, garante aos autores o direito exclusivo de utilização, publicação ou reprodução de suas obras. Não restam dúvidas de que esta proteção constitucional abrange também o meio eletrônico da internet.

Desde Roma antiga já eram reconhecidos os direitos do autor sobre sua obra, contudo a estes eram atribuídas somente a glória e as honras que advinham do feito, de sorte que o direito à remuneração pertencia ao copista ou, sendo o autor escravo, ao seu senhor.

Durante o Renascimento, o direito às publicações pertencia aos editores, os quais mantinham o monopólio sobre as obras. Os autores contentavam-se apenas com suas criações intelectuais.

No ano de 1709, na Inglaterra, o direito autoral foi reconhecido formalmente, com o *Copyright Act* da Rainha Ana. Consta, porém, que a proteção das obras literárias já existia desde 1662, graças ao *Licensing Act,* que proibiu a impressão de qualquer livro que não fosse licenciado ou registrado devidamente.

Na França, durante a Revolução Francesa de 1789, em meio às discussões dos direitos individuais, surge o *droit dáuter,* que aprimorou o direito autoral, adicionando a este o conceito de direito moral.

No Brasil, desde a primeira Constituição da República, de 1891, o direito autoral possui proteção constitucional. Atualmente, o diploma legal que regulamenta os direitos de autor e dos que lhe são conexos é a lei n° 9.610 de 19 de Fevereiro de 1998 e a lei 9.609 [1], da mesma data, que dispõe sobre a proteção da propriedade intelectual de programa de computador, com a observância das garantias contidas na Constituição Federal de 1988, no artigo 5º, incisos XXVII, XXVIII e XXIX.

OBJETO DO DIREITO

Ressalte-se que independente do meio físico em que se encontre a obra (livro, *Compact Disc*, Internet etc), o objeto do direito autoral será sempre o de proteger as obras intelectuais pela originalidade ou criatividade da forma. O bem jurídico protegido pelo legislador é, portanto, o produto da criação intelectual. As idéias em si não são protegidas. O direito autoral passa a existir no momento em que se materializa, seja qual for o “corpus mechanicus”.

TITULARIDADE E REGISTRO

O sujeito do direito autoral é o autor ou o titular de autoria de obra intelectual – o escritor, o compositor, o artista plástico, o desenhista, o fotógrafo, o *web designer* etc. O titular originário, portanto, é a pessoa física criadora da obra intelectual.

De outro lado, existe a possibilidade jurídica do reconhecimento de titularidade do direito à pessoa jurídica. A Lei do Software reconhece a proteção jurídica dos programas de computador à pessoa jurídica.

Concernente ao registro da obra intelectual, ressalte-se que a simples menção de autoria, independente de registro, identifica sua titularidade. Portanto, verifica-se que o registro não é obrigatório, trata-se apenas de datação e de uma segurança a mais para os titulares. Cabe mencionar que os *softwares* são passíveis de registros perante o INPI, de sorte que a falta do registro não retira o caráter de proteção autoral (art. 3º, lei 9.609/98).

---

[1] Anexo 1

INOVAÇÕES EM RELAÇÃO AO MEIO ELETRÔNICO

A lei 9.610/98 trouxe uma inovação, qual seja, a proteção aos titulares dos direitos patrimoniais sobre as bases de dados, o armazenamento em computador, a microfilmagem e as demais formas de arquivamento do gênero.

Ressalte-se que, se o autor autoriza a inclusão de sua obra num banco de dados, deverá estipular sua forma de uso e os limites de transmissão, comunicação e utilização com clareza, no interesse das partes.

Após a promulgação da Lei 9.610/98, que revogou a Lei 5.988/73, ampliou-se o conceito de reprodução, considerando-se como tal a cópia feita de qualquer forma tangível, incluindo qualquer armazenamento permanente ou temporário por meios eletrônicos ou qualquer outro meio que exista ou venha a ser criado, podendo-se incluir, conseqüentemente, a internet.

O suporte em que a obra for fixada, sendo ele tangível ou não, é irrelevante. Basta que a obra seja uma criação do espírito para receber a proteção conferida em lei, esteja ela em livro, disco, CD-ROM, banco de dados, meio magnético, fonograma etc.

O FORMATO MP3 E OS DIREITOS CONEXOS

A extensão do conceito de autor foi consolidado pela 9.610/98, através da criação do direito conexo, que reconheceu ao artista intérprete ou executante, ao produtor de fonogramas e aos organismos de rádio-difusão, proteção sob o manto do direito autoral.

Os direitos conexos conferiram aos produtores fonográficos um reconhecimento que antes somente era atribuído ao criador da música propriamente dito. Aqueles passam a ter, agora, uma garantia de remuneração ao seu investimento. Neste contexto, surge o litígio judicial entre as multinacionais produtoras de fonogramas e o NAPSTER/MP3.

O MP3 começou a ser desenvolvido em 1987, época em que a internet não era tão divulgada e utilizada como é nos dias de hoje. Em 1992, o formato foi aceito como um padrão para compactação de arquivos musicais, recebeu a denominação

ISO-MPEG (*International Electro Technical – Moving Pictures Experts Group*) Áudio Layer-3, reduzido depois para apenas duas letras e um número – MP3.

Os criadores do MP3, pesquisadores do Instituto Fraünhofer, na Alemanha, desenvolveram uma forma inovadora de reduzir o tamanho de arquivos sonoros. Eles conseguiram retirar das músicas os sons cujas freqüências não são captadas pelos ouvidos humanos. Os pesquisadores lograram transformar arquivos sonoros cuja taxa de bits era de 1,4 Mbyte por segundo de música em arquivos com uma taxa de 128 kbytes por segundo. Este método, por ser capaz de reduzir a um décimo o tamanho de arquivos musicais, levou a música para a internet.

Os arquivos em formato MP3, por si só, não representam violação a direitos de autor, sendo apenas um novo formato de gravação de obras musicais que possibilita o armazenamento de um grande número de músicas utilizando pouca memória.

À luz da lei nº 9.610/98, conclui-se que a transferência de arquivos MP3, havendo intuito comercial por parte do usuário ou não, constitui verdadeira infração aos direitos autorais de seus titulares, exceto se houver a devida autorização dos mesmos para a referida reprodução e execução públicas.

O Napster e outros programas para intercâmbio de arquivos, tais como o Gnuttela, o Aimster e o Imesh, são apenas vias facilitadoras da distribuição e compartilhamento dos arquivos em MP3.

Acrescente-se que, não é o *software* especializado em arquivos MP3 que é considerado ilegal, embora existam algumas decisões judiciais norte-americanas condenando as empresas criadoras de tais *softwares*, fundamentadas no argumento de que a colocação de músicas no servidor sem autorização de seus autores ou titulares é ilegal. Com efeito, a ilegalidade reside na distribuição e na cópia dos referidos arquivos sem a devida autorização do autor ou titular da composição musical.

A Justiça norte americana, em 2001, considerou que o Napster desrespeitava as leis que estabeleciam o pagamento de direitos autorais e, por força desta decisão, foi proibido de veicular músicas que não fossem autorizadas expressamente pelos seus titulares de direito autoral. As Associações da Indústria Fonográfica sustentavam que o *software* desencorajava a compra de CDs e fitas cassete (*contributory copyright infringement*). As gravadoras estimam que perderam mais de U$ 150 milhões de dólares por causa dos programas como o Napster (dados retirados do *site www.terra.com.br/informática*).

A reprodução de música ambiente em áreas comuns também já foi objeto de decisão no Brasil, tomada pela 3.ª Turma do STJ, no julgamento do recurso apresentado pelo Escritório Central de Arrecadação e Distribuição contra um hotel de luxo. O Superior Tribunal de Justiça entendeu que a reprodução de música ambiente em áreas comuns de hotéis, bem como restaurantes, salas de convenção e quadras esportivas é motivo para pagamento de direitos autorais. Por sua vez, a música veiculada em aparelhos de rádio ou televisão à disposição dos hóspedes nos quartos não enseja o dever dos hotéis ao pagamento dos direitos autorais. (*STJ – Resp 140.024*).

A matéria consolidou-se na Súmula 261 do STJ que orienta os futuros julgamentos sobre a mesma questão, no sentido de que a cobrança de direitos autorais pela retransmissão de músicas em hotéis deve ser feita conforme a taxa média de utilização do equipamento, apurada em liquidação.

PIRATARIA

A pirataria é o termo vulgarmente usado para definir a cópia, reprodução ou utilização indevida e sem a autorização de seu titular, de qualquer suporte que contenha obras intelectuais legalmente protegidas, inclusive a internet.

Não se considera, no entanto, pirata a cópia única, realizada em casa, para uso exclusivamente pessoal. Se esta cópia, porém, sair desta esfera para ser reproduzida, alugada, trocada, exibida publicamente, ou de qualquer forma utilizada sem a expressa autorização dos respectivos titulares, aí sim, ela se torna pirata.

Em 20 de fevereiro de 2002, foi proferida uma das mais importantes decisões sobre a pirataria de *software*, pelo juiz da 12.ª Vara Cível do Rio de Janeiro. A empresa HJ Software foi condenada a pagar R$ 270 mil à Multimídia por ter plagiado programas.

Nessa decisão o juiz, após estabelecer as devidas diferenças entre pirataria e plágio, concluiu que “plagiar um programa de computador não significa criar um novo programa com a mesma finalidade de um outro pré-existente, mas sim aproveitar-se da materialização dessa idéia, ou seja, da forma como ela é apresentada e percebida pelo usuário e dar-lhe, sutilmente, uma roupagem diversa” (*Autos n° 122036-4 e 109071-7, 12ª. Vara Cível, Rio de Janeiro-RJ*) [2].

[2] Anexo 3

SANÇÕES APLICÁVEIS

As sanções previstas pela lei dos direitos autorais são apenas de caráter civil, eis que as penais estão estabelecidas em capítulo específico do Código Penal – Dos Crimes Contra a Propriedade Intelectual (artigos 184, 185 e 186).

A lei garante ao titular da obra fraudulentamente reproduzida, divulgada ou de qualquer forma utilizada o direito de requerer a apreensão dos exemplares reproduzidos ou a suspensão da divulgação, sem prejuízo das indenizações cabíveis.

O artigo 103 da lei aludida dispõe que o responsável pela violação dos direitos autorais pagará, a título de indenização patrimonial, o valor dos exemplares que tiver vendido, o que corresponde, logicamente, ao número de exemplares fraudulentamente editados, utilizados, apreendidos ou vendidos, multiplicado pelo valor unitário.

O transgressor deverá pagar, caso não se conheça o montante da edição fraudulenta, por um mínimo de três mil exemplares, além dos apreendidos. De igual forma, quem vender, expuser à venda, ocultar, adquirir, distribuir, tiver em depósito ou utilizar obras ou fonogramas reproduzidos com fraude será solidariamente responsável com o contrafator, inclusive o importador e o distribuidor em caso de reprodução no exterior.

No caso da transgressão ocorrer no âmbito da Internet, consideramos que o número de exemplares fraudulentamente editados seria aquele correspondente ao número de acessos de usuários que a obra intelectual atingiu dentro do *web site* infrator.

Porém, obviamente, o número de acessos à obra é prova difícil de ser realizada, vez que depende de perícia nos equipamentos do próprio infrator, que facilmente poderá ocultar tais dados, sem qualquer vestígio. Assim, inviabilizada a perícia, basta aplicar o mandamento legal supra referido e calcular a indenização sobre o valor da obra, multiplicado por 3.000 (três mil), sem qualquer óbice.

FAIR USE

O *Fair Use* é uma exceção ao direito do autor. Foi criado nos EUA e consiste numa tentativa de tornar legítimo o uso de obras literárias através da internet, desde

que sem o intuito de lucro, bastando que certos requisitos sejam observados. O fundamento para esta prática se encontra no princípio de que a veiculação corresponderia a uma finalidade social, e não a uma violação dos direitos autorais.

Importante frisar que o instituto do *fair use* não foi recepcionado pela legislação brasileira, constituindo apenas uma questão de discussões jurídicas e outras pertinentes. Vale dizer que não obstante o *fair use* não esteja previsto em lei pátria, o STJ já se pronunciou no sentido de que os shows oferecidos pelos municípios, em que não são cobrados os ingressos, não violam os direitos autorais dos artistas, o que poderíamos chamar de um atípico *"fair use"* brasileiro.

O Ecad ajuizou ação contra o município de Santos, alegando existir a necessidade de autorização prévia para a utilização de obras artísticas e musicais de seus filiados. O aviso teria sido ignorado e os shows foram realizados sem qualquer recolhimento dos direitos. Após perder nas duas instâncias da Justiça paulista, o Ecad recorreu ao STJ, o qual decidiu que os direitos autorais só podem ser cobrados por shows subvencionados por prefeituras quando há algum tipo de proveito econômico, apresentações realizadas na ruas, sem a cobrança de ingressos, nem remuneração de artistas estão isentas de pagamento (*STJ - RESP 302583,* Notícias Superior Tribunal de Justiça, extraído do site *http://www.stj.gov.br/webstj/Noticias/detalhes_noticias.asp?seq_ noticia=3562).*

File Sharing

File-Sharing é o ato de disponibilizar para cópia, um ou mais arquivos, por meio de *software* que permita fazê-lo.

As obras passíveis de serem objetos do *File Sharing* são todas aquelas que possam ser digitalizadas e disponibilizadas na rede, sendo as mais comumente encontradas os fonogramas, os filmes, fotografias, livros e inclusive *softwares*. Não havendo prévia autorização do titular do direito autoral ou conexo sobre estas obras, a prática do *File Sharing* constituirá infração sob a égide da lei 9.610/98.

Spiders

Nos últimos anos, *sites* de busca começaram a vasculhar a internet procurando não somente textos, mas também imagens. Estes *sites* especializados em busca

utilizam ferramentas conhecidas como *spiders*, que permitem copiar as imagens que encontram na rede, ainda que sem autorização. As imagens encontradas são então exibidas na lista de resultados do *site*, sem a aprovação dos artistas que as criaram.

As empresas de busca e os artistas ou fotógrafos que contenham imagens divulgadas na internet devem estar atentos. Ao contrário da concepção de alguns, nem tudo que se encontra na *web* pode ser usado gratuitamente.

Todo trabalho de criação, inclusive os que se encontram na internet, são protegidos por direitos autorais, mesmo que não tenha sido registrado no departamento competente.

PROTEÇÃO JURÍDICA DO *WEB SITE*

O *Web Site* de uma empresa é um elemento diferenciador em relação a seus competidores e faz parte da imagem corporativa da empresa. Por isso, deve-se prestar atenção suficiente a todos os aspectos que incidem na criação e desenvolvimento de um *Web Site*.

O desenho e a programação de um *Web Site* tem uma dupla proteção. Por um lado, e como representação gráfica, é uma criação artística (como uma fotografia ou um quadro) e por outro, tudo quanto consta expressado em uma linguagem (HTML, JavaSript, Visual Basic...), o código fonte, pode ser considerado como um programa de computador, e obter a proteção da lei como tal.

A titularidade destas criações gera problemas entre as partes implicadas. Pela lei 9.609/98, a presunção é de que o programa desenvolvido para o *Web Site* pertence ao contratante do serviço. Para que sejam atribuídos com exclusividade ao *web designer*, mister pactuar-se que a titularidade destas criações pertence a seus criadores, de sorte que se conceda apenas um direito de uso em favor do cliente que contratou o serviço de criação.

De outro lado, a programação de *Web Sites* supõe, também, a organização ou sistematização de um conteúdo (criação de imagens, sons etc), e nesse sentido, deve ser protegida sob à égide da lei 9.610/98.

Portanto, mais do que um programa de computador, a criação de *Web Sites* se assemelha ao desenvolvimento da base de dados, daquelas que a Lei de Proteção

Autoral reconhece seu valor como criações intelectuais, sem prejuízo dos direitos que possam subsistir sobre tais conteúdos, enquanto programa de computador.

Tanto o desenho das páginas, que incorpora elementos visuais, como seu conteúdo e o código de fonte, estão protegidos de acordo com a legislação sobre propriedade intelectual. A diferença com as patentes e marcas, além do critério de novidade, é que se nestas a lei protege estes direitos desde o momento de sua inscrição ou registro perante o organismo competente, não sucede assim com as criações literárias, artísticas ou científicas, cujos direitos nascem no momento de sua criação. Portanto, se no primeiro caso o registro confere direitos e, por tanto, segurança, no segundo caso o registro serve unicamente como um instrumento de prova da titularidade e de datação. Mas não por isso seja menos recomendável.

PROTEÇÃO JURÍDICA DO *SOFTWARE*

A lei n° 9.609/98 [3], regulamentada posteriormente pelo Decreto n° 2.556/98, passou a normatizar inteiramente todas as operações realizadas com programas de computador, tanto os de origem nacional, como os estrangeiros, revogando a lei n.° 7.646/87, que antes cuidava desta matéria.

Assim como as obras literárias, o programa de computador é considerado uma criação do espírito, exteriorizada por meio da elaboração, por seu criador, de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, para utilização em máquinas de processamento de dados.

No que concerne à indenização por dano moral do autor do *software*, a lei 9.609/98 não trouxe nenhuma disposição expressa quanto ao assunto. Por isso, deverá ser aplicada a regra da lei dos direitos autorais, prevista no art. 103.

Com o advento da lei do *software*, a tutela dos direitos relativos a programa de computador foi estendida de 25 para 50 anos, de sorte que a proteção aos direitos sobre a sua proteção independe de registro em qualquer órgão ou entidade.

Segundo o critério do autor, poderão os programas de computador ser registrados no Instituto da Propriedade Industrial – INPI, salientando que a falta de

[3] Anexo 2

tal registro não lhe retirará a proteção autoral, tampouco influenciará no prazo de contagem do exercício desse direito, vale dizer, 50 anos.

Acrescente-se que as informações do programa prestadas para o pedido de registro serão consideradas sigilosas, não podendo ser reveladas a terceiros, salvo por ordem judicial ou a requerimento do próprio titular.

Outrossim, com o advento da referida lei, foi eliminada a necessidade de cadastro prévio do *software*, o registro do contrato de comercialização de programas estrangeiros e a obrigatoriedade de comercialização de programas exclusivamente por empresas brasileiras.

Anteriormente, a lei n.° 7.646/87 determinava a necessidade de contratação de licença do autor do programa de computador apenas no caso de comercialização de *software*. A lei n° 9.609/98, contudo, modificou a matéria no sentido de que o simples uso de programa de computador no país deverá ser objeto de contrato de licença (art. 9°). Na hipótese de eventual inexistência do contrato de licenciamento, o documento fiscal relativo à aquisição ou licenciamento de cópia servirá para sua comprovação da regularidade de seu uso (parágrafo único).

Outra questão importante diz respeito ao empregado e ao empregador em relação aos direitos de autor. É clara a lei ao dizer que, "salvo disposição em contrário, pertencerão exclusivamente ao empregador contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses serviços" (art. 4.°).

Destaque-se que somente pertencerão ao empregado, com exclusividade, os direitos relativos a programas gerados sem relação com o contrato de trabalho, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador. Da mesma forma, aplica-se esta regra para os bolsistas, estagiários e assemelhados que desenvolverem programas de computador.

Renato M. S. Opice Blum e Juliana Canha Abrusio,

advogados

ANEXOS

I-

LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998.

Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Título I

Disposições Preliminares

Art. 1º Esta Lei regula os direitos autorais, entendendo-se sob esta denominação os direitos de autor e os que lhes são conexos.

Art. 2º Os estrangeiros domiciliados no exterior gozarão da proteção assegurada nos acordos, convenções e tratados em vigor no Brasil.

Parágrafo único. Aplica-se o disposto nesta Lei aos nacionais ou pessoas domiciliadas em país que assegure aos brasileiros ou pessoas domiciliadas no Brasil a reciprocidade na proteção aos direitos autorais ou equivalentes.

Art. 3º Os direitos autorais reputam-se, para os efeitos legais, bens móveis.

Art. 4º Interpretam-se restritivamente os negócios jurídicos sobre os direitos autorais.

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

I - publicação - o oferecimento de obra literária, artística ou científica ao conhecimento do público, com o consentimento do autor, ou de qualquer outro titular de direito de autor, por qualquer forma ou processo;

II - transmissão ou emissão - a difusão de sons ou de sons e imagens, por meio de ondas radioelétricas; sinais de satélite; fio, cabo ou outro condutor; meios óticos ou qualquer outro processo eletromagnético;

III - retransmissão - a emissão simultânea da transmissão de uma empresa por outra;

IV - distribuição - a colocação à disposição do público do original ou cópia de obras literárias, artísticas ou científicas, interpretações ou execuções fixadas e fonogramas, mediante a venda, locação ou qualquer outra forma de transferência de propriedade ou posse;

V - comunicação ao público - ato mediante o qual a obra é colocada ao alcance do público, por qualquer meio ou procedimento e que não consista na distribuição de exemplares;

VI - reprodução - a cópia de um ou vários exemplares de uma obra literária, artística ou científica ou de um fonograma, de qualquer forma tangível, incluindo qualquer armazenamento permanente ou temporário por meios eletrônicos ou qualquer outro meio de fixação que venha a ser desenvolvido;

VII - contrafação - a reprodução não autorizada;

VIII - obra:

a) em co-autoria - quando é criada em comum, por dois ou mais autores;

b) anônima - quando não se indica o nome do autor, por sua vontade ou por ser desconhecido;

c) pseudônima - quando o autor se oculta sob nome suposto;

d) inédita - a que não haja sido objeto de publicação;

e) póstuma - a que se publique após a morte do autor;

f) originária - a criação primígena;

g) derivada - a que, constituindo criação intelectual nova, resulta da transformação de obra originária;

h) coletiva - a criada por iniciativa, organização e responsabilidade de uma pessoa física ou jurídica, que a publica sob seu nome ou marca e que é constituída pela participação de diferentes autores, cujas contribuições se fundem numa criação autônoma;

i) audiovisual - a que resulta da fixação de imagens com ou sem som, que tenha a finalidade de criar, por meio de sua reprodução, a impressão de movimento, independentemente dos processos de sua captação, do suporte usado inicial ou posteriormente para fixá-lo, bem como dos meios utilizados para sua veiculação;

IX - fonograma - toda fixação de sons de uma execução ou interpretação ou de outros sons, ou de uma representação de sons que não seja uma fixação incluída em uma obra audiovisual;

X - editor - a pessoa física ou jurídica à qual se atribui o direito exclusivo de reprodução da obra e o dever de divulgá-la, nos limites previstos no contrato de edição;

XI - produtor - a pessoa física ou jurídica que toma a iniciativa e tem a responsabilidade econômica da primeira fixação do fonograma ou da obra audiovisual, qualquer que seja a natureza do suporte utilizado*;*

XII - radiodifusão - a transmissão sem fio, inclusive por satélites, de sons ou imagens e sons ou das representações desses, para recepção ao público e a transmissão de sinais codificados, quando os meios de decodificação sejam oferecidos ao público pelo organismo de radiodifusão ou com seu consentimento;

XIII - artistas intérpretes ou executantes - todos os atores, cantores, músicos, bailarinos ou outras pessoas que representem um papel, cantem, recitem, declamem, interpretem ou executem em qualquer forma obras literárias ou artísticas ou expressões do folclore.

Art. 6º Não serão de domínio da União, dos Estados, do Distrito Federal ou dos Municípios as obras por eles simplesmente subvencionadas.

Título II

Das Obras Intelectuais

Capítulo I

Das Obras Protegidas

Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:

I - os textos de obras literárias, artísticas ou científicas;

II - as conferências, alocuções, sermões e outras obras da mesma natureza;

III - as obras dramáticas e dramático-musicais;

IV - as obras coreográficas e pantomímicas, cuja execução cênica se fixe por escrito ou por outra qualquer forma;

V - as composições musicais, tenham ou não letra;

VI - as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas;

VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia;

VIII - as obras de desenho, pintura, gravura, escultura, litografia e arte cinética;

IX - as ilustrações, cartas geográficas e outras obras da mesma natureza;

X - os projetos, esboços e obras plásticas concernentes à geografia, engenharia, topografia, arquitetura, paisagismo, cenografia e ciência;

XI - as adaptações, traduções e outras transformações de obras originais, apresentadas como criação intelectual nova;

XII - os programas de computador;

XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

§ 1º Os programas de computador são objeto de legislação específica, observadas as disposições desta Lei que lhes sejam aplicáveis.

§ 2º A proteção concedida no inciso XIII não abarca os dados ou materiais em si mesmos e se entende sem prejuízo de quaisquer direitos autorais que subsistam a respeito dos dados ou materiais contidos nas obras.

§ 3º No domínio das ciências, a proteção recairá sobre a forma literária ou artística, não abrangendo o seu conteúdo científico ou técnico, sem prejuízo dos direitos que protegem os demais campos da propriedade imaterial.

Art. 8º Não são objeto de proteção como direitos autorais de que trata esta Lei:

I - as idéias, procedimentos normativos, sistemas, métodos, projetos ou conceitos matemáticos como tais;

II - os esquemas, planos ou regras para realizar atos mentais, jogos ou negócios;

III - os formulários em branco para serem preenchidos por qualquer tipo de informação, científica ou não, e suas instruções;

IV - os textos de tratados ou convenções, leis, decretos, regulamentos, decisões judiciais e demais atos oficiais;

V - as informações de uso comum tais como calendários, agendas, cadastros ou legendas;

VI - os nomes e títulos isolados;

VII - o aproveitamento industrial ou comercial das idéias contidas nas obras.

Art. 9º À cópia de obra de arte plástica feita pelo próprio autor é assegurada a mesma proteção de que goza o original.

Art. 10. A proteção à obra intelectual abrange o seu título, se original e inconfundível com o de obra do mesmo gênero, divulgada anteriormente por outro autor.

Parágrafo único. O título de publicações periódicas, inclusive jornais, é protegido até um ano após a saída do seu último número, salvo se forem anuais, caso em que esse prazo se elevará a dois anos.

Capítulo II

Da Autoria das Obras Intelectuais

Art. 11. Autor é a pessoa física criadora de obra literária, artística ou científica.

Parágrafo único. A proteção concedida ao autor poderá aplicar-se às pessoas jurídicas nos casos previstos nesta Lei.

Art. 12. Para se identificar como autor, poderá o criador da obra literária, artística ou científica usar de seu nome civil, completo ou abreviado até por suas iniciais, de pseudônimo ou qualquer outro sinal convencional.

Art. 13. Considera-se autor da obra intelectual, não havendo prova em contrário, aquele que, por uma das modalidades de identificação referidas no artigo anterior, tiver, em conformidade com o uso, indicada ou anunciada essa qualidade na sua utilização.

Art. 14. É titular de direitos de autor quem adapta, traduz, arranja ou orquestra obra caída no domínio público, não podendo opor-se a outra adaptação, arranjo, orquestração ou tradução, salvo se for cópia da sua.

Art. 15. A co-autoria da obra é atribuída àqueles em cujo nome, pseudônimo ou sinal convencional for utilizada.

§ 1º Não se considera co-autor quem simplesmente auxiliou o autor na produção da obra literária, artística ou científica, revendo-a, atualizando-a, bem como fiscalizando ou dirigindo sua edição ou apresentação por qualquer meio.

§ 2º Ao co-autor, cuja contribuição possa ser utilizada separadamente, são asseguradas todas as faculdades inerentes à sua criação como obra individual, vedada, porém, a utilização que possa acarretar prejuízo à exploração da obra comum.

Art. 16. São co-autores da obra audiovisual o autor do assunto ou argumento literário, musical ou lítero-musical e o diretor.

Parágrafo único. Consideram-se co-autores de desenhos animados os que criam os desenhos utilizados na obra audiovisual.

Art. 17. É assegurada a proteção às participações individuais em obras coletivas.

§ 1º Qualquer dos participantes, no exercício de seus direitos morais, poderá proibir que se indique ou anuncie seu nome na obra coletiva, sem prejuízo do direito de haver a remuneração contratada.

§ 2º Cabe ao organizador a titularidade dos direitos patrimoniais sobre o conjunto da obra coletiva.

§ 3º O contrato com o organizador especificará a contribuição do participante, o prazo para entrega ou realização, a remuneração e demais condições para sua execução.

Capítulo III

Do Registro das Obras Intelectuais

Art. 18. A proteção aos direitos de que trata esta Lei independe de registro.

Art. 19. É facultado ao autor registrar a sua obra no órgão público definido no *caput* e no § 1º do art. 17 da Lei nº 5.988, de 14 de dezembro de 1973.

Art. 20. Para os serviços de registro previstos nesta Lei será cobrada retribuição, cujo valor e processo de recolhimento serão estabelecidos por ato do titular do órgão da administração pública federal a que estiver vinculado o registro das obras intelectuais.

Art. 21. Os serviços de registro de que trata esta Lei serão organizados conforme preceitua o § 2º do art. 17 da Lei nº 5.988, de 14 de dezembro de 1973.

Título III

Dos Direitos do Autor

Capítulo I

Disposições Preliminares

Art. 22. Pertencem ao autor os direitos morais e patrimoniais sobre a obra que criou.

Art. 23. Os co-autores da obra intelectual exercerão, de comum acordo, os seus direitos, salvo convenção em contrário.

Capítulo II

Dos Direitos Morais do Autor

Art. 24. São direitos morais do autor:

I - o de reivindicar, a qualquer tempo, a autoria da obra;

II - o de ter seu nome, pseudônimo ou sinal convencional indicado ou anunciado, como sendo o do autor, na utilização de sua obra;

III - o de conservar a obra inédita;

IV - o de assegurar a integridade da obra, opondo-se a quaisquer modificações ou à prática de atos que, de qualquer forma, possam prejudicá-la ou atingi-lo, como autor, em sua reputação ou honra;

V - o de modificar a obra, antes ou depois de utilizada;

VI - o de retirar de circulação a obra ou de suspender qualquer forma de utilização já autorizada, quando a circulação ou utilização implicarem afronta à sua reputação e imagem;

VII - o de ter acesso a exemplar único e raro da obra, quando se encontre legitimamente em poder de outrem, para o fim de, por meio de processo fotográfico ou assemelhado, ou audiovisual, preservar sua memória, de forma que cause o menor inconveniente possível a seu detentor, que, em todo caso, será indenizado de qualquer dano ou prejuízo que lhe seja causado.

§ 1º Por morte do autor, transmitem-se a seus sucessores os direitos a que se referem os incisos I a IV.

§ 2º Compete ao Estado a defesa da integridade e autoria da obra caída em domínio público.

§ 3º Nos casos dos incisos V e VI, ressalvam-se as prévias indenizações a terceiros, quando couberem.

Art. 25. Cabe exclusivamente ao diretor o exercício dos direitos morais sobre a obra audiovisual.

Art. 26. O autor poderá repudiar a autoria de projeto arquitetônico alterado sem o seu consentimento durante a execução ou após a conclusão da construção.

Parágrafo único. O proprietário da construção responde pelos danos que

causar ao autor sempre que, após o repúdio, der como sendo daquele a autoria do projeto repudiado.

Art. 27. Os direitos morais do autor são inalienáveis e irrenunciáveis.

Capítulo III

Dos Direitos Patrimoniais do Autor e de sua Duração

Art. 28. Cabe ao autor o direito exclusivo de utilizar, fruir e dispor da obra literária, artística ou científica.

Art. 29. Depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, tais como:

I - a reprodução parcial ou integral;

II - a edição;

III - a adaptação, o arranjo musical e quaisquer outras transformações;

IV - a tradução para qualquer idioma;

V - a inclusão em fonograma ou produção audiovisual;

VI - a distribuição, quando não intrínseca ao contrato firmado pelo autor com terceiros para uso ou exploração da obra;

VII - a distribuição para oferta de obras ou produções mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para percebê-la em um tempo e lugar previamente determinados por quem formula a demanda, e nos casos em que o acesso às obras ou produções se faça por qualquer sistema que importe em pagamento pelo usuário;

VIII - a utilização, direta ou indireta, da obra literária, artística ou científica, mediante:

a) representação, recitação ou declamação;

b) execução musical;

c) emprego de alto-falante ou de sistemas análogos;

d) radiodifusão sonora ou televisiva;

e) captação de transmissão de radiodifusão em locais de freqüência coletiva;

f) sonorização ambiental;

g) a exibição audiovisual, cinematográfica ou por processo assemelhado;

h) emprego de satélites artificiais;

i) emprego de sistemas óticos, fios telefônicos ou não, cabos de qualquer tipo e meios de comunicação similares que venham a ser adotados;

j) exposição de obras de artes plásticas e figurativas;

IX - a inclusão em base de dados, o armazenamento em computador, a microfilmagem e as demais formas de arquivamento do gênero;

X - quaisquer outras modalidades de utilização existentes ou que venham a ser inventadas.

Art. 30. No exercício do direito de reprodução, o titular dos direitos autorais poderá colocar à disposição do público a obra, na forma, local e pelo tempo que desejar, a título oneroso ou gratuito.

§ 1º O direito de exclusividade de reprodução não será aplicável quando ela for temporária e apenas tiver o propósito de tornar a obra, fonograma ou interpretação perceptível em meio eletrônico ou quando for de natureza transitória e incidental, desde que ocorra no curso do uso devidamente autorizado da obra, pelo titular.

§ 2º Em qualquer modalidade de reprodução, a quantidade de exemplares será informada e controlada, cabendo a quem reproduzir a obra a responsabilidade de manter os registros que permitam, ao autor, a fiscalização do aproveitamento econômico da exploração.

Art. 31. As diversas modalidades de utilização de obras literárias, artísticas ou científicas ou de fonogramas são independentes entre si, e a autorização concedida pelo autor, ou pelo produtor, respectivamente, não se estende a quaisquer das demais.

Art. 32. Quando uma obra feita em regime de co-autoria não for divisível, nenhum dos co-autores, sob pena de responder por perdas e danos, poderá, sem consentimento dos demais, publicá-la ou autorizar-lhe a publicação, salvo na coleção de suas obras completas.

§ 1º Havendo divergência, os co-autores decidirão por maioria.

§ 2º Ao co-autor dissidente é assegurado o direito de não contribuir para as despesas de publicação, renunciando a sua parte nos lucros, e o de vedar que se inscreva seu nome na obra.

§ 3º Cada co-autor pode, individualmente, sem aquiescência dos outros, registrar a obra e defender os próprios direitos contra terceiros.

Art. 33. Ninguém pode reproduzir obra que não pertença ao domínio público, a pretexto de anotá-la, comentá-la ou melhorá-la, sem permissão do autor.

Parágrafo único. Os comentários ou anotações poderão ser publicados separadamente.

Art. 34. As cartas missivas, cuja publicação está condicionada à permissão do autor, poderão ser juntadas como documento de prova em processos administrativos e judiciais.

Art. 35. Quando o autor, em virtude de revisão, tiver dado à obra versão definitiva, não poderão seus sucessores reproduzir versões anteriores.

Art. 36. O direito de utilização econômica dos escritos publicados pela imprensa, diária ou periódica, com exceção dos assinados ou que apresentem sinal de reserva, pertence ao editor, salvo convenção em contrário.

Parágrafo único. A autorização para utilização econômica de artigos assinados, para publicação em diários e periódicos, não produz efeito além do prazo da periodicidade acrescido de vinte dias, a contar de sua publicação, findo o qual recobra o autor o seu direito.

Art. 37. A aquisição do original de uma obra, ou de exemplar, não confere ao adquirente qualquer dos direitos patrimoniais do autor, salvo convenção em contrário entre as partes e os casos previstos nesta Lei.

Art. 38. O autor tem o direito, irrenunciável e inalienável, de perceber, no mínimo, cinco por cento sobre o aumento do preço eventualmente verificável em cada revenda de obra de arte ou manuscrito, sendo originais, que houver alienado.

Parágrafo único. Caso o autor não perceba o seu direito de seqüência no ato da revenda, o vendedor é considerado depositário da quantia a ele devida, salvo se a operação for realizada por leiloeiro, quando será este o depositário.

Art. 39. Os direitos patrimoniais do autor, excetuados os rendimentos resultantes de sua exploração, não se comunicam, salvo pacto antenupcial em contrário.

Art. 40. Tratando-se de obra anônima ou pseudônima, caberá a quem publicá-la o exercício dos direitos patrimoniais do autor.

Parágrafo único. O autor que se der a conhecer assumirá o exercício dos direitos patrimoniais, ressalvados os direitos adquiridos por terceiros.

Art. 41. Os direitos patrimoniais do autor perduram por setenta anos contados de 1° de janeiro do ano subseqüente ao de seu falecimento, obedecida a ordem sucessória da lei civil.

Parágrafo único. Aplica-se às obras póstumas o prazo de proteção a que alude o *caput* deste artigo.

Art. 42. Quando a obra literária, artística ou científica realizada em co-autoria for indivisível, o prazo previsto no artigo anterior será contado da morte do último dos co-autores sobreviventes.

Parágrafo único. Acrescer-se-ão aos dos sobreviventes os direitos do co-autor que falecer sem sucessores.

Art. 43. Será de setenta anos o prazo de proteção aos direitos patrimoniais sobre as obras anônimas ou pseudônimas, contado de 1° de janeiro do ano imediatamente posterior ao da primeira publicação.

Parágrafo único. Aplicar-se-á o disposto no art. 41 e seu parágrafo único, sempre que o autor se der a conhecer antes do termo do prazo previsto no *caput* deste artigo.

Art. 44. O prazo de proteção aos direitos patrimoniais sobre obras audiovisuais e fotográficas será de setenta anos, a contar de 1° de janeiro do ano subseqüente ao de sua divulgação.

Art. 45. Além das obras em relação às quais decorreu o prazo de proteção aos direitos patrimoniais, pertencem ao domínio público:

I - as de autores falecidos que não tenham deixado sucessores;

II - as de autor desconhecido, ressalvada a proteção legal aos conhecimentos étnicos e tradicionais.

Capítulo IV

Das Limitações aos Direitos Autorais

Art. 46. Não constitui ofensa aos direitos autorais:

I - a reprodução:

a) na imprensa diária ou periódica, de notícia ou de artigo informativo, publicado em diários ou periódicos, com a menção do nome do autor, se assinados, e da publicação de onde foram transcritos;

b) em diários ou periódicos, de discursos pronunciados em reuniões públicas de qualquer natureza;

c) de retratos, ou de outra forma de representação da imagem, feitos sob encomenda, quando realizada pelo proprietário do objeto encomendado, não havendo a oposição da pessoa neles representada ou de seus herdeiros;

d) de obras literárias, artísticas ou científicas, para uso exclusivo de deficientes visuais, sempre que a reprodução, sem fins comerciais, seja feita mediante o sistema Braille ou outro procedimento em qualquer suporte para esses destinatários;

II - a reprodução, em um só exemplar de pequenos trechos, para uso privado do copista, desde que feita por este, sem intuito de lucro;

III - a citação em livros, jornais, revistas ou qualquer outro meio de comunicação, de passagens de qualquer obra, para fins de estudo, crítica ou polêmica, na medida justificada para o fim a atingir, indicando-se o nome do autor e a origem da obra;

IV - o apanhado de lições em estabelecimentos de ensino por aqueles a quem elas se dirigem, vedada sua publicação, integral ou parcial, sem autorização prévia e expressa de quem as ministrou;

V - a utilização de obras literárias, artísticas ou científicas, fonogramas e transmissão de rádio e televisão em estabelecimentos comerciais, exclusivamente

para demonstração à clientela, desde que esses estabelecimentos comercializem os suportes ou equipamentos que permitam a sua utilização;

VI - a representação teatral e a execução musical, quando realizadas no recesso familiar ou, para fins exclusivamente didáticos, nos estabelecimentos de ensino, não havendo em qualquer caso intuito de lucro;

VII - a utilização de obras literárias, artísticas ou científicas para produzir prova judiciária ou administrativa;

VIII - a reprodução, em quaisquer obras, de pequenos trechos de obras preexistentes, de qualquer natureza, ou de obra integral, quando de artes plásticas, sempre que a reprodução em si não seja o objetivo principal da obra nova e que não prejudique a exploração normal da obra reproduzida nem cause um prejuízo injustificado aos legítimos interesses dos autores.

Art. 47. São livres as paráfrases e paródias que não forem verdadeiras reproduções da obra originária nem lhe implicarem descrédito.

Art. 48. As obras situadas permanentemente em logradouros públicos podem ser representadas livremente, por meio de pinturas, desenhos, fotografias e procedimentos audiovisuais.

Capítulo V

Da Transferência dos Direitos de Autor

Art. 49. Os direitos de autor poderão ser total ou parcialmente transferidos a terceiros, por ele ou por seus sucessores, a título universal ou singular, pessoalmente ou por meio de representantes com poderes especiais, por meio de licenciamento, concessão, cessão ou por outros meios admitidos em Direito, obedecidas as seguintes limitações:

I - a transmissão total compreende todos os direitos de autor, salvo os de natureza moral e os expressamente excluídos por lei;

II - somente se admitirá transmissão total e definitiva dos direitos mediante estipulação contratual escrita;

III - na hipótese de não haver estipulação contratual escrita, o prazo máximo será de cinco anos;

IV - a cessão será válida unicamente para o país em que se firmou o contrato, salvo estipulação em contrário;

V - a cessão só se operará para modalidades de utilização já existentes à data do contrato;

VI - não havendo especificações quanto à modalidade de utilização, o contrato

será interpretado restritivamente, entendendo-se como limitada apenas a uma que seja aquela indispensável ao cumprimento da finalidade do contrato.

Art. 50. A cessão total ou parcial dos direitos de autor, que se fará sempre por escrito, presume-se onerosa.

§ 1º Poderá a cessão ser averbada à margem do registro a que se refere o art. 19 desta Lei, ou, não estando a obra registrada, poderá o instrumento ser registrado em Cartório de Títulos e Documentos.

§ 2º Constarão do instrumento de cessão como elementos essenciais seu objeto e as condições de exercício do direito quanto a tempo, lugar e preço.

Art. 51. A cessão dos direitos de autor sobre obras futuras abrangerá, no máximo, o período de cinco anos.

Parágrafo único. O prazo será reduzido a cinco anos sempre que indeterminado ou superior, diminuindo-se, na devida proporção, o preço estipulado.

Art. 52. A omissão do nome do autor, ou de co-autor, na divulgação da obra não presume o anonimato ou a cessão de seus direitos.

Título IV

Da Utilização de Obras Intelectuais e dos Fonogramas

Capítulo I

Da Edição

Art. 53. Mediante contrato de edição, o editor, obrigando-se a reproduzir e a divulgar a obra literária, artística ou científica, fica autorizado, em caráter de exclusividade, a publicá-la e a explorá-la pelo prazo e nas condições pactuadas com o autor.

Parágrafo único. Em cada exemplar da obra o editor mencionará:

I - o título da obra e seu autor;

II - no caso de tradução, o título original e o nome do tradutor;

III - o ano de publicação;

IV - o seu nome ou marca que o identifique.

Art. 54. Pelo mesmo contrato pode o autor obrigar-se à feitura de obra literária, artística ou científica em cuja publicação e divulgação se empenha o editor.

Art. 55. Em caso de falecimento ou de impedimento do autor para concluir a obra, o editor poderá:

I - considerar resolvido o contrato, mesmo que tenha sido entregue parte considerável da obra;

II - editar a obra, sendo autônoma, mediante pagamento proporcional do preço;

III - mandar que outro a termine, desde que consintam os sucessores e seja o fato indicado na edição.

Parágrafo único. É vedada a publicação parcial, se o autor manifestou a vontade de só publicá-la por inteiro ou se assim o decidirem seus sucessores.

Art. 56. Entende-se que o contrato versa apenas sobre uma edição, se não houver cláusula expressa em contrário.

Parágrafo único. No silêncio do contrato, considera-se que cada edição se constitui de três mil exemplares.

Art. 57. O preço da retribuição será arbitrado, com base nos usos e costumes, sempre que no contrato não a tiver estipulado expressamente o autor.

Art. 58. Se os originais forem entregues em desacordo com o ajustado e o editor não os recusar nos trinta dias seguintes ao do recebimento, ter-se-ão por aceitas as alterações introduzidas pelo autor.

Art. 59. Quaisquer que sejam as condições do contrato, o editor é obrigado a facultar ao autor o exame da escrituração na parte que lhe corresponde, bem como a informá-lo sobre o estado da edição.

Art. 60. Ao editor compete fixar o preço da venda, sem, todavia, poder elevá-lo a ponto de embaraçar a circulação da obra.

Art. 61. O editor será obrigado a prestar contas mensais ao autor sempre que a retribuição deste estiver condicionada à venda da obra, salvo se prazo diferente houver sido convencionado.

Art. 62. A obra deverá ser editada em dois anos da celebração do contrato, salvo prazo diverso estipulado em convenção.

Parágrafo único. Não havendo edição da obra no prazo legal ou contratual, poderá ser rescindido o contrato, respondendo o editor por danos causados.

Art. 63. Enquanto não se esgotarem as edições a que tiver direito o editor, não poderá o autor dispor de sua obra, cabendo ao editor o ônus da prova.

§ 1º Na vigência do contrato de edição, assiste ao editor o direito de exigir que se retire de circulação edição da mesma obra feita por outrem.

§ 2º Considera-se esgotada a edição quando restarem em estoque, em poder do editor, exemplares em número inferior a dez por cento do total da edição.

Art. 64. Somente decorrido um ano de lançamento da edição, o editor poderá vender, como saldo, os exemplares restantes, desde que o autor seja notificado de que, no prazo de trinta dias, terá prioridade na aquisição dos referidos exemplares pelo preço de saldo.

Art. 65. Esgotada a edição, e o editor, com direito a outra, não a publicar, poderá o autor notificá-lo a que o faça em certo prazo, sob pena de perder aquele direito, além de responder por danos.

Art. 66. O autor tem o direito de fazer, nas edições sucessivas de suas obras, as emendas e alterações que bem lhe aprouver.

Parágrafo único. O editor poderá opor-se às alterações que lhe prejudiquem os interesses, ofendam sua reputação ou aumentem sua responsabilidade.

Art. 67. Se, em virtude de sua natureza, for imprescindível a atualização da obra em novas edições, o editor, negando-se o autor a fazê-la, dela poderá encarregar outrem, mencionando o fato na edição.

Capítulo II

Da Comunicação ao Público

Art. 68. Sem prévia e expressa autorização do autor ou titular, não poderão ser utilizadas obras teatrais, composições musicais ou lítero-musicais e fonogramas, em representações e execuções públicas.

§ 1º Considera-se representação pública a utilização de obras teatrais no gênero drama, tragédia, comédia, ópera, opereta, balé, pantomimas e assemelhadas, musicadas ou não, mediante a participação de artistas, remunerados ou não, em locais de freqüência coletiva ou pela radiodifusão, transmissão e exibição cinematográfica.

§ 2º Considera-se execução pública a utilização de composições musicais ou lítero-musicais, mediante a participação de artistas, remunerados ou não, ou a utilização de fonogramas e obras audiovisuais, em locais de freqüência coletiva, por quaisquer processos, inclusive a radiodifusão ou transmissão por qualquer modalidade, e a exibição cinematográfica.

§ 3º Consideram-se locais de freqüência coletiva os teatros, cinemas, salões de baile ou concertos, boates, bares, clubes ou associações de qualquer natureza, lojas, estabelecimentos comerciais e industriais, estádios, circos, feiras, restaurantes, hotéis, motéis, clínicas, hospitais, órgãos públicos da administração direta ou indireta, fundacionais e estatais, meios de transporte de passageiros terrestre, marítimo, fluvial ou aéreo, ou onde quer que se representem, executem ou transmitam obras literárias, artísticas ou científicas.

§ 4º Previamente à realização da execução pública, o empresário deverá apresentar ao escritório central, previsto no art. 99, a comprovação dos recolhimentos relativos aos direitos autorais.

§ 5º Quando a remuneração depender da freqüência do público, poderá o empresário, por convênio com o escritório central, pagar o preço após a realização da execução pública.

§ 6º O empresário entregará ao escritório central, imediatamente após a execução pública ou transmissão, relação completa das obras e fonogramas utilizados, indicando os nomes dos respectivos autores, artistas e produtores.

§ 7º As empresas cinematográficas e de radiodifusão manterão à imediata disposição dos interessados, cópia autêntica dos contratos, ajustes ou acordos, individuais ou coletivos, autorizando e disciplinando a remuneração por execução pública das obras musicais e fonogramas contidas em seus programas ou obras audiovisuais.

Art. 69. O autor, observados os usos locais, notificará o empresário do prazo para a representação ou execução, salvo prévia estipulação convencional.

Art. 70. Ao autor assiste o direito de opor-se à representação ou execução que não seja suficientemente ensaiada, bem como fiscalizá-la, tendo, para isso, livre acesso durante as representações ou execuções, no local onde se realizam.

Art. 71. O autor da obra não pode alterar-lhe a substância, sem acordo com o empresário que a faz representar.

Art. 72. O empresário, sem licença do autor, não pode entregar a obra a pessoa estranha à representação ou à execução.

Art. 73. Os principais intérpretes e os diretores de orquestras ou coro, escolhidos de comum acordo pelo autor e pelo produtor, não podem ser substituídos por ordem deste, sem que aquele consinta.

Art. 74. O autor de obra teatral, ao autorizar a sua tradução ou adaptação, poderá fixar prazo para utilização dela em representações públicas.

Parágrafo único. Após o decurso do prazo a que se refere este artigo, não poderá opor-se o tradutor ou adaptador à utilização de outra tradução ou adaptação autorizada, salvo se for cópia da sua.

Art. 75. Autorizada a representação de obra teatral feita em co-autoria, não poderá qualquer dos co-autores revogar a autorização dada, provocando a suspensão da temporada contratualmente ajustada.

Art. 76. É impenhorável a parte do produto dos espetáculos reservada ao autor e aos artistas.

Capítulo III

Da Utilização da Obra de Arte Plástica

Art. 77. Salvo convenção em contrário, o autor de obra de arte plástica, ao alienar o objeto em que ela se materializa, transmite o direito de expô-la, mas não transmite ao adquirente o direito de reproduzi-la.

Art. 78. A autorização para reproduzir obra de arte plástica, por qualquer processo, deve se fazer por escrito e se presume onerosa.

Capítulo IV

Da Utilização da Obra Fotográfica

Art. 79. O autor de obra fotográfica tem direito a reproduzi-la e colocá-la à venda, observadas as restrições à exposição, reprodução e venda de retratos, e sem prejuízo dos direitos de autor sobre a obra fotografada, se de artes plásticas protegidas.

§ 1º A fotografia, quando utilizada por terceiros, indicará de forma legível o nome do seu autor.

§ 2º É vedada a reprodução de obra fotográfica que não esteja em absoluta consonância com o original, salvo prévia autorização do autor.

Capítulo V

Da Utilização de Fonograma

Art. 80. Ao publicar o fonograma, o produtor mencionará em cada exemplar:

I - o título da obra incluída e seu autor;

II - o nome ou pseudônimo do intérprete;

III - o ano de publicação;

IV - o seu nome ou marca que o identifique.

Capítulo VI

Da Utilização da Obra Audiovisual

Art. 81. A autorização do autor e do intérprete de obra literária, artística ou científica para produção audiovisual implica, salvo disposição em contrário, consentimento para sua utilização econômica.

§ 1º A exclusividade da autorização depende de cláusula expressa e cessa dez anos após a celebração do contrato.

§ 2º Em cada cópia da obra audiovisual, mencionará o produtor:

I - o título da obra audiovisual;

II - os nomes ou pseudônimos do diretor e dos demais co-autores;

III - o título da obra adaptada e seu autor, se for o caso;

IV - os artistas intérpretes;

V - o ano de publicação;

VI - o seu nome ou marca que o identifique.

Art. 82. O contrato de produção audiovisual deve estabelecer:

I - a remuneração devida pelo produtor aos co-autores da obra e aos artistas intérpretes e executantes, bem como o tempo, lugar e forma de pagamento;

II - o prazo de conclusão da obra;

III - a responsabilidade do produtor para com os co-autores, artistas intérpretes ou executantes, no caso de co-produção.

Art. 83. O participante da produção da obra audiovisual que interromper, temporária ou definitivamente, sua atuação, não poderá opor-se a que esta seja utilizada na obra nem a que terceiro o substitua, resguardados os direitos que adquiriu quanto à parte já executada.

Art. 84. Caso a remuneração dos co-autores da obra audiovisual dependa dos rendimentos de sua utilização econômica, o produtor lhes prestará contas semestralmente, se outro prazo não houver sido pactuado.

Art. 85. Não havendo disposição em contrário, poderão os co-autores da obra audiovisual utilizar-se, em gênero diverso, da parte que constitua sua contribuição pessoal.

Parágrafo único. Se o produtor não concluir a obra audiovisual no prazo ajustado ou não iniciar sua exploração dentro de dois anos, a contar de sua conclusão, a utilização a que se refere este artigo será livre.

Art. 86. Os direitos autorais de execução musical relativos a obras musicais, lítero-musicais e fonogramas incluídos em obras audiovisuais serão devidos aos seus titulares pelos responsáveis dos locais ou estabelecimentos a que alude o § 3o do art. 68 desta Lei, que as exibirem, ou pelas emissoras de televisão que as transmitirem.

Capítulo VII

Da Utilização de Bases de Dados

Art. 87. O titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da referida base, de autorizar ou proibir:

I - sua reprodução total ou parcial, por qualquer meio ou processo;

II - sua tradução, adaptação, reordenação ou qualquer outra modificação;

III - a distribuição do original ou cópias da base de dados ou a sua comunicação ao público;

IV - a reprodução, distribuição ou comunicação ao público dos resultados das operações mencionadas no inciso II deste artigo.

Capítulo VIII

Da Utilização da Obra Coletiva

Art. 88. Ao publicar a obra coletiva, o organizador mencionará em cada exemplar:

I - o título da obra;

II - a relação de todos os participantes, em ordem alfabética, se outra não houver sido convencionada;

III - o ano de publicação;

IV - o seu nome ou marca que o identifique.

Parágrafo único. Para valer-se do disposto no § 1º do art. 17, deverá o participante notificar o organizador, por escrito, até a entrega de sua participação.

Título V

Dos Direitos Conexos

Capítulo I

Disposições Preliminares

Art. 89. As normas relativas aos direitos de autor aplicam-se, no que couber, aos direitos dos artistas intérpretes ou executantes, dos produtores fonográficos e das empresas de radiodifusão.

Parágrafo único. A proteção desta Lei aos direitos previstos neste artigo deixa intactas e não afeta as garantias asseguradas aos autores das obras literárias, artísticas ou científicas.

Capítulo II

Dos Direitos dos Artistas Intérpretes ou Executantes

Art. 90. Tem o artista intérprete ou executante o direito exclusivo de, a título oneroso ou gratuito, autorizar ou proibir:

I - a fixação de suas interpretações ou execuções;

II - a reprodução, a execução pública e a locação das suas interpretações ou execuções fixadas;

III - a radiodifusão das suas interpretações ou execuções, fixadas ou não;

IV - a colocação à disposição do público de suas interpretações ou execuções, de maneira que qualquer pessoa a elas possa ter acesso, no tempo e no lugar que individualmente escolherem;

V - qualquer outra modalidade de utilização de suas interpretações ou execuções.

§ 1º Quando na interpretação ou na execução participarem vários artistas, seus direitos serão exercidos pelo diretor do conjunto.

§ 2º A proteção aos artistas intérpretes ou executantes estende-se à reprodução da voz e imagem, quando associadas às suas atuações.

Art. 91. As empresas de radiodifusão poderão realizar fixações de interpretação ou execução de artistas que as tenham permitido para utilização em determinado número de emissões, facultada sua conservação em arquivo público.

Parágrafo único. A reutilização subseqüente da fixação, no País ou no exterior, somente será lícita mediante autorização escrita dos titulares de bens intelectuais incluídos no programa, devida uma remuneração adicional aos titulares para cada nova utilização.

Art. 92. Aos intérpretes cabem os direitos morais de integridade e paternidade de suas interpretações, inclusive depois da cessão dos direitos patrimoniais, sem prejuízo da redução, compactação, edição ou dublagem da obra de que tenham participado, sob a responsabilidade do produtor, que não poderá desfigurar a interpretação do artista.

Parágrafo único. O falecimento de qualquer participante de obra audiovisual, concluída ou não, não obsta sua exibição e aproveitamento econômico, nem exige autorização adicional, sendo a remuneração prevista para o falecido, nos termos do contrato e da lei, efetuada a favor do espólio ou dos sucessores.

Capítulo III

Dos Direitos dos Produtores Fonográficos

Art. 93. O produtor de fonogramas tem o direito exclusivo de, a título oneroso ou gratuito, autorizar-lhes ou proibir-lhes:

I - a reprodução direta ou indireta, total ou parcial;

II - a distribuição por meio da venda ou locação de exemplares da reprodução;

III - a comunicação ao público por meio da execução pública, inclusive pela radiodifusão;

IV - (VETADO)

V - quaisquer outras modalidades de utilização, existentes ou que venham a ser inventadas.

Art. 94. Cabe ao produtor fonográfico perceber dos usuários a que se refere o art. 68, e parágrafos, desta Lei os proventos pecuniários resultantes da execução pública dos fonogramas e reparti-los com os artistas, na forma convencionada entre eles ou suas associações.

Capítulo IV

Dos Direitos das Empresas de Radiodifusão

Art. 95. Cabe às empresas de radiodifusão o direito exclusivo de autorizar ou proibir a retransmissão, fixação e reprodução de suas emissões, bem como a comunicação ao público, pela televisão, em locais de freqüência coletiva, sem prejuízo dos direitos dos titulares de bens intelectuais incluídos na programação.

Capítulo V

Da Duração dos Direitos Conexos

Art. 96. É de setenta anos o prazo de proteção aos direitos conexos, contados a partir de 1º de janeiro do ano subseqüente à fixação, para os fonogramas; à transmissão, para as emissões das empresas de radiodifusão; e à execução e representação pública, para os demais casos.

Título VI

Das Associações de Titulares de Direitos de Autor e dos que lhes são Conexos

Art. 97. Para o exercício e defesa de seus direitos, podem os autores e os titulares de direitos conexos associar-se sem intuito de lucro.

§ 1º É vedado pertencer a mais de uma associação para a gestão coletiva de direitos da mesma natureza.

§ 2º Pode o titular transferir-se, a qualquer momento, para outra associação, devendo comunicar o fato, por escrito, à associação de origem.

§ 3º As associações com sede no exterior far-se-ão representar, no País, por associações nacionais constituídas na forma prevista nesta Lei.

Art. 98. Com o ato de filiação, as associações tornam-se mandatárias de seus associados para a prática de todos os atos necessários à defesa judicial ou extrajudicial de seus direitos autorais, bem como para sua cobrança.

Parágrafo único. Os titulares de direitos autorais poderão praticar, pessoalmente, os atos referidos neste artigo, mediante comunicação prévia à associação a que estiverem filiados.

Art. 99. As associações manterão um único escritório central para a arrecadação e distribuição, em comum, dos direitos relativos à execução pública das obras musicais e lítero-musicais e de fonogramas, inclusive por meio da radiodifusão e transmissão por qualquer modalidade, e da exibição de obras audiovisuais.

§ 1º O escritório central organizado na forma prevista neste artigo não terá finalidade de lucro e será dirigido e administrado pelas associações que o integrem.

§ 2º O escritório central e as associações a que se refere este Título atuarão em juízo e fora dele em seus próprios nomes como substitutos processuais dos titulares a eles vinculados.

§ 3º O recolhimento de quaisquer valores pelo escritório central somente se fará por depósito bancário.

§ 4º O escritório central poderá manter fiscais, aos quais é vedado receber do empresário numerário a qualquer título.

§ 5º A inobservância da norma do parágrafo anterior tornará o faltoso inabilitado à função de fiscal, sem prejuízo das sanções civis e penais cabíveis.

Art. 100. O sindicato ou associação profissional que congregue não menos de um terço dos filiados de uma associação autoral poderá, uma vez por ano, após notificação, com oito dias de antecedência, fiscalizar, por intermédio de auditor, a exatidão das contas prestadas a seus representados.

Título VII

Das Sanções às Violações dos Direitos Autorais

Capítulo I

Disposição Preliminar

Art. 101. As sanções civis de que trata este Capítulo aplicam-se sem prejuízo das penas cabíveis.

Capítulo II

Das Sanções Civis

Art. 102. O titular cuja obra seja fraudulentamente reproduzida, divulgada ou de qualquer forma utilizada, poderá requerer a apreensão dos exemplares reproduzidos ou a suspensão da divulgação, sem prejuízo da indenização cabível.

Art. 103. Quem editar obra literária, artística ou científica, sem autorização do titular, perderá para este os exemplares que se apreenderem e pagar-lhe-á o preço dos que tiver vendido.

Parágrafo único. Não se conhecendo o número de exemplares que constituem a edição fraudulenta, pagará o transgressor o valor de três mil exemplares, além dos apreendidos.

Art. 104. Quem vender, expuser a venda, ocultar, adquirir, distribuir, tiver em depósito ou utilizar obra ou fonograma reproduzidos com fraude, com a finalidade de vender, obter ganho, vantagem, proveito, lucro direto ou indireto, para si ou para outrem, será solidariamente responsável com o contrafator, nos termos dos artigos precedentes, respondendo como contrafatores o importador e o distribuidor em caso de reprodução no exterior.

Art. 105. A transmissão e a retransmissão, por qualquer meio ou processo, e a comunicação ao público de obras artísticas, literárias e científicas, de interpretações

e de fonogramas, realizadas mediante violação aos direitos de seus titulares, deverão ser imediatamente suspensas ou interrompidas pela autoridade judicial competente, sem prejuízo da multa diária pelo descumprimento e das demais indenizações cabíveis, independentemente das sanções penais aplicáveis; caso se comprove que o infrator é reincidente na violação aos direitos dos titulares de direitos de autor e conexos, o valor da multa poderá ser aumentado até o dobro.

Art. 106. A sentença condenatória poderá determinar a destruição de todos os exemplares ilícitos, bem como as matrizes, moldes, negativos e demais elementos utilizados para praticar o ilícito civil, assim como a perda de máquinas, equipamentos e insumos destinados a tal fim ou, servindo eles unicamente para o fim ilícito, sua destruição.

Art. 107. Independentemente da perda dos equipamentos utilizados, responderá por perdas e danos, nunca inferiores ao valor que resultaria da aplicação do disposto no art. 103 e seu parágrafo único, quem:

I - alterar, suprimir, modificar ou inutilizar, de qualquer maneira, dispositivos técnicos introduzidos nos exemplares das obras e produções protegidas para evitar ou restringir sua cópia;

II - alterar, suprimir ou inutilizar, de qualquer maneira, os sinais codificados destinados a restringir a comunicação ao público de obras, produções ou emissões protegidas ou a evitar a sua cópia;

III - suprimir ou alterar, sem autorização, qualquer informação sobre a gestão de direitos;

IV - distribuir, importar para distribuição, emitir, comunicar ou puser à disposição do público, sem autorização, obras, interpretações ou execuções, exemplares de interpretações fixadas em fonogramas e emissões, sabendo que a informação sobre a gestão de direitos, sinais codificados e dispositivos técnicos foram suprimidos ou alterados sem autorização.

Art. 108. Quem, na utilização, por qualquer modalidade, de obra intelectual, deixar de indicar ou de anunciar, como tal, o nome, pseudônimo ou sinal convencional do autor e do intérprete, além de responder por danos morais, está obrigado a divulgar-lhes a identidade da seguinte forma:

I - tratando-se de empresa de radiodifusão, no mesmo horário em que tiver ocorrido a infração, por três dias consecutivos;

II - tratando-se de publicação gráfica ou fonográfica, mediante inclusão de errata nos exemplares ainda não distribuídos, sem prejuízo de comunicação, com destaque, por três vezes consecutivas em jornal de grande circulação, dos domicílios do autor, do intérprete e do editor ou produtor;

III - tratando-se de outra forma de utilização, por intermédio da imprensa, na forma a que se refere o inciso anterior.

Art. 109. A execução pública feita em desacordo com os arts. 68, 97, 98 e 99 desta Lei sujeitará os responsáveis a multa de vinte vezes o valor que deveria ser originariamente pago.

Art. 110. Pela violação de direitos autorais nos espetáculos e audições públicas, realizados nos locais ou estabelecimentos a que alude o art. 68, seus proprietários, diretores, gerentes, empresários e arrendatários respondem solidariamente com os organizadores dos espetáculos.

Capítulo III

Da Prescrição da Ação

Art. 111. (VETADO)

Título VIII

Disposições Finais e Transitórias

Art. 112. Se uma obra, em conseqüência de ter expirado o prazo de proteção que lhe era anteriormente reconhecido pelo § 2º do art. 42 da Lei nº. 5.988, de 14 de dezembro de 1973, caiu no domínio público, não terá o prazo de proteção dos direitos patrimoniais ampliado por força do art. 41 desta Lei.

Art. 113. Os fonogramas, os livros e as obras audiovisuais sujeitar-se-ão a selos ou sinais de identificação sob a responsabilidade do produtor, distribuidor ou importador, sem ônus para o consumidor, com o fim de atestar o cumprimento das normas legais vigentes, conforme dispuser o regulamento.

Art. 114. Esta Lei entra em vigor cento e vinte dias após sua publicação.

Art. 115. Ficam revogados os arts. 649 a 673 e 1.346 a 1.362 do Código Civil e as Leis nºs 4.944, de 6 de abril de 1966; 5.988, de 14 de dezembro de 1973, excetuando-se o art. 17 e seus §§ 1º e 2º; 6.800, de 25 de junho de 1980; 7.123, de 12 de setembro de 1983; 9.045, de 18 de maio de 1995, e demais disposições em contrário, mantidos em vigor as Leis nºs 6.533, de 24 de maio de 1978 e 6.615, de 16 de dezembro de 1978. Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

FERNANDO HENRIQUE CARDOSO

II-

LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998.

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

CAPÍTULO II

DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

§ 1º Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvado, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.

§ 2º Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinqüenta anos, contados a partir de 1º de janeiro do ano subseqüente ao da sua publicação ou, na ausência desta, da sua criação.

§ 3º A proteção aos direitos de que trata esta Lei independe de registro.

§ 4º Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.

§ 5º Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.

§ 6º O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.

Art. 3º Os programas de computador poderão, a critério do titular, ser registrados em órgão ou entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério responsável pela política de ciência e tecnologia.

§ 1º O pedido de registro estabelecido neste artigo deverá conter, pelo menos, as seguintes informações:

I - os dados referentes ao autor do programa de computador e ao titular, se distinto do autor, sejam pessoas físicas ou jurídicas;

II - a identificação e descrição funcional do programa de computador; e

III - os trechos do programa e outros dados que se considerar suficientes para identificá-lo e caracterizar sua originalidade, ressalvando-se os direitos de terceiros e a responsabilidade do Governo.

§ 2º As informações referidas no inciso III do parágrafo anterior são de caráter sigiloso, não podendo ser reveladas, salvo por ordem judicial ou a requerimento do próprio titular.

Art. 4º Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

§ 1º Ressalvado ajuste em contrário, a compensação do trabalho ou serviço prestado limitar-se-á à remuneração ou ao salário convencionado.

§ 2º Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.

§ 3º O tratamento previsto neste artigo será aplicado nos casos em que o programa de computador for desenvolvido por bolsistas, estagiários e assemelhados.

Art. 5º Os direitos sobre as derivações autorizadas pelo titular dos direitos de programa de computador, inclusive sua exploração econômica, pertencerão à pessoa

autorizada que as fizer, salvo estipulação contratual em contrário.

Art. 6º Não constituem ofensa aos direitos do titular de programa de computador:

I - a reprodução, em um só exemplar, de cópia legitimamente adquirida, desde que se destine à cópia de salvaguarda ou armazenamento eletrônico, hipótese em que o exemplar original servirá de salvaguarda;

II - a citação parcial do programa, para fins didáticos, desde que identificados o programa e o titular dos direitos respectivos;

III - a ocorrência de semelhança de programa a outro, preexistente, quando se der por força das características funcionais de sua aplicação, da observância de preceitos normativos e técnicos, ou de limitação de forma alternativa para a sua expressão;

IV - a integração de um programa, mantendo-se suas características essenciais, a um sistema aplicativo ou operacional, tecnicamente indispensável às necessidades do usuário, desde que para o uso exclusivo de quem a promoveu.

CAPÍTULO III

DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

Art. 7º O contrato de licença de uso de programa de computador, o documento fiscal correspondente, os suportes físicos do programa ou as respectivas embalagens deverão consignar, de forma facilmente legível pelo usuário, o prazo de validade técnica da versão comercializada.

Art. 8º Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

Parágrafo único. A obrigação persistirá no caso de retirada de circulação comercial do programa de computador durante o prazo de validade, salvo justa indenização de eventuais prejuízos causados a terceiros.

CAPÍTULO IV

DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO
E DE TRANSFERÊNCIA DE TECNOLOGIA

Art. 9º O uso de programa de computador no País será objeto de contrato de licença.

Parágrafo único. Na hipótese de eventual inexistência do contrato referido no *caput* deste artigo, o documento fiscal relativo à aquisição ou licenciamento de cópia servirá para comprovação da regularidade do seu uso.

Art. 10. Os atos e contratos de licença de direitos de comercialização referentes a programas de computador de origem externa deverão fixar, quanto aos tributos e encargos exigíveis, a responsabilidade pelos respectivos pagamentos e estabelecerão a remuneração do titular dos direitos de programa de computador residente ou domiciliado no exterior.

§ 1º Serão nulas as cláusulas que:

I - limitem a produção, a distribuição ou a comercialização, em violação às disposições normativas em vigor;

II - eximam qualquer dos contratantes das responsabilidades por eventuais ações de terceiros, decorrentes de vícios, defeitos ou violação de direitos de autor.

§ 2º O remetente do correspondente valor em moeda estrangeira, em pagamento da remuneração de que se trata, conservará em seu poder, pelo prazo de cinco anos, todos os documentos necessários à comprovação da licitude das remessas e da sua conformidade ao *caput* deste artigo.

Art. 11. Nos casos de transferência de tecnologia de programa de computador, o Instituto Nacional da Propriedade Industrial fará o registro dos respectivos contratos, para que produzam efeitos em relação a terceiros.

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

CAPÍTULO V

DAS INFRAÇÕES E DAS PENALIDADES

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Art. 13. A ação penal e as diligências preliminares de busca e apreensão, nos casos de violação de direito de autor de programa de computador, serão precedidas de vistoria, podendo o juiz ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando.

Art. 14. Independentemente da ação penal, o prejudicado poderá intentar ação para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito.

§ 1º A ação de abstenção de prática de ato poderá ser cumulada com a de perdas e danos pelos prejuízos decorrentes da infração.

§ 2º Independentemente de ação cautelar preparatória, o juiz poderá conceder medida liminar proibindo ao infrator a prática do ato incriminado, nos termos deste artigo.

§ 3º Nos procedimentos cíveis, as medidas cautelares de busca e apreensão observarão o disposto no artigo anterior.

§ 4º Na hipótese de serem apresentadas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.

§ 5º Será responsabilizado por perdas e danos aquele que requerer e promover as medidas previstas neste e nos arts. 12 e 13, agindo de má-fé ou por espírito de emulação, capricho ou erro grosseiro, nos termos dos arts. 16, 17 e 18 do Código de Processo Civil.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 15. Esta Lei entra em vigor na data de sua publicação.

Art. 16. Fica revogada a Lei nº 7.646, de 18 de dezembro de 1987.

Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

FERNANDO HENRIQUE CARDOSO

III.

ESTADO DO RIO DE JANEIRO
PODER JUDICIÁRIO
COMARCA DA CAPITAL
JUÍZO DE DIREITO DA 12ª VARA CÍVEL
Autos n° 99.001.122036-4 e 99.001.109071-7

S E N T E N Ç A

VISTOS ETC.

Tratam-se os presentes autos de uma ação que, pelo procedimento ordinário, NVL SOFTWARE & MULTIMÍDIA LTDA. move em face da H&J SOFTWARE LTDA., ambas já devidamente qualificadas, objetivando, em síntese, o ressarcimento por danos patrimoniais e moral que entende ter experimentado em razão de violação de seus direitos autorais, posto que alega que os programas de computador por si desenvolvidos foram plagiados pela empresa Ré.

Narra a inicial que a Autora desenvolve diversos programas de sucesso no mercado de informática nacional e, objetivando uma maior comercialização de seus produtos, celebrou com a Ré, em junho de 1996, um contrato de cessão de direitos de uso e comercialização de software, pelo qual, em sua essência, obrigou-se a desenvolver alguns determinados programas a fim de que a empresa Ré os comercializasse, obrigando-se esta, por sua vez, ao pagamento de 20% do valor bruto total recebido.

Esclarece ainda a Autora que os pagamentos foram efetuados irregularmente, até que cessaram por completo em fevereiro de 1997, o que a levou a promover uma notificação extrajudicial a fim de que a Ré apresentasse as notas fiscais dos produtos vendidos e efetuasse o respectivo pagamento, sendo certo, no entanto, que as partes não chegaram a um consenso quanto ao valor devido, o que levou a Ré a enviar, por fax, em janeiro de 1998, uma minuta de rescisão do contrato, que acabou por não se formalizar, posto que, desde então, não mais se comunicaram.

Assevera a Autora que, posteriormente, veio a verificar que a empresa Ré fez colocar no mercado os seguintes produtos: “HJ – Curso Windows 95” e “HJ – Internet” e, fazendo uma comparação com os programas por si desenvolvidos, constatou tratar-se de um plágio, razão pela qual contratou um perito especializado para fazer um

laudo preliminar, que foi conclusivo no sentido de que os programas eram quase que idênticos.

Entendendo, pois, que os seus programas foram plagiados pela empresa Ré, violando assim os seus direitos autorais, nos termos da Lei do Software (Lei nº 9.609/98) e da Lei dos Direitos Autorais (lei nº 9.610/98), noticia a Autora que fez ajuizar uma Medida Cautelar de Busca e Apreensão dos alegados produtos plagiados, na qual a liminar requerida foi concedida, postulando, por fim, indenização pelos danos patrimoniais e morais que entende ter experimentado em razão do plágio constatado.

A inicial veio instruída com os documentos de fls.18/72.

Regularmente citada, ofertou a Ré a contestação que juntada foi às fls.78/86, pela qual se insurge contra a pretensão autoral por negar a ocorrência do alegado plágio.

Por referida peça de bloqueio, afirma a Ré, em síntese, que, ao contrário do alegado, sempre honrou com as obrigações decorrentes do contrato firmado, contrato esse que tinha por objeto o "código fonte", que vem a ser um dos itens que compõem um software, sendo certo que o roteiro dos programas questionados foram por si comprados, quando da celebração do contrato, pela quantia de R$ 1.500,00 (um mil e quinhentos reais) por cada software, sendo, portanto, de sua propriedade, como se verifica da cláusula sétima do contrato, pois a mesma especifica claramente quais seriam as incumbências da Autora, dentre as quais não se menciona o roteiro, posto que o mesmo não mais lhe pertencia.

Ademais, afirma ainda a empresa Ré que os roteiros dos produtos questionados são distintos, não se configurando o alegado plágio, até porque um software é composto por 13 (treze) itens padrões e somente o item "tela" foi analisado, o que não se faz suficiente para a comprovação de plágio, até porque o item "tela" é ainda composto de oito sub-itens (tamanho, fundo, navegação, gravuras, lay out, texto, sons e título) e a semelhança entre os programas está presente apenas nos textos, que representam uma das partes da tela, que por sua vez, é apenas um dos itens que compõem um software.

Assevera também a Ré que tais semelhanças constatadas não constituem ofensa aos direitos do titular de programa de computador, a teor do que dispõe o art. 6º, III da Lei 9.609/98 e que as semelhanças existentes referem-se, em verdade, às telas padrões do programa Windows, que não pertencem nem a Autora e nem a Ré, pertencendo tão-somente a Microsoft.

Em assim sendo, defende a Ré a tese da inexistência do alegado plágio, isto porque os programas de computador não podem ser desconsideradas no momento de sua explicação, por serem iguais em qualquer parte do mundo, sendo impossível, pois, dar uma aula sobre o uso do Windows ou Internet sem mostrar as telas padrões.

Que em razões de tais fatos, conclui a empresa Ré que a pretensão autoral não merece acolhida, posto que não comprovado o alegado plágio ou mesmo pirataria e tampouco demonstrado os prejuízos supostamente experimentados.

Registre-se, por relevante, que antes da propositura da presente ação de indenização, como já relatado, fez a Autora ajuizar uma medida cautelar de busca, apreensão e vistoria, cujos respectivos autos seguem em apenso (Proc. nº 99.001.109071-7).

Articulando os mesmos argumentos já expostos, postula a Autora, por aludida medida cautelar, a busca e apreensão de todos os produtos "plagiados" que forem encontrados e a realização de perícia para a constatação do alegado plágio.

A respectiva petição inicial, na qual constou pedido liminar, veio instruída com os documentos de fls.14/50 e com o laudo da perícia preliminar que a Autora mandou realizar e que juntado foi às fls.53/754, formando, assim, o segundo, terceiro e parte do quarto volume de mencionada ação cautelar.

O pedido para que a busca e apreensão fosse realizada liminarmente foi deferido por decisão de fls.755 e verso, decisão essa que veio a ser atacada por recurso de agravo de instrumento (v. fls.774/800) que, por sua vez, veio a ser desprovido por acórdão unânime da Quinta Câmara Cível, do qual foi relator o eminente Desembargador Otávio Rodrigues (v. fls. 1032 e seguintes).

Realizada a apreensão dos produtos e tendo sido a Ré regularmente citada, ofertou a mesma a contestação que juntada foi às fls.806/812, pela qual, articulando os mesmos argumentos já expostos, assevera inexistir o alegado plágio, esperando, assim, a rejeição da pretensão autoral.

Pela mesma decisão que deferiu liminarmente a busca e apreensão foi determinada a realização de perícia, cujo laudo foi juntado às fls.832/845, sendo certo que antes, por petições que seguem às fls,824/827 e 828/829, ofertaram as partes os seus respectivos quesitos.

Sobre o laudo manifestou-se a Autora por petição que juntada foi às fls.851/852, pela qual requereu a respectiva homologação. A parte Ré, por sua vez, fazendo

juntar o laudo crítico de sua assistente técnica, impugnou o laudo (v. fls.853/869), tendo os peritos do Juízo respondido a tal impugnação às fls.873/878.

Face a resposta dos Srs. peritos, nova impugnação foi ofertada pela parte Ré (v. fls.882/883), sobre a qual se manifestaram os peritos, como se verifica da petição de fls.895, oportunidade em que se reportaram ao inteiro teor do laudo pericial e dos esclarecimentos antes prestados.

Insatisfeita com os esclarecimentos dos Srs. Peritos, requereu a empresa Ré, por petição de fls.898, a realização de uma audiência especial para a oitiva dos mesmos.

Antes que houvesse qualquer apreciação sobre tal pedido, interpôs a Autora a petição de fls.900/901, que veio instruída com os documentos de fls.902/904, e pela qual se noticiou que a Ré vinha desrespeitando a liminar concedida, isto porque a mesma continuava distribuindo os produtos objetos da ação. Sobreveio, então, a decisão irrecorrida de fls.905/906, pela qual, ante a denúncia de que os produtos ainda estavam sendo comercializados, foi fixada multa em caso de conduta refratária, da ordem de R$ 30.000,00 (trinta mil reais), tendo sido determinado, também, a apreensão dos produtos junto ao ponto de venda noticiado, restando posteriormente esclarecido, por decisão igualmente irrecorrida de fls.911/912, que a multa fixada só se faria incidir se descobertos e apreendidos os produtos em data posterior à mencionada decisão.

Por petição de fls.919/921, que instruída foi com os documentos de fls.922/930, voltou a parte Autora a noticiar que a empresa Ré, em flagrante desrespeito às ordens judiciais, continuava a comercializar e distribuir os produtos, o que levou este julgador a prolatar a decisão de fls.931/933,pela qual restou estabelecida a obrigação da Ré de pagar, a título de multa e a favor da Autora, a quantia de R$ 90.000,00 (noventa mil reais), quantia essa que, por força das petições e documentos de fls.935/974, veio a ser retificada por decisão de fls.976/979 para a quantia de R$ 300.000,00 (trezentos mil reais).

Aludida decisão veio a ser atacada por recurso de agravo de instrumento, como se verifica às fls.983/991, sendo certo que, pelas respectivas razões, alegou a Ré que os produtos que estavam sendo comercializados já não mais correspondiam aos produtos objetos da ação, o que levou este julgador, por conseguinte, a adquirir o produto que estava sendo comercializado pela Ré, para fins de comparação, e a designar uma audiência especial, como se verifica da decisão de fls.992 e verso.

Referida audiência se realizou consoante os termos consignados na assentada de fls.997/999, oportunidade em que este julgador constatou que os produtos que

estavam sendo comercializados pela empresa Ré eram justamente aqueles que por decisão liminar foi determinada a retirada do mercado, restando mantida, por conseguinte, a decisão atacada, retificando-se tão-somente o valor da multa, já agora para R$ 270.000,00.

Tal decisão veio a ser confirmada pela superior instância, como se verifica da notícia do julgamento consignada em ofício de fls.1006 e do respectivo acórdão da 5ª Câmara Cível, do qual foi relator o eminente Desembargador Carlos Ferrari, e que por cópia segue às fls.1032 e seguintes.

Voltando aos autos desta ação indenizatória (Proc. nº 99.001.122036-4), tem-se que, por força das impugnações ao laudo pericial ofertadas pela parte Ré, foi designada uma audiência especial para que os Srs. Peritos prestassem esclarecimentos quanto ao laudo elaborado, audiência essa que se realizou consoante os termos consignados em assentada de fls.156/158 e termo de depoimento de fls. 159/160.

Nesta ocasião foi designada audiência de instrução e julgamento para a colheita do depoimento pessoal do representante legal da Autora, como se verifica da respectiva assentada e termo de fls.176/182, oportunidade em que a Ré fez juntar a petição e documento de fls.183/185.

Os debates orais foram substituídos por memoriais, tendo a Autora ofertado o seu arrazoado final que juntado foi às fls.189/201 e pelo qual, em síntese, rechaçando as teses da parte Ré, reitera os seus argumentos anteriores, asseverando, ainda, que se encontra devidamente comprovada a ocorrência de plágio, esperando, por conseguinte, a condenação da empresa Ré ao pagamento de indenização por dano patrimonial e moral em razão da ofensa ao seus direitos autorais, requerendo, por fim, que o valor da indenização seja de imediato determinado, evitando-se, assim, a liquidação do julgado.

A empresa Ré, por sua vez, fez juntar o seu respectivo memorial às fls.203/212, pelo qual reitera os termos de sua contestação, reafirmando o seu entendimento no sentido da não ocorrência de violação a direito autoral, notadamente porque não configurado o alegado plágio, ante a impossibilidade de se produzir e desenvolver cursos para microcomputador e Internet sem que haja um mínimo de similaridade, sendo certo, ainda, que seus programas foram desenvolvidos a partir dos roteiros que legalmente adquiriu da Autora, como prova o documento que fez juntar em audiência, o que afasta qualquer presunção ou indício de violação de direito autoral.

É o relatório. Tudo visto e examinado, passo a decidir.

De plano importante se faz esclarecer o âmbito da controvérsia, posto que, como bem articulado pela empresa Ré em seu arrazoado final, "pirataria e plágio são situações absolutamente diferentes em termos de Direito Autoral e capazes, cada uma, de conduzir a rumos e decisões diferentes".

No caso em tela, é verdade que a Autora se utilizou em sua inicial, por vezes, do termo "pirataria", sendo certo, no entanto, que, indubitavelmente, a causa de pedir se consubstancia na imputação de plágio.

Com efeito, de uma simples análise do pedido inicial, ainda que superficial, conclui-se, indiscutivelmente, que a pretensão autoral tem por escopo compelir a Ré a pagar indenização por violação de seus direitos autorais sobre programas de computador em razão de plágio. Sob esta ótica, pois, que a questão posta em debate deverá, e efetivamente será, apreciada.

Para tanto, impõe-se, preliminarmente, um breve estudo a respeito da proteção jurídica que o nosso ordenamento confere ao *software* para, em seguida, se proceder a uma investigação, à luz dos autos, a respeito da titularidade do respectivo direito autoral, passando, depois, a analisar se a hipótese em tela retrata ou não a ocorrência do alegado plágio para, finalmente, em caso de conclusão afirmativa, determinar quais são as sanções aplicáveis à espécie.

Passemos, pois, a apreciar tais questões.

Dissertando a respeito da proteção normativa do *software* no Brasil, esclarece-nos Luiz Augusto Azevedo Sette que, "até 1987, o Brasil não dispunha de legislação que, expressamente, protegesse qualquer direito ligado a criação de *software*. A Lei dos Direitos Autorais de 1973 somente tratava das obras literárias, artísticas e científicas, não mencionando os programas de computador". (*Dados Sobre a Proteção Jurídica do Software no Brasil, in* Direito Eletrônico – A Internet e os Tribunais, Coord. Renato Opice Blum, Edipro, p. 617).

Somente em dezembro de 1987, com o advento da Lei 7.647/87, que o Brasil produziu legislação específica para a proteção dos direitos dos criadores de programas de computador, sendo certo que o regime de proteção então escolhido, seguindo a maioria da doutrina e jurisprudência mundiais, foi o de direitos autorais.

Posteriormente, tal orientação foi mantida e, objetivando regulamentar o art. 5º, XXVII da Constituição Federal, foi promulgada nova lei especial para a proteção

de direitos autorais ligados ao *software*, conhecida como *Lei do Software* (Lei 9.609/98) e, em seguida, foi publicada a nova lei referente aos direitos autorais (Lei 9.610/98), que, supletivamente, também se aplica aos programas de computador.

Tem-se, pois, que, como concluiu o Mestre em Direito pela University of Pennsylvania supra referenciado, " a atual *Lei do Software* assegura o mesmo regime de proteção das obras literárias aos programas de computador, com as particularidades e exceções previstas em seu texto. Portanto, o regime jurídico de proteção escolhido no Brasil é ainda o dos direitos autorais".

De fato, a outra conclusão não se pode chegar, posto ser o que deflui da análise do art. 7º, XII de Lei 9.610/98 c/c art. 2º da Lei 9.609/98.

Em assim sendo, há que se investigar se a Autora efetivamente detém os direitos autorais sobre os programas de computador que alega que foram plagiados pela empresa Ré.

Tem-se como fato incontroverso que foi a empresa Autora que, originariamente, com tecnologia própria, produziu os softwares interativos que ensinam a utilizar os programas DOS, Lótus 123, Carta Certa, dentre outros, inclusive Windows e Internet (que se consubstanciam nos programas objeto do litígio), lançando no mercado a série *Aprendendo*, como amplamente divulgado pela imprensa (v. fls.26/31).

Dúvidas não restam, pois, que os programas objeto do litígio foram desenvolvidos pela empresa Autora, até porque constituem os mesmos, dentre outros, o objeto do contrato de cessão de direitos de uso e comercialização de software firmado pelas partes e que segue às fls.32/35.

Conclui-se, assim, que tais programas de computador foram criados e desenvolvidos pela empresa Autora que, por conseguinte, detém, indubitavelmente, os direitos autorais sobre os mesmos, salientando-se, por relevante, que a proteção a mencionados direitos se dá independentemente de qualquer registro, a teor do que dispõe o parágrafo terceiro do art. 2º da Lei 9.609/98.

A questão que se coloca, pois, é saber se tais direitos de autor foram transferidos para a empresa Ré, seja pelo contrato firmado entre as partes, seja pelo documento apresentado quando da audiência de instrução e julgamento e que se constitui no recibo emitido pela Autora, referente ao pagamento integral do desenvolvimento dos roteiros dos cursos que menciona (v. fls.185).

Assevera a Ré em sua contestação que comprou os roteiros dos programas questionados, conforme cláusula sétima do contrato e, mais adiante, em seu respectivo memorial, fazendo referência ao recibo de fls.185, afirma que o mesmo, "por sua própria natureza jurídica e comercial afasta qualquer presunção ou indício de violação de direito autoral" e "o fato de ter desenvolvido os seus próprios cursos, a partir dos roteiros que legalmente adquiriu da Autora, em nada sublinha ou infere a ocorrência de violação em sede de direito autoral".

Com a *maxima permissa venia*, razão não assiste a parte Ré.

Ora, pelo contrato firmado pelas partes tem-se que a Autora cedeu a favor da Ré os direitos de uso e comercialização dos *softwares* por ela desenvolvidos, pelo prazo e preço ajustados, não se fazendo referência, em momento algum, a qualquer transferência de direitos autorais, ou seja, não obstante a cessão de uso e comercialização, reteve a Autora os direitos patrimoniais e morais de autor dos programas de computador por si desenvolvidos.

E assim é porque, como dispõe o art.4º da lei 9.610/98, interpretam-se restritivamente os negócios jurídicos sobre os direitos autorais, isto é, não devem ser considerados conferidos ao usuário mais direitos do que os expressamente indicados.

Neste passo, como antes consignado, no contrato firmado não foi ajustada nenhuma transferência dos direitos autorais sobre os programas de computador objetos do presente litígio, sendo certo que, ao contrário do que quer fazer crer a parte Ré, a cláusula sétima de referido instrumento não autoriza uma conclusão diversa.

Reza mencionada cláusula que "a cedente (a Autora) realizará manutenção corretiva para os eventuais defeitos e incorreções que os softwares descritos na Cláusula primeira apresentarem, mantendo atualizado os Códigos Fontes, Manual do Usuário e documentação interna do sistema". Tem-se, pois, que trata-se, em verdade, de uma cláusula pela qual se estabeleceu a obrigação da Autora em prestar assistência em caso de constatação de eventuais defeitos e incorreções dos programas cedidos, até porque detentora da tecnologia que permitiu o desenvolvimento dos mesmos e o fato de não se fazer menção aos roteiros não quer dizer, em absoluto, que os respectivos direitos autorais tenham sido alienados, até porque nada neste sentido ficou expresso.

De igual forma, da análise do recibo que acostado foi às fls.185 não se pode concluir que tenha ocorrido transferência dos direitos autorais.

Ora, o que mencionado recibo expressa é uma remuneração paga à Autora pelo desenvolvimento dos roteiros dos cursos que menciona, a fim de que os mesmos pudessem ser utilizados e comercializados pela empresa Ré, nos termos do contrato firmado, não havendo qualquer menção em tal documento quanto a uma eventual transferência de direitos autorais sobre os mesmos.

De fato, razão assiste à Autora quando afirma que aludido recibo "nada mais comprova do que a prestação de serviços iniciais" por ela prestados. Tal recibo consubstancia-se, pois, em documento imprestável para comprovação de transferência de direitos de autor que, a toda evidência, realmente não foram adquiridos pela parte Ré, pois, do contrário, não haveria necessidade de se estabelecer contratualmente que o registro dos *softwares* junto aos órgãos competentes seria efetivado em nome da Autora (v. § único da cláusula primeira do contrato firmado pelas partes – fls.32/35).

Tem-se, pois, que a Autora, não obstante o contrato de cessão de direitos de uso e comercialização e o recibo de fls.185, é a titular dos direitos de autor sobre os programas de computador por si desenvolvidos.

Em sendo a Autora a titular de tais direitos, resta apreciar se os mesmos não lhe foram usurpados, ou seja, resta analisar se, à luz da prova produzida nos autos, configurou-se efetivamente o alegado plágio.

Plagiar, como já definiu o eminente Desembargador paulista Villa da Costa, quando do julgamento da Ap. 178.064-1/0 (RT 698/81), "é trazer para si a criação de terceiros, dando-lhe roupagem que transmude, com certa aparência, a criatura".

"Não é o plágio a mera cópia ou reprodução servil da obra alheia", como leciona o professor lusitano José de Oliveira Ascensão, "é algo de mais sutil: é um aproveitamento da essência criativa da obra anterior, embora apresentada com roupagem diversa" (*in*, Direito Autoral, Forense, 1980, p.13).

Tendo em linha de conta um programa de computador e partindo de sua definição legal (art. 1º da Lei 9.609/98), é possível afirmar, como fez Luiz Augusto Azevedo Sette (op. cit., p.613), "que o ponto diferencial entre dois programas é a sua expressão, isto é, a forma pela qual o conjunto organizado de instruções em linguagem natural ou codificada (código-fonte) se apresenta ao usuário. Assim, poderíamos dizer que um programa não será cópia ilegítima de outro, pelo simples fato de possuir a mesma função ou finalidade. O que torna único um software é a forma pela qual essa função ou finalidade pode ser obtida ou sentida por quem o utiliza".

"Nesse sentido", continua o supracitado jurista, "o que está protegido pelos direitos autorais não é a idéia, mas sim a expressão. Num software, a idéia seria os algoritmos, e a expressão é a materialização dessa idéia perceptível ao homem".

Frente a tais lições, podemos concluir que plagiar um programa de computador não significa criar um novo programa com a mesma finalidade de um outro pré-existente, mas sim, aproveitar-se da materialização dessa idéia, ou seja, da forma como ela é apresentada e percebida pelo usuário e dar-lhe, sutilmente, uma roupagem diversa.

Foi o que efetivamente ocorreu no caso em tela. Vejamos o porquê.

Dissertando a respeito da finalidade dos programas de computador objetos da presente ação, esclareceram os Srs. Peritos, ao responderem ao primeiro quesito da parte Autora, que "os programas de computador objetos da ação, a saber, HJ – Curso de Windows 95, NVL – Aprendendo Windows 95, HJ – Curso de Internet e NVL – Aprendendo Internet, representam softwares denominados CBT (computer based training) ou cursos que têm por objetivo ensinar, através da utilização do computador, os conceitos e a operação do software Windows 95 e da tecnologia da Internet".

Tem-se, assim, que aludidos programas possuem a mesma função ou finalidade, ou seja, ambos são cursos interativos para aprendizagem de utilização da Internet e do programa Windows 95. Ambos são frutos, pois, de uma mesma idéia, qual seja, promover a habilitação do usuário para utilização do Windows 95 e da Internet.

Até aí ilícito algum pode ser imputado, posto que, como antes consignado, não é a idéia em si ou a identidade quanto a função que irá configurar o plágio. Este, como dito, surge do aproveitamento da materialização dessa idéia perceptível ao homem, vale dizer, da forma como ele é apresentado ao usuário.

E nosso caso em tela a perícia levada a efeito nos revelou que o programa colocado no mercado pela empresa Ré foi efetivamente desenvolvido aproveitando-se da mesma materialização da idéia levada a efeito pela Autora, vale dizer, da mesma forma como o software da Autora é apresentado ao usuário.

Ora, como se verifica do laudo de fls.832/845 e da documentação que instrui a perícia preliminar, notadamente a que se refere às telas impressas (v. fls.75/751), para alcançar o seu objetivo de ensinar o usuário a manusear o programa Windows 95 e a "navegar" pela Internet, utilizou-se a empresa Ré, de maneira extremamente significativa, dos mesmos textos, exemplos e também das mesmas figuras ilustrativas utilizadas pela Autora.

A título de exemplo, atentemo-nos para as telas reproduzidas às fls.664. Por tais telas, ambos os programas ensinam o usuário a "salvar" uma HomePage. Não há, é verdade, muita margem à criatividade, quando se transmitem instruções. Entretanto, convenhamos, até a HomePage escolhida (a do clube de futebol Flamengo) é a mesma. A cópia é perfeita...Poderia, ao menos, a empresa Ré, eleger outro time de futebol para ilustrar a sua tela...

Ainda exemplificativamente, atentemo-nos para as telas reproduzidas às fls.677. Pelas mesmas, ensina-se o usuário a colocar o nome do responsável pela conta Internet. A Ré, com a devida venia, sequer se deu ao trabalho de imaginar um outro nome do fictício usuário, posto que se utilizou do mesmo que empregado foi pela Autora – Marcos Araújo Lima. E não foi só nesta tela que o episódio se deu, como se pode verificar do laudo pericial, mais precisamente da resposta dada ao quesito de nº 7 formulado pela Autora (v. fls.835).

Inúmeros outros exemplos de "pura cópia" poderiam ser apontados, pois tais ocorrências se deram em número bastante expressivo, como constatado pela perícia, sendo relevante anotar que não foram consideradas as telas padrões do Windows para tal constatação (v. quesito de nº 8 formulado pela Ré, fls.843).

Afora a identidade das telas, tem-se que a estrutura dos tópicos de ambos os programas foram elaborados de maneira muito similar, para não dizer quase que idêntica, como se verifica do apêndice B do laudo preliminar, não impugnado (v. fls.72/74).

Tem-se, pois, que a materialização da idéia de se ensinar aos usuários de computador a manusear o programa Windows 95 e a "navegar" pela Internet, deu-se, em ambos os programas, da mesma forma, ou seja, foram utilizados os mesmos exemplos, o mesmo texto de instrução, as mesmas figuras ilustrativas, a mesma disposição dos tópicos de ensinamento, etc.

Anote-se, por relevante, que tal semelhança, para não dizer verdadeira cópia, poderia ser evitada, posto não configurar, *in casu*, a hipótese prevista pelo inciso III do art.6º da lei 9.069/98, pois como esclareceram os Srs. Peritos, "de acordo com o número de identidades e semelhanças entre os programas de ambas as partes, podemos afirmar que nas coincidências encontradas as semelhanças não ocorreram por força de característica funcional ou ainda por limitação de forma alternativa de expressão, visto que, embora os temas sejam os mesmos (nos dois programas), a amplitude de cada um permite infinitas variações em termos de didática, com diferentes abordagens e

modos de apresentação dos itens" (v. resposta ao quesito 15 formulado pela Autora, fls.838).

De fato, há que se endossar a conclusão alcançada pelos Srs. Peritos, no sentido de que, tendo em linha de conta a natureza dos programas em questão – cursos interativos de aprendizagem -, o item que apresenta maior relevância para caracterizar a semelhança ou diferença entre dois programas é o conteúdo, conteúdo esse que, como constatado, é extremamente semelhante entre os dois programas, o que configura o plágio.

Ora, como esclareceram os Srs. Peritos em audiência (v. fls.159/160), "inúmeros são os produtos existentes na praça que ensinam a trabalhar com o Windows 95; que, no entanto, entende que existem várias e distintas maneiras de ensinar a trabalhar com o Windows 95; (...); no caso em tela, no entanto, tal não ocorreu, porque é muito semelhante os dois programas utilizados, ou seja, ambos se utilizaram de caminhos muito semelhantes para promover o ensino dos usuários do Windows 95 e da Internet; que quer esclarecer que no caso em tela não ocorreu pirataria; pirataria é quando alguém reproduz um programa e dele se utiliza sem a devida autorização; no caso em tela o que ocorreu foi que o produto final dos programas, ou seja, o roteiro utilizado por ambos os programas para promover aos usuários o ensino do Windows 95 e da Internet são muito semelhantes".

E mais adiante complementam os Srs. Peritos: "que quer esclarecer que quando afirmou que há muita semelhança ewntre os dois programas quanto ao conteúdo é porque a forma de ensinar a mexer tanto no Windows quanto na Internet é efetivamente muito semelhante porque em ambos os programas foi utilizada a mesma ordem, ou seja, a mesma seqüência para dar os ensinamentos, inclusive quanto aos exemplos".

Tem-se, pois, que, indubitavelmente, o conteúdo dos programas, ou seja, a sua expressão e forma pela qual a finalidade dos mesmos é exposta aos usuários, é significativamente semelhante, o que leva à conclusão que o programa colocado no mercado pela Ré foi desenvolvido tendo em linha de conta praticamente o mesmo conteúdo do programa que anteriormente desenvolvido foi pela Autora. Eis aí o plágio.

Configurado o plágio, impõe-se agora apreciar as conseqüências jurídicas ou, em outras palavras, as sanções aplicáveis à espécie.

Como se verifica da inicial, pretende a Autora ver-se ressarcida pelos danos patrimoniais e morais que entende ter experimentado.

Em relação ao dano moral, tal pretensão não merece acolhimento.

Ora, como se sabe, em sede de Direito Moral do Autor, o termo “moral” não é utilizado no sentido do dano moral, vinculado a sentimento de tristeza, dor, vexame, sofrimento e humilhação. Como leciona o eminente Desembargador Sérgio Cavalieri Filho, “quando a lei fala em direito moral do autor está se referindo àquele direito que decorre da manifestação da sua personalidade, emanação do seu espírito criativo, sem levar em conta qualquer conteúdo econômico”.

E continua o renomado Desembargador fluminense: “ Só a pessoa física pode ser titular do direito moral de autor porque só o ser humano é capaz de criar uma obra intelectual. A Lei Autoral, em seu artigo 11, ao dizer que autor é a pessoa física criadora de obra literária, artística ou científica, afastou definitivamente a discussão ensejada pelo parágrafo único do art. 15 da Lei anterior sobre a possibilidade de ser a pessoa jurídica considerada autora. Pode ser ela titular de direito patrimonial do autor, mas do direito moral nunca, simplesmente porque a pessoa jurídica não é capaz de criar nada; não tem talento, não tem espírito, não tem imaginação”.

Vê-se, pois, que não há que se falar em dano moral, até porque, tratando-se de programa de computador, não se aplicam as disposições relativas aos direitos morais, na forma disposta pelo parágrafo primeiro do art. 2º da Lei 9.609/98.

Ademais, mesmo se considerarmos o dano moral em seu sentido mais amplo, ou seja, fora da esfera do Direito Moral do Autor, ainda assim o mesmo não restou configurado, isto porque, como se sabe, tendo em linha de conta a pessoa jurídica, o dano moral só se configura quando há uma ofensa à sua honra objetiva,.vale dizer, quando a imagem que terceiros têm da pessoa jurídica fica arranhada, quando abalada resta a sua credibilidade.

No caso em tela não logrou êxito a Autora em demonstrar e tampouco comprovar tais conseqüências, advindas da ofensa perpetrada pela Ré ao seu direito patrimonial de autor, não se configurando, por conseguinte, o dano moral indenizável.

Tem-se, pois, que a hipótese dos autos autoriza, tão-somente, a fixação de indenização em razão da ofensa ao direito patrimonial.

E tal indenização há que ser fixada de acordo com os ditames estabelecidos pelo parágrafo único do art.103 da Lei 9.610/98, ou seja, por não se conhecer o quantitativo da produção dos exemplares plagiados, pagará a Ré o valor de três mil exemplares de cada um dos programas plagiados, além dos apreendidos.

Em assim sendo, constata-se pelo auto de busca e apreensão que juntado foi às

fls.766/768 dos autos da ação cautelar em apenso, que 126 foram os CD – ROM's apreendidos do programa HJ – Curso Windows 95 e 71 do programa HJ - Internet. A base de cálculo para a indenização, tendo em linha de conta o número de exemplares, será, então, de 3126 (três mil, cento e vinte e seis) exemplares do programa HJ – Curso Windows 95 e 3071 (três mil e setenta e um) exemplares do programa HJ- Internet.

Como os preços praticados no mercado são variáveis, como se verifica das dezenas de notas fiscais juntadas aos autos da ação cautelar (v. fls.922/930, 937/957, 960/968 e 971), apresenta-se mais justo e razoável fixar o valor de cada exemplar, para efeitos de cálculos da verba indenizatória, o valor médio.

Assim, analisando supracitada documentação, tem-se que o preço oscilava entre as cifras de R$ 9,90 (nove reais e noventa centavos) – fls.923/924 e R$ 48,00 (quarenta e oito reais) – fls.964, sendo o preço médio, pois, o da ordem de R$ 28,95 (vinte e oito reais e noventa e cinco centavos).

Após tais considerações, possível se faz fixar o valor da indenização pela ocorrência de plágio do software "Ensinando Windows 95" de titularidade da Autora em R$ 90.497,70 (noventa mil, quatrocentos e noventa e sete reais e setenta centavos) – (3126 exemplares X valor médio de R$ 28,95) e, pela ocorrência de plágio do software "Ensinando Internet", igualmente de titularidade da Autora, em R$ 88.905,45 (oitenta e oito mil, novecentos e cinco reais e quarenta e cinco centavos), totalizando, pois, o valor da indenização por dano patrimonial em R$ 179.403,15 (cento e setenta e nove mil, quatrocentos e três reais e quinze centavos).

Por derradeiro, algumas observações quanto a multa aplicada nos autos da ação cautelar, por desrespeito a ordem liminar concedida, ainda se fazem necessárias.

Não restam dúvidas que a multa aplicada no seio da ação cautelar teve por escopo induzir a Ré ao cumprimento de uma obrigação determinada na ordem liminar, qual seja, retirar do mercado os produtos tidos por plagiados, fixando o MM Juiz prolator da respectiva decisão, multa da ordem de R$ 30.000,00 (trinta mil reais) por cada ponto de venda, restando fixada a multa, então, em R$ 270.000,00 (duzentos e setenta mil reais), como se verifica da decisão consignada em assentada de fls.991/999 dos autos em apenso.

Sabe-se que, à toda evidência, a multa fixada não tem por objetivo ressarcir, não se confundindo, em absoluto, ante a diversa natureza, com a indenização por perdas e danos, mas é fato, também, que a mesma deve guardar uma relação de

proporcionalidade, não sendo razoável que a mesma venha superar o próprio valor da obrigação principal.

Em assim sendo, como a multa foi fixada por decisão interlocutória, nada obsta que o valor da mesma seja revisto por esta sentença, até porque poderia a mesma vir a ser modificada pelo juiz da execução (§ único do art. 644 do CPC) posto que, uma vez apurado o valor da indenização, verificou-se que a multa aplicada foi verdadeiramente excessiva, maculando, por conseguinte, no meu sentir, o princípio da razoabilidade.

Tem-se, assim, que impõe-se a adequação da multa antes fixada ao real conteúdo econômico da demanda, razão pela qual há que se reduzir a multa 2/3, para que a mesma reste estabelecida em valor aproximado ao da metade do valor da obrigação principal, que se consubstancia na indenização nesta fixada, resultando, pois, o valor da multa, em R$ 90.000,00 (noventa mil reais), valor esse que se torna definitivo pela presente sentença e que se apresenta mais consentâneo com o princípio da razoabilidade.

Ante ao exposto e por tudo mais que dos autos consta, ratificando a liminar concedida nos autos da ação cautelar e homologando o laudo pericial na mesma produzido, JULGO PROCEDENTE, em parte, o pedido inicial e, por conseqüência, CONDENO a Ré, a título de indenização por ofensa aos direitos de autor da empresa Requerente, ao pagamento da quantia de R$ 179.403,15 (cento e setenta e nove mil, quatrocentos e três reais e quinze centavos), sem prejuízo do pagamento da multa fixada nos autos da ação cautelar, ora reduzida para R$ 90.000,00 (noventa mil reais), quantias essas que deverão ser devidamente atualizadas quando do efetivo pagamento, a primeira acrescidas de juros legais contados da citação e a segunda a partir da decisão que a estabeleceu. Aplica-se, *in casu,* a regra estatuída pelo parágrafo único do art.21 do CPC, razão pela qual CONDENO, ainda, a empresa Ré, ao pagamento das custas processuais de ambos os feitos, inclusive as despesas da perícia, e honorários advocatícios, estes fixados em 15% sobre o valor total da condenação, que deverão ser devidamente atualizados quando do efetivo pagamento.

P.R.I.

Rio de Janeiro, 8 de fevereiro de 2002

Álvaro Henrique Teixeira de Almeida

Juiz de Direito

BIBLIOGRAFIA

ALBERTIN, Alberto Luiz – Comércio Eletrônico, São Paulo, Atlas, 1999.

ALEJANDRO, Javier Ribas, Aspectos jurídicos Del comercio electrónico en Internet, Pamplona, Aranzadi Editorial, 1999.

BITTAR, Carlos Alberto, Direito de Autor na Obra Feita por Encomenda, São Paulo, RT, 1977.

_____. A Lei do Software e se Regulamento. Rio de Janeiro. Forense, 1988

BITTENCOURT, Guilherme - Inteligência Artificial - Ferramentas e Teorias, Florianópolis, Ed. da UFSC, 1998.

BLUM, Renato M. S. Opice – Direito Eletrônico – a internet e os tribunais, São Paulo, Edipro, 2001 - ISBN 85-7283-324-2.

CARVALHO, Luis Gustavo Grandinetti - Direito de Informação e Liberdade de Expressão, Rio de Janeiro, Renovar, 1999.

CASTELLS, Manuel - A Sociedade em Rede, São Paulo, Paz e Terra, 1999.

FASSY, Amaury - A Informática e o Futuro do Brasil, São Paulo, EMW Editores, 1985.

COSTA, José Carlos Netto. Direito Autoral no Brasil, São Paulo, FTD, 1998.

FERREIRA, Aurélio B. de Holanda. Novo dicionário da língua portuguesa. Rio de Janeiro, N. Fronteira, 1996.

FONSECA FILHO, Cléuzio. História da Computação, São Paulo, LTR - ISBN 85-7322-713-3.

FRANCO, Marcelo Araújo - Ensaio Sobre as Tecnologias Digitais da Inteligência, São Paulo, Papirus Editora, 1997 .

GANDELMAN, Henrique - De Gutemberg à Internet, São Paulo, Record, 2001.

GARCIA, Dinio de Santis - Introdução à Informática Jurídica, São Paulo, Ed. da USP, 1976.

Harris, Lesley Ellen. Digital Property – Currency of the 21st. Century. Canadá: McGraw-Hill, 2000.

HARRIS, Suart - Cyberlife! Descubra as Novas Tecnologias do Nosso Mundo Cibernético, São Paulo, Berkeley, 1995.

Il Codice delo Diritto dell'informática e di Internet - Emilio Tosi,Casa Editrice La Tribuna- Piacenza, 2000.

ISAGUIRRE, Katya Regina – Internet Responsabilidade das empresas que desenvolvem sites para web-com, Curitiba, Ed. Juruá, 2001 – ISBN 85-7394-840-X.

LÉVY, Pierre - O Que é Virtual?, São Paulo, Ed. 34, 1998.

LESSIG, Lawrence. The Future of Ideas – The Fate of the Commons in a Connected World. EUA: Random House.

LUCCA, Newton - SIMÃO FILHO, Adalberto - Direito e Internet - aspectos Jurídicos Relevantes, São Paulo, Ed. Edipro, 2000, ISBN 85-7283-294-7.

MACEDO, Manuel Lopes Rocha, MÁRIO, Macedo, Direito no Ciberespaço, Lisboa, Ed. Cosmos, 1996.

MAESTRE, Javier A - El Derecho al Nombre de Dominio - ISBN 84-607-2175-2.

MANSO, Eduardo Vieira - A Informática e os Direitos Intelectuais, São Paulo, RT, 1985.

NEGROPONTE, Nicholas - A Vida Digital, São Paulo, Companhia das Letras, 1995.

OLIVO, Luis Carlos Cancellier - Direito e Internet – A Regulamentação do Ciberespaço – Ed. UFSC.

PAESANI, Liliana M. – Direito de Informática – Atlas – São Paulo - 1997 – ISBN 85-224-1769-5.

PAESANI, Liliana Minardi – Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil – ed. Atlas – São Paulo - 2000 – ISBN 85-224-2674-0.

PIMENTEL, Alexandre Freire - O Direito Cibernético: um enfoque teórico e lógico-aplicativo, Rio de Janeiro, ed. Renovar, 2000, ISBN 85-7147-178-9.

PLINIO, CABRAL - A Nova Lei de Direitos Autorais, Ed. Sagra Luzzatto, p. 242, 1998.

Revista Iberoamericana de derecho informático, 30-32, Jornadas sobre Contratación Electrónica, Privacidad e Internet, Univ. Nacional de Educación a distancia, Centro Regional de Extremadura – Mérida, 1999.

Revista USP nº 35 – set/out/nov 1997 – Informática/Internet – ed. EDUSP – ISBN BKNET0005956418.

Rony, Ellen e Rony, Peter, The Domain Name Handbook – High Stakes and Strategies in Cyberspace. EUA: R&D Books, 2000.

ROVER, Aires José - Direito, Sociedade e Informática - Limites e perspectivas da vida digital, Fundação Boiteux, 2000.

SCHAFF, Adam - A Sociedade Informática, São Paulo, Brasiliense, 1998.

SCORZELLI, Patrícia – A Comunidade Cibernética e o Direito – Rio de Janeiro – Lumen Juris, 1997.

SCHOUERI, Luís Eduardo – Internet o direito na era virtual, 2ª ed., Rio de Janeiro, Forense, 2001.

SILVA Jr., Ronaldo Lemos da – WAISBERG, Ivo – Comércio Eletrônico, São Paulo, 2001, ed. RT – ISBN 85-203-2066-X.

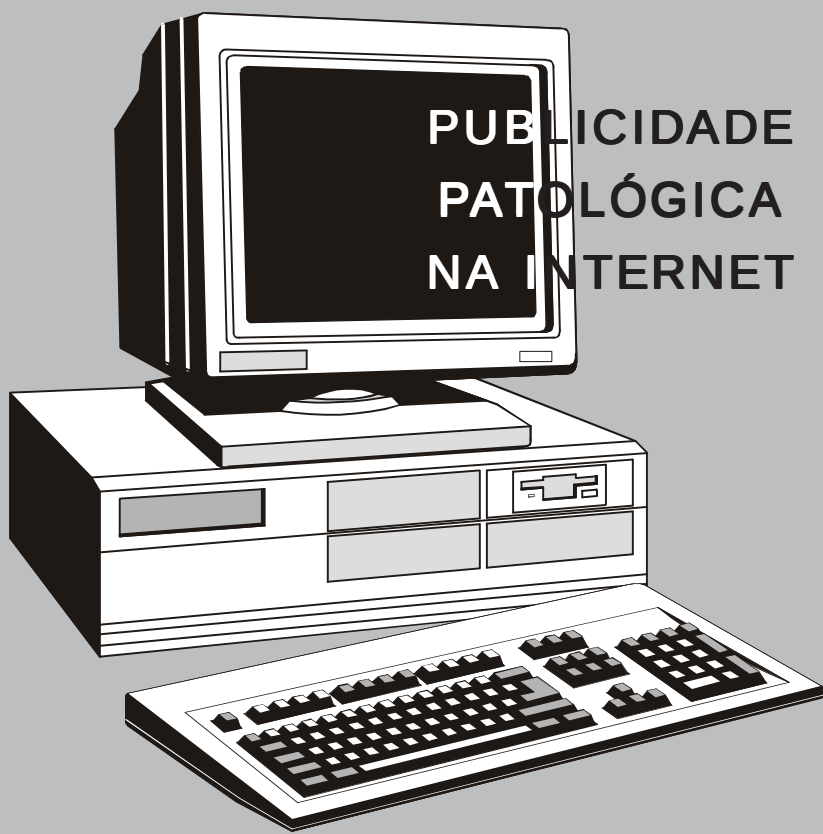
STOCCO, Rui – FIGUEIRA JÚNIOR, Joel Dias – Responsabilidade Civil do Fabricante e Intermediários por Defeitos de Equipamentos e Programas de Informática, São Paulo, RT, 2000 - ISBN 85-203-1943-2.

VOLPI NETO, Ângelo – Comércio Eletrônico – direito e segurança, Curitiba, 2001, ed. Juruá – ISBN 85-7394-891-4.

WILLINGTON e OLIVEIRA, João e Jaury - A Nova Lei Brasileira de Direitos Autorais, 1999, Ed. Lúmen Júris, pág. 10.

WYLLLIE, Eduardo – Economia da internet – ed. Axcel Books – ISBN 8573231254.

PUBLICIDADE PATOLÓGICA NA INTERNET



Jean Jacques Erenberg

PUBLICIDADE PATOLÓGICA NA INTERNET

Jean Jacques Erenberg

SUMÁRIO: 1.Pequeno histórico da Publicidade na Internet – 2. Tendências para um futuro próximo – 3. Patologias mais comuns – 4. Publicidade enganosa – 5. Publicidade Abusiva; 5.a. Abusividade Intrínseca; 5.b. Abusividade Extrínseca; 5.c. Desrespeito à privacidade – 6. Correção do desvio publicitário – 7. Bibliografia.

PEQUENO HISTÓRICO DA PUBLICIDADE NA INTERNET

Desde o início alguns visionários vaticinavam que seria apenas uma questão de tempo para que interesses comerciais, e conseqüentemente a publicidade, invadissem e dominassem a rede mundial de computadores. Foi exatamente o que aconteceu.

Analisando os artigos publicados na imprensa leiga e na especializada em assuntos da internet, verifica-se que as maiores preocupações da comunidade de internautas se ligam às questões dos vírus de computador, da segurança das transações financeiras *on line*, da privacidade e da publicidade abusiva (aqui no sentido da publicidade que é incômoda, invasiva, imposta, indesejada - uma abusividade extrínseca).

A internet, por suas características tecnológicas, possibilita um direcionamento impressionante da mensagem publicitária. O *site*[1] de uma livraria, por exemplo, analisa o comportamento de compra e consulta de um determinado cliente cadastrado e pode periodicamente exibir-lhe ou enviar-lhe mensagens nas quais, tratando-o pelo próprio nome, oferece exatamente o tipo de literatura que mais lhe interessa. Isso já é rotina.

Mas nem sempre foi uma boa idéia veicular publicidade pela rede. A primeira experiência foi negativa.

Desde o seu surgimento, a internet sempre foi uma espécie de comunidade livre. Sem governantes, sem regras que não fossem consensualmente estipuladas e aceitas por seus membros. Sem interesses comerciais, os membros dessa comunidade se habituaram a oferecer e receber gratuitamente as dádivas eletrônicas, por

[1] Local onde se verifica a presença virtual de uma pessoa física ou jurídica ou ente despersonalizado na internet.

puro espírito comunitário. Quando estavam conectados, viam-se inseridos numa verdadeira utopia, onde reinava a anarquia (no sentido de ausência de comando central) e onde cada um distribuía o que produzia aos demais membros e recebia deles em troca o que por sua vez haviam realizado.

Em 1993, quando caíram as restrições comerciais e a *World Wide Web*[2] se tornou acessível ao público, surgiu a primeira publicação comercial *on-line*, a *GNN*. Outros *sites* pioneiros se seguiram, tendo como anunciantes empresas de tecnologia como a Microsoft e a MCI. Até então não surgiriam maiores problemas, vez que somente eram expostos à publicidade aqueles que optavam por digitar o endereço eletrônico de uma dessas publicações, sabidamente comerciais.

Em 1994, porém, ocorreu a primeira divulgação comercial massiva pela rede, nos Estados Unidos. O escritório de advocacia Canter e Siegel enviou um anúncio que oferecia seus serviços para a obtenção do *green card*[3] para mais de sete mil grupos de discussão[4] (o que viola a regra de *netiqueta* – a etiqueta da net – que deter-mina que não se deve postar material comercial em grupos de discussão). Esse episódio ficou mundialmente conhecido pela violenta reação que provocou entre os usuários, que enviaram 30 mil *flames* (respostas indignadas) em apenas 18 horas, sobrecarregando o provedor de serviço dessa empresa e causando sucessivos colapsos, bem como pela cobertura dada pela imprensa ao episódio, o que abalou seriamente a reputação do escritório de advocacia, especialmente entre os membros da comunidade da internet.

A partir desse episódio, as empresas interessadas em utilizar a nova mídia, temendo novas reações adversas, reduziram as dimensões pretendidas para o modelo de publicidade na rede. Surgia o *banner*, pequeno anúncio em forma gráfica.

Para surpresa geral, os primeiros *banners*, veiculados no *site* comercial Hot Wired, em 1994, anunciando produtos da IBM e da Pepsi, não foram criticados.

Nesse mesmo ano, surgem vários *sites* de diretórios e mecanismos de busca, como o Yahoo!, facilitando a localização de informações sobre empresas e produtos na rede. O interesse das empresas em estabelecer presença na internet cresce, e logo a internet se tornaria algo semelhante a um *shopping center* virtual de proporções

---

[2] WWW, "teia" (no sentido de rede) mundial de computadores.

[3] Permissão de residência e trabalho em território norte-americano, concedida a estrangeiros.

[4] Grupos virtuais onde os internautas debatem os mais variados temas.

planetárias. Os usuários foram forçados a compreender que não faziam mais parte de uma comunidade exclusivamente acadêmica e filantrópica. A cultura livre da internet tem de ceder espaço aos interesses comerciais.

Em 1995 os anúncios eletrônicos ganham som, animação e até pequenos vídeos.

As vantagens de estar presente na rede são incomparáveis: baixo custo, acessibilidade constante (24 horas por dia, 365 dias por ano); alta interatividade (o consumidor pode clicar no anúncio para obter mais informações sobre o produto, analisá-lo, testá-lo, interagir com ele e realizar a compra de imediato); possibilidade de rastreamento do comportamento do consumidor em relação ao produto ou serviço; flexibilidade para alterações na campanha publicitária em poucas horas; massificação da mensagem, porém com alto grau de segmentação e dirigibilidade; associação da marca e da empresa à idéia de modernidade; flexibilidade na formação dos preços; redução de estoques; dentre outras.

No entanto, nem sempre o simples fato de utilizar a internet como mídia publicitária surte bons resultados.

As razões disso passam necessariamente por dois fatores: a autorização para estabelecer o contato comercial e o uso adequado e profissional dos instrumentos de marketing.

É intuitivo que, para que a mensagem publicitária seja bem recebida pelo internauta, é necessário que ele a tenha solicitado ou, no mínimo, autorizado previamente seu envio.

O envio de milhões de *e-mails*[5] indiscriminadamente, por exemplo, é altamente improdutivo e forma uma imagem negativa do anunciante em face da comunidade de internautas[6].

Outra situação observável é o amadorismo publicitário. Muitas empresas consideram um luxo caro e desnecessário entregar suas campanhas publicitárias a agências especializadas e tratam de elaborar elas mesmas as mais estapafúrdias mensagens, repletas de agressões à língua, erros técnicos e violações às normas

---

[5] *Electronic mail*, correio eletrônico. Expressão que tanto significa o sistema de envio de mensagens através da internet, quanto a mensagem em si.

[6] Além de dar ensejo a situações inúteis como uma loja localizada em Goiás oferecer ração para gado a um estudante de contabilidade em São Paulo.

legais (oferta de material ilegal, referência a legislações inaplicáveis no país, relatórios pseudojurídicos para justificar suas ações, publicidade abusiva – tanto extrínseca como intrinsecamente – e enganosa). Os resultados geralmente são desfavoráveis.

É que a internet tem como grande diferencial a inversão do controle da comunicação. Quem recebe a mensagem assume (ou gosta de pensar que assume) o controle da comunicação, determinando o que, de quem, quando e como recebe a mensagem. Contrariar essa expectativa pode ser extremamente prejudicial para a imagem da empresa ou produto e até mesmo atingir direitos atribuídos ao consumidor, criando problemas de ordem legal.

Para fomentar e disciplinar a atividade publicitária na rede, foi criada, em 1998, a Associação de Mídia Interativa (AMI), filiada ao Conselho Nacional de Auto-regulamentação Publicitária (Conar), que disciplina as normas e os padrões de planejamento e execução de campanhas publicitárias na internet, a serem seguidos por seus associados. Para isso, a AMI elaborou um Código de Ética para a publicidade *on line*, baseado no próprio Código Brasileiro de Auto-regulamentação Publicitária.

Para o consumidor também há vantagens na presença dos fornecedores na rede, como o acesso a um grande número de informações e benefícios, a custo baixo ou sem custo; possibilidade de pesquisar amplamente em pouco tempo, facilitando sua decisão entre comprar ou não, e entre uma dentre tantas marcas; a redução do preço decorrente da grande concorrência; facilidade de obtenção de assistência técnica e esclarecimento de dúvidas sobre o produto ou serviço, por meio de canais de comunicação permanentemente abertos.

Porém armadilhas diversas espreitam, inclusive no que tange à preservação de seus direitos em face da publicidade e seus operadores.

A concorrência na internet se torna cada vez mais acirrada. No final do século, mais de 100 milhões de páginas povoavam a *Web* e 170 mil novas eram criadas a cada dia. Em razão disso, proliferam os mecanismos de busca, metabusca (várias buscas simultâneas) e agentes de comparação (mecanismos de busca que comparam o preço de um determinado produto em diversos *sites*, a fim de selecionar as a melhores ofertas).

Para tentar atrair e prender a atenção dos consumidores em potencial, as empresas se valem de instrumentos cada vez mais sofisticados e técnicas de abordagem cada vez mais contundentes, invadindo muitas vezes os limites da patologia jurídica.

É então que se revela um dos dilemas da publicidade: vender a qualquer custo ou respeitar os limites éticos e jurídicos?

TENDÊNCIAS PARA UM FUTURO PRÓXIMO

Além das formas de publicidade já correntes, o futuro próximo da publicidade na internet aponta para dois desdobramentos:

Envio de mensagens para dispositivos móveis. Telefones celulares, computadores de mão (*palmtops, handhelds*) e outros dispositivos móveis já estão conectados à internet e outros estão sendo preparados para sê-los muito em breve.

O envio de mensagens diretamente a esses dispositivos já é corrente. Breve, com o aumento da velocidade de transmissão de dados, essa nova mídia se tornará atraente para o mercado publicitário[7].

A possibilidade de rastrear a localização de um desses equipamentos no espaço (graças ao sistema de células característico da telefonia celular), com precisão de metros, aponta para uma nova forma de abordagem: a oferta do produto ou serviço é enviada ao aparelho do consumidor no exato momento em que ele se encontra nas proximidades de uma loja que os comercialize.

Aproveitamento da convergência tecnológica TV/Internet. Grande promessa de popularização definitiva da internet, a convergência dessas duas tecnologias já é uma realidade, restando apenas que a altíssima velocidade de transmissão de dados seja uma realidade disponível em larga escala.

As possibilidades para a publicidade serão inúmeras: o produto ou serviço anunciado na tela da TV poderá ser adquirido de imediato, bastando apontar o controle remoto para ele e acionar um botão; a venda (ou oferecimento gratuito, mediante patrocínio) de facilidades como a possibilidade de assistir a qualquer filme (ou capítulo de novela, ou partida de futebol) da grade de programação das emissoras onde, quando, como e quantas vezes o usuário quiser (sob demanda, na expressão técnica).

---

[7] Algumas companhias operadoras de sistemas de telefonia celular já têm efetuado testes, enviando mensagens aos seus usuários com ofertas de seus próprios produtos.

A união dessas tecnologias com a dos *home theater* (cinema doméstico), já bastante comum, traz à mente a idéia de receber como brinde numa caixa de achocolatado a senha para assistir em casa o lançamento que sequer chegou às telas de cinema.

Não há limites visíveis para o aproveitamento dessa nova mídia pela indústria da publicidade.

PATOLOGIAS MAIS COMUNS

As patologias detectadas na publicidade que atualmente se veicula por meio da internet podem ser classificadas da seguinte forma:

a. publicidade enganosa (contendo falsas informações quanto ao produto ou serviço ofertado);

b. publicidade abusiva:

b.1. publicidade intrinsecamente abusiva (abusiva quanto ao seu conteúdo), categoria na qual se insere também a publicidade de produtos ilícitos ou de produtos controlados sem a adoção das cautelas determinadas em leis ou regulamentos (como a publicidade de tabaco, na qual se exige advertências quanto aos males causados à saúde);

b.2 publicidade extrinsecamente abusiva (invasiva; abusiva quanto à forma de abordagem do destinatário).

Para o presente trabalho, o enquadramento das condutas nessas categorias de publicidade patológica será realizado com base nos princípios e preceitos contidos no direito positivo brasileiro (constitucional e infraconstitucional). Os preceitos auto-regulatórios não serão utilizados diretamente como fundamentação para tal, vez que a análise de seu conteúdo dá conta de que o seu sentido não diverge do que se extrai do próprio direito[8].

[8] Com efeito, os códigos de ética do Conar e da AMI somente explicitam aquilo que já vem implícito na Constituição e no Código de Defesa do Consumidor. É por isso que os preceitos desses códigos de ética são judicialmente sustentáveis: traduzem normas jurídicas postas e exigíveis.

PUBLICIDADE ENGANOSA

Oferta de produtos ou serviços inexistentes. O anunciante oferece e comercializa produtos ou serviços e recebe o respectivo pagamento, porém jamais os entregará ao consumidor. Trata-se de modalidade de publicidade enganosa, vulnerante do princípio da veracidade (art. 37, § 1º, CDC), bem como intrinsecamente abusiva (art. 37, § 2º, CDC), por ferir o princípio da vinculação da oferta publicitária (art. 30, CDC), sem prejuízo de se tratar de infração penal, tanto na esfera do CDC, quanto na do Código Penal.

Oferta de produtos ou serviços mediante informações falsas ou omissão de informações relevantes sobre os mesmos. Publicidade enganosa, contrária ao princípio da veracidade (art. 37, § 1º) e ao princípio da informação (arts. 31 e 33, CDC).

Oferta de produtos por preços que não serão praticados. Detectou a pesquisa ofertas de produtos por preços que o anunciante não pretende praticar. Empresas têm, inclusive, utilizado os chamados *sites* de leilão para a venda de produtos e freqüentemente iludem os consumidores com ofertas como "computadores a partir de R$1,00", que na realidade são falsas, vez que não há a menor pretensão por parte dessas empresas de honrar tal preço inicial anunciado. Tal forma de publicidade é claramente enganosa (art. 37, § 1º, CDC), violadora do princípio da veracidade.

PUBLICIDADE ABUSIVA

Abusividade intrínseca

Editoriais pagos. Trata-se de publicidade travestida de notícia ou informação. A publicidade assume a forma editorial pela semelhança visual e gráfica com um texto não-publicitário. Os publicitários reputam ser essa "uma boa maneira de atrair a atenção do internauta", vez que na internet os usuários estão sempre procurando por informação. No entanto, além de tratar-se de técnica que gera no usuário a sensação de ter sido enganado, o que pode denegrir a imagem do produto e da empresa, constitui publicidade intrinsecamente abusiva (art. 37, § 2º, CDC) por infração ao princípio da identificação da mensagem publicitária como tal, inscrito no art. 36, do CDC.

Omissão de dados do fornecedor, tais como nome, endereço físico, registro no CNPJ e *e-mail* para retorno das mensagens. É modalidade de publicidade intrinsecamente abusiva (art. 37, § 2º, CDC) por ferir o princípio da informação (arts. 31 e 33, CDC).

Exploração de situações desfavoráveis ao consumidor, como o medo, a superstição, a dor, a revolta, a deficiência de julgamento da criança, do adolescente e do idoso, a incitação de violência e práticas perigosas à saúde ou segurança do consumidor ou de terceiros etc. Todas essas formas de publicidade são intrinsecamente abusivas (art. 37, § 2º, CDC).

Publicidade contrária à moral, aos bons costumes e à lei. Oferta não solicitada de pornografia, utilização de material ofensivo para a divulgação de produtos ou serviços, falsas promessas de fortuna, oferta de produtos ilícitos (jogo a dinheiro, aparelhos que podem ser utilizados para ferir pessoas e animais, cópias não autorizadas de obras autorais – música, imagem, literatura, *software* – etc). Publicidade dessa natureza, ao incitar e fomentar a violência e o crime ou agredir valores pessoais e sociais viola garantias diversas, como autodeterminação, segurança, saúde, proteção econômica, sendo, pois, modalidade abusiva tanto intrínseca quanto extrinsecamente (art. 37, § 2º, CDC), sem prejuízo de sua caracterização como ilícito penal.

Abusividade extrínseca

Imposição da mensagem publicitária. A oferta é exibida na tela do computador do usuário sem que este tenha voluntariamente buscado o acesso. É comum a utilização de subterfúgios[9] para forçar o direcionamento do programa de navegação do usuário a determinados *sites*. Tal conduta, fortemente inoportuna e invasiva, configura publicidade extrinsecamente abusiva (art. 37, § 20, CDC), por violar a garantia constitucional de autodeterminação.

Obstrução de saída. Impossibilidade de o usuário menos experiente sair de um determinado *site* sem que tenha de desconectar-se da internet ou desligar o

[9] Mensagens eletrônicas contendo comandos ocultos que determinam a abertura pelo programa de navegação de determinada página da internet sem a intervenção do usuário; páginas que ao serem abertas ou fechadas disparam a abertura de outras; páginas que são abertas sorrateiramente por uma das formas *retro* descritas e permanecem ocultas, determinando a abertura de outras a intervalos regulares; etc.

computador. Certos *sites* incluem em suas páginas instruções que determinam a ocupação total da tela do computador, ocultando a visualização dos botões de comando do navegador, ou ainda, que determinam que a cada tentativa de saída, o usuário seja conduzido a novas páginas do mesmo *site*. Também é comum a utilização de *frames* para impossibilitar ou dificultar a saída do usuário de um *site*.

Trata-se igualmente de publicidade extrinsecamente abusiva (art. 37, § 20, CDC) que viola a garantia constitucional de autodeterminação.

Insinceridade de link. A peça publicitária apresenta *links* que supostamente apontam para informações, brindes ou qualquer outra página de conteúdo. Na realidade, porém, conduzem o visitante a uma mensagem publicitária. É igualmente uma forma de publicidade extrinsecamente abusiva, violadora do princípio da identificação da mensagem publicitária como tal (art. 36, CDC).

Truncamento do fluxo natural de navegação ou leitura. O uso excessivo de páginas intercaladas, *banners*, janelas *pop-up*, pode tornar desgastante a utilização dos serviços da rede pelo usuário, forçando-o a desviar sua atenção freqüentemente daquilo que realmente constitui o objeto de seu interesse. Pode ocorrer, por exemplo, de várias janelas *pop-up* serem disparadas simultânea ou sucessivamente, de forma muito rápida, sobrecarregando o equipamento do usuário e chegando a causar travamentos. Podem também estar as janelas encadeadas, de forma que se o usuário fecha uma, logo surgem outras. E já foram registrados casos de janelas *pop-up* ocultas, que não se abrem no navegador, mas permanecem minimizadas, determinando a abertura de outras novas janelas de tempos em tempos.

São, pois, por si sós, modalidades extrinsecamente abusivas de publicidade (art. 37, § 2º, CDC), por contrárias ao princípio da autodeterminação.

Desrespeito à privacidade.

Para melhor direcionar suas campanhas publicitárias, os fornecedores se valem das facilidades tecnológicas proporcionadas pelo ambiente virtual para colher um grande número de informações dos visitantes de seus *sites*.

Para isso, recorrem a várias formas de coleta de informações: preenchimento de formulários de registro ou de participação em promoções e concursos; aferição do trajeto do usuário no *site* (por onde ingressou, quanto tempo permaneceu em cada página, onde clicou, etc); registro de preferências (armazenando-se as informações

sobre os produtos adquiridos ou pesquisados por cada usuário); o *data mining*[10]; os polêmicos *cookies*[11]; e mesmo, mais recentemente, "programas espiões"[12].

Em termos mundiais, há duas grandes linhas de procedimento em relação à privacidade do consumidor na internet.

A linha européia, fundada em uma legislação mais restritiva que tem por base uma Diretiva da Comunidade Européia, que impõe às empresas informar previamente os tipos de dados coletados, o uso que se pretende dar a esses dados, as alternativas e meios de o consumidor limitar a cessão desses dados a terceiros e a permissão do acesso do consumidor às informações detalhadas a seu respeito constantes nos bancos de dados. A linha européia parte, pois, do princípio da *positive option*, na qual a utilização de uma lista de endereços eletrônicos só deve ocorrer após manifestação inequívoca do consumidor, concordando com a ação.

Já a linha norte-americana funda-se no princípio da *negative option*, ou seja, a utilização presume-se consentida, até que o consumidor se manifeste em contrário. Lá a Direct Marketing Association (DMA), órgão de auto-regulamentação, recomenda que em cada peça deve constar um campo onde o consumidor assinala sua opção de continuar ou não recebendo informações ou se seu nome pode ser divulgado para outras empresas. A legislação norte-americana permite que a informação seja usada comercialmente, em benefício das pessoas e sem comprometer a sua privacidade[13].

---

[10] *Data mining* (garimpagem de dados) consiste em um sistema interativo no qual um software vai colhendo e armazenando informações sobre as preferências do usuário para utilizar de duas formas: em tempo real, acompanhando o cliente desde sua entrada na loja virtual e, conforme a navegação avança, sugerindo produtos e serviços que se relacionem àquelas preferências; e ao longo do tempo, mantendo uma base de dados permanente e cumulativa a respeito das preferências do cliente, o que possibilita reconhece-lo assim que entra no *site* e selecionar somente as ofertas de produtos e serviços que lhe sejam interessantes, bem como remeter-lhe via *e-mail* essas ofertas personalizadas.

[11] Cookies são pequenas peças de informação codificadas, contendo dados do usuário, como nome, endereço eletrônico (*e-mail*), listagem das compras e pesquisas realizadas no *site*, preferências reveladas pelas ações do usuário dentro do *site*, senha de acesso ao *site*, etc, implantadas por programas residentes no *site*, de forma não perceptível, no próprio disco rígido do computador do usuário, de forma que a cada retorno desse usuário, essas informações sejam vasculhadas e recuperadas, possibilitando alto grau de personalização e direcionamento das ofertas. São considerados grandes ferramentas de marketing pelas empresas.

[12] Programas que, de forma oculta, rastreiam e registram informações sobre os internautas, sem pedir permissão, com o fito de pesquisar seus hábitos de consumo. Sua utilização aumentou 500% de 1999 a 2001. Em 2001 3,9% dos *sites* os utilizavam (conforme a empresa Cyvellance).

[13] Em qualquer das duas formas, tem-se o chamado marketing de permissão, vez que o consumidor dá sua permissão (explícita e prévia ou implícita e póstuma) para receber comunicações de determinada empresa. Em outras palavras, o consumidor oferece voluntariamente sua atenção. Importante dizer que essa permissão é inalienável, ou seja, o consumidor não estende essa autorização para a comunicação a outra empresa, sendo, pois desperdício de recursos adquirir listas de endereços eletrônicos formados por outras empresas. Outra razão relevante para essa inalienabilidade é que a empresa que colheu os dados direcionou sua coleta para os consumidores que demonstram preferências que se conformam com precisão aos produtos e serviços que comercializa, sendo o conjunto de dados inservível para qualquer outra empresa que não comercialize exatamente as mesmas coisas na mesma área geográfica e para o mesmo perfil de cliente, ou seja, um concorrente direto. Mesmo assim, se uma empresa desejar adquirir dados de outra, é imprescindível permissão específica do consumidor.

Como se vê, de certa forma essas linhas de procedimento são antagônicas. Para possibilitar ações de marketing de empresas norte-americanas no mercado europeu, criou-se o conceito de *safe harbour* (porto seguro), segundo o qual empresas norte-americanas aceitam administrar seus bancos de dados de cidadãos europeus de acordo com as regras da Comunidade Européia.

No Brasil, a questão da privacidade não conta ainda com regulamentação específica, mas a interpretação sistemática da Constituição e do CDC aponta para um sistema mais parecido com o europeu (*positive option)* do que com o norte-americano.

Em sentido contrário, as associações que atuam na área, Associação Brasileira de Marketing Direto (Abemd), Instituto Brasileiro de Database Marketing (IBDM) e Associação Brasileira de Telemarketing (ABT) formaram um Comitê de Privacidade para sugerir a formação legislativa a respeito da matéria, com base no sistema norte-americano da *negative option*.

Nesse contexto, várias condutas podem configurar publicidade patológica.

a. Coleta de informações do visitante por meio do preenchimento de formulários de cadastramento ou de forma automática (mediante o acompanhamento e a gravação das ações do consumidor no ambiente do *site*) sem informar que o faz;

b. ausência de informação adequada e suficiente a respeito da política de privacidade de dados e cessão das informações pessoais do consumidor a terceiros;

c. ausência de informação ao usuário sobre a existência de banco de dados contendo informações a seu respeito, bem como sobre seu conteúdo exato, ou recusa-se a exclui-las ou corrigi-las quando solicitado;

d. envio ao consumidor de correspondência eletrônica em massa ou cessão de listas contendo seus dados a terceiros para qualquer fim, sem a devida e prévia autorização.

e. Utilização de *cookies* sem o conhecimento e a autorização prévia e expressa do usuário. É prática fortemente condenada pela comunidade de internautas.

O *cookie* é extremamente útil, tanto para a empresa quanto para o consumidor, vez que possibilita, por exemplo, a utilização de saudação pessoal ao consumidor,

evitar perda de tempo com o preenchimento de novos cadastros em *sites* constantemente visitados, facilitar as buscas por produtos e serviços de interesse específico do usuário sem que ofertas que não lhe interessam sejam exibidas etc.

A abusividade reside na implantação de *cookies* sem autorização e conhecimento do usuário, e na ausência de comunicação formal de que tais dados foram colhidos e qual o seu efetivo teor, por violar o direito à privacidade.

Tratam-se de situações de abusividade extrínseca (art. 37, § 2º, CDC) por violarem o princípio constitucional da privacidade, bem como disposições expressas no bojo do Código, ensejadoras de sanções de natureza administrativa, civil e penal[14].

Spamming. Remessa indiscriminada e massificada de mensagens para endereços desconhecidos. Costuma desencadear respostas hostis, vez que a comunidade de internautas considera tal prática uma intolerável invasão de privacidade.

O *Spam* foi o primeiro grande problema diretamente ligado à questão da publicidade surgido no seio da internet. Sinônimo de publicidade comercial não-solicitada (e portanto não desejada), a expressão foi inspirada num filme do grupo de comediantes ingleses *Monty Pyton*, no qual se via, numa antológica cena, vikings barulhentos reunidos em torno de uma mesa, bradando "*Spam! Spam! Spam!*", para exigir presunto enlatado da marca "Spam", o qual os britânicos consideram de sabor intragável, porém algo inevitável à mesa, até que ninguém mais suporta a gritaria.

Essa prática publicitária abusiva consiste em enviar mensagens via correio eletrônico, lista de distribuição ou *newsgroup*[15], indiscriminadamente e em grande quantidade, com o objetivo de divulgar publicidade, propaganda, correntes, pirâmides, pedidos de donativos, boatos e esquemas "infalíveis" para ganhar dinheiro, dentre outras informações indesejáveis e geralmente inúteis (quando não danosas).

Tal conduta, reputada insuportável pelos usuários da rede, em virtude da inconveniência de receber enormes quantidades de mensagens não-solicitadas (chamadas de *lixo* pelos internautas), o que torna a recuperação de mensagens lenta (em virtude do grande volume de dados), frustrante (já que a maioria das mensagens é de pouco ou nenhum interesse) e perigosa (pela efetiva possibilidade de distribuição de vírus).

---

[14] CDC, arts. 43, 59, 72, 73; Código Civil, art. 129.

[15] Listas de distribuição são cadastros contendo endereços de usuários regularmente cadastrados para o recebimento de certas informações periódicas ou não; *newsgroups*, ou grupos de notícias, são sistemas de troca de mensagens no qual cada usuário pode postar informações para todos os integrantes do grupo.

Para estudar estratégias com o objetivo de tentar deter ou ao menos reduzir essa prática, criou-se no Brasil o Grupo de Trabalho de Segurança do Comitê Gestor Internet, em conjunto com os provedores. Também há iniciativas não-oficiais, como a organização Anti *Spam* (www.antispam.org.br), criada por provedores de acesso decididos a contribuirem para o combate a esse abuso.

A organização recebe denúncias de usuários vitimados por *spam*, notificando o provedor utilizado pelo *spammer* para que em 48 horas adote atitude que bloqueie a remessa de novas mensagens. Caso o provedor não responda adequadamente, são enviadas duas reiterações a cada 48 horas, após o que, se não houver providências, o provedor é colocado numa lista de domínios banidos que é utilizada para barrar quaisquer mensagens oriundas desses provedores (que não chegam, pois, aos seus destinatários, causando grande inconveniente para o provedor), a fim de inibir novas tentativas de *spamming*[16] [17].

Hoje o *Spam* representa um terço do tráfego na rede e, conforme o Instituto Jupiter Media Metrix, 41% das reclamações dos usuários são relativas ao recebimento de *e-mails* indesejados.

Outra constatação é a de que os anunciantes inescrupulosos buscam dissimular o caráter ilícito de certas mensagens comerciais por meio da inserção de falsas afirmações, formas propositalmente ineficazes de remoção do endereço do consumidor do *mailing list*, invocação de regras inaplicáveis no país e mesmo orientações pseudo-jurídicas que induzem o consumidor a crer que está sendo abordado de forma legítima[18].

Mesmo tendo sido solicitado ou autorizado o envio de mensagens, pode surgir abusividade extrínseca (art. 37, § 2º, CDC) caso se ultrapasse o limite de uma mensagem por semana (salvo se as peculiaridades do assunto tratado o exigirem, e isso for desejado pelo consumidor). Igualmente, as mensagens devem conter informações claras,

---

[16] O provedor gratuito brasileiro IG (Internet Grátis) disponibilizou endereços eletrônicos a seus milhares de usuários sem que fosse necessária a confirmação de identidade, o que tornou o serviço atraente a quem deseja enviar mensagens de forma anônima ou sob falsa identidade. A utilização de endereços fornecidos pelo IG para a prática do *spamming* fez com que mensagens desse provedor fossem bloqueadas em diversos serviços da Internet como grupos de discussão. Hoje esse provedor busca solução (em vão, ao que parece) para tal problema. Não é caso isolado.

[17] Nos EUA tem-se utilizado uma antiga norma, há muito aplicada na oferta de produtos por meio de telefonemas não desejados: primeiramente o anunciante recebe um aviso de que o consumidor não quer mais receber mensagens comerciais. Se as mensagens não pararem é aplicada uma multa de US$500. Se ainda assim não pararem, a multa sobe para US$25.000.

[18] Uma das mensagens colhidas na pesquisa que originou este trabalho trazia um *link* para um artigo, supostamente escrito por um jurista, que "explicava" porquê o consumidor deveria resignar-se em receber mensagens comerciais não solicitadas.

objetivas e em quantidade e qualidade adequadas. Textos que não revelam desde logo sua natureza comercial, de conteúdo irrelevante, obscuros, incompletos, confusos ou muito longos são potenciais fatores de abusividade.

De outro ângulo, autorizada ou não, essa forma de publicidade será extrinsecamente abusiva quando a mensagem não contiver forma fácil, imediata e efetiva de remoção dos dados do consumidor do banco de dados do anunciante, de forma a cessar o envio[19].

O *spam* normalmente começa com a coleta, sem qualquer critério, do maior número possível de endereços eletrônicos (milhares, milhões deles), que são reunidos em listas (*mailing lists*) e oferecidos na internet[20]. Normalmente, os "profissionais"[21] que reúnem e comercializam esse material adicionam um ou mais aplicativos que automatizam a remessa de uma quantidade fabulosa de mensagens comerciais aos endereços da lista em poucas horas[22].

É muito comum que esse tipo de mensagem publicitária patológica oculte o nome e endereço eletrônico do remetente ou indique nome e endereço falsos, a fim de bloquear *flames* (respostas indignadas) e evitar que o programa de recuperação de mensagens do usuário possa ser configurado para recusar a mensagem. Também o próprio endereço do remetente é oculto ou alterado, a fim de que não seja possível o descadastramento ou para que, ao tentar solicitar a exclusão de seu endereço do *mailing list*, o consumidor seja obrigado a informá-lo, o que no mais das vezes serve para confirmar ao emissor da mensagem o fato de aquele endereço se encontrar ativo (e, claro, saber que as mensagens comerciais estão sendo recebidas, a fim de continuar remetendo).

Mesmo o título (assunto ou *subject*, no jargão internauta) da mensagem por vezes é suprimido, a fim de confundir o consumidor e impossibilitar a configuração de sistemas de bloqueio de mensagens indesejadas.

---

[19] Não é incomum que as mensagens não disponham de informações sobre como descadastrar o consumidor ou que a forma de descadastramento disponibilizada seja ineficaz, extremamente complexa ou simplesmente um engodo (ao clicar no *link* que supostamente levaria à abertura de uma página ou mensagem de solicitação de descadastramento, o consumidor obtém a mensagem de "página inexistente" ou é exposto a mais publicidade).

[20] Numa espécie de círculo vicioso, as mensagens oferecendo esse material chegam às pessoas e empresas principalmente por meio de *spamming*.

[21] Segundo a AMI a participação das agências na publicidade veiculada pela Internet é de menos de 10%.

[22] É assim que um engenheiro mecânico do Rio Grande do Sul pode receber quase que diariamente ofertas irresistíveis de cursos em certa academia de dança localizada em Pindamonhangaba, interior de São Paulo.

Outro subterfúgio muito utilizado é dissimular a natureza do *spam*, inserindo nas mensagens justificativas falsas como "você está recebendo essa mensagem por ter se cadastrado em nosso *site*", "um amigo recomendou seu endereço", "você foi indicado", ou mesmo pedidos de desculpas antecipados, como "obtivemos seu endereço eletrônico na internet, se não queria receber essa mensagem, desculpe-nos".

Mais um recurso comum é dar à mensagem um título que tenta fazê-la parecer com a resposta a uma solicitação pessoal: "resultado de sua pesquisa", "sobre a sua consulta", "conforme sua solicitação".

É também freqüente "travestir" a mensagem comercial como pessoal, com títulos como "você não imagina que oferta maravilhosa eu encontrei", "aquele produto que você me pediu para procurar eu só encontrei no *site*...", "Oi, lembra de mim?". E o conteúdo pode ser no mesmo sentido: "Eu estava navegando e encontrei um preço incrível para aquele equipamento de som que você tanto queria".

Também se tornou bastante comum que os perpetradores dessa prática tentem justificar sua conduta mediante uma série de procedimentos que visam iludir o consumidor. Assim, surgem afirmações como "isso não é *spam*!", como se o poder da vontade do emissor da mensagem fosse o suficiente para afastar o caráter abusivo.

Para embasar essa negativa, os anunciantes recorrem a subterfúgios como o falso permissivo legal. Oito em cada dez *spam* contém a seguinte frase: ***Esta mensagem é enviada com a complacência da nova legislação sobre o correio eletrônico, seção 301, Parágrafo (a) (2) (c) Decreto S.1618, Título Terceiro aprovado pelo "105 Congresso Base de Normativas Internacionais sobre SPAM". Este e-mail não poderá ser considerado SPAM quando inclui uma forma de ser removido de futuros correios. Clique aqui para excluir seu e-mail da nossa listagem.***

É bom lembrar que no Brasil essa norma norte-americana não tem aplicação. Na sistemática do Código de Defesa do Consumidor brasileiro, que adotou a teoria européia da *positive option*, independentemente de a mensagem conter ou não forma de solicitar a remoção do usuário da lista, será extrinsecamente abusiva se não foi previamente autorizada, por violar os princípios da autodeterminação e boa-fé e a garantia constitucional de privacidade[23].

---

[23] Importante ressaltar a iniciativa de alguns anunciantes que buscam fazer constar do título de suas mensagens expressões como "mensagem comercial", "*no spam*", "MEPPS - Mensagem Eletrônica de Publicidade de Produtos e Serviços", a fim de alertar o consumidor de imediato sobre a natureza das mensagens, bem como possibilitar a configuração de filtros no programa de recuperação de mensagens, a fim de bloqueá-las.

De qualquer forma, o *spam* é extremamente ineficaz, tendo taxas baixíssimas de retorno em relação ao *push advertising* legítimo[24] e gerando altas taxas de rejeição no seio da comunidade de usuários em relação aos produtos, serviços, marcas e empresas que se utilizam desse recurso.

Também será considerada *spam*, e portanto abusiva, a eventual e futura prática de remeter mensagens comerciais não-solicitadas a dispositivos móveis como telefones celulares, *palmtops* e *handhelds*, especialmente se o anunciante se utilizar da facilidade de localização espacial do usuário para impor-lhe mensagens comerciais quando se aproximar de um ponto de venda.

Uso inadequado dos sites de aproximação, corretagem e leilão. Como se sabe, esses *sites* destinam-se precipuamente a promover o contato entre particulares para que possam comprar e vender entre si.

Não se trata, pois, de relações de consumo, mas sim de contratos regidos pelo Código Civil.

Por vezes, um fornecedor de produtos e serviços se utiliza dessa modalidade de comunicação, o que não acarretará problemas se o seu anúncio classificado estiver claramente identificado como mensagem publicitária. Para tal situação aplicam-se as regras do Código de Defesa do Consumidor.

Patologias surgem, porém, quando fornecedores se fazem passar por particulares, levando o consumidor a crer que estará celebrando o contrato proposto com pessoa física que não se dedica à comercialização daqueles produtos ou serviços.

Nessa hipótese, verifica-se a violação do princípio da informação (arts. 31 e 33, CDC), tornando a publicidade abusiva (art. 37, § 2º, CDC).

Também tem sido comum encontrar casos de empresas utilizando-se dos *sites* de "leilão" para anunciar produtos. Da mesma forma, ao ocultarem sua condição de fornecedores e o conseqüente caráter comercial de sua mensagem, surgirá a patologia.

Patrocínio abusivo. Essa modalidade de publicidade é pouco dada a patologias. Vislumbram-se desvios ocasionalmente em relação à inadequação entre o produto anunciado (ou o comportamento a ele associado) e o tema ou público-alvo do *site*.

---

[24] Envio de mensagens publicitárias em massa somente a usuários que solicitaram ou autorizaram previamente a sua remessa.

Assim, por exemplo, será abusiva (art. 37, § 2º, CDC) a publicidade que consistir no patrocínio de um *site* destinado a adolescentes por uma marca de cigarro ou bebida alcoólica. Seria caso de lesão a princípios como o da autodeterminação, bem como agressão a garantias constitucionais como saúde, segurança e proteção econômica.

Merchandising e publicidade subliminar. O merchandising está presente também na internet. Jogos desenvolvidos especialmente para promover determinado produto, uma tendência atual, por exemplo, somente não configurarão publicidade abusiva se, desde o momento em que se informa ao consumidor sobre a existência do jogo ele for clara e adequadamente informado de sua finalidade de promoção de vendas. Caso esse esclarecimento não seja feito ou seja adequado e insuficiente, presente estará a abusividade (art. 37, § 2º, CDC), por violação dos princípios da informação (art. 31, CDC) e autodeterminação.

Igualmente abusivo será o *merchandising* que se aproveitar da convergência tecnológica internet/TV para, sem aviso prévio quanto à natureza comercial do evento, induzir o consumidor a adquirir por impulso os produtos e serviços que sejam ostensivamente consumidos pelos personagens de peças de teledramaturgia, filmes ou eventos culturais e esportivos.

Publicação de mensagem publicitária em ambiente indevido (*chat* ou *newsgroup*). Trata-se de forma extrinsecamente abusiva de publicidade, vez que a cultura da Internet considera esses ambientes inadequados à atividade comercial. Realmente, o *chat* destina-se à comunicação interpessoal em tempo real, enquanto que os *newsgroup* têm como finalidade a troca de informações sobre assuntos muito específicos (religião, sexo, ufologia, saúde). Não tendo sido o usuário clara e previamente informado que se trata de um ambiente de *chat* ou de *newsgroup* especialmente destinado à divulgação de produtos e serviços, a conduta é francamente abusiva (art. 37, § 2º, CDC), por violadora dos princípios da autodeterminação, privacidade, informação (art. 31, CDC) e, se a mensagem não for claramente identificável como comercial, do princípio da identificação da mensagem publicitária (art. 36, CDC).

Oportunismo diante do erro. É conduta claramente abusiva a que é adotada por alguns *sites* comerciais ao adquirir domínios específicos ou genéricos que atraem para si o usuário que digitou erroneamente um endereço eletrônico. Assim, por exemplo, ao digitar por engano ".com" em lugar de ".org", para acessar o *site* de uma organização sem fins lucrativos, o usuário é conduzido para um *site* comercial.

Não se trata aqui somente de estabelecer confusão de marcas (procedimento abusivo tanto no aspecto concorrencial quanto no que tange à defesa do consumidor), já que nem sempre o endereço que se desejava acessar pertence a uma empresa, mas também e principalmente de criar mecanismos de atração sempre que um endereço com determinadas características, porém inexistente, for digitado. A abusividade (art. 37, § 2º, CDC) aqui é patente, vez que a conduta contraria o princípio da autodeterminação.

Figuração indevida em mecanismos de busca. Diante do fantástico volume de informações contido na internet, impossível seria localizar aquela que se deseja sem o auxílio de mecanismos de busca, que são aplicativos nos quais se informa os argumentos de pesquisa, a fim de que seja exibida uma listagem de todos os *sites* que contenham as expressões indicadas.

Para figurar num mecanismo de busca, dois caminhos são possíveis: o cadastramento e a utilização de *metatags*.

O cadastramento consiste no preenchimento de um formulário pelo responsável por um *site*, no qual serão informados os temas e palavras-chave pelas quais o *site* possa ser localizado.

Já o *metatag* ou simplesmente *tag* consiste em "bandeirolas" inseridas no *site*, que sinalizam a existência de determinado tema ali. Na realidade, são informações invisíveis ao usuário que contêm palavras-chave (tantas quantas e quais queira o responsável pelo *site*) embutidas no código-fonte de uma página da internet. Essas informações são lidas e armazenadas por *spiders* (aranhas, vez que circulam na *Web*, teia) ou *bots* (contração de *robots*, robôs, por traba-lharem continuamente e sem descanso), que permanentemente varrem a internet em busca desses *tags*.

Assim, diariamente os mecanismos de busca que se utilizam desse sistema têm seus bancos de dados atualizados, a fim de fornecer informações mais precisas a seus usuários.

O problema da abusividade surge quando a empresa faz inserir dados no formulário de cadastramento ou nas *metatags* de suas páginas informações inverídicas. Por exemplo, ao inserir o argumento "consumidor" num mecanismo de busca, poderá ser exibido um *link* que na realidade leva a uma página comercial ou

a um *site* onde se paga para se ter acesso a material pornográfico[25]. Quando isso ocorre, estamos diante de conduta abusiva (art. 37, § 2º, CDC), por lesiva aos princípios da autodeterminação, informação (art. 31, CDC), identificação da mensagem publicitária (art. 36, CDC, especialmente se a dissimulação se estender além da página de abertura do *site*).

CORREÇÃO DO DESVIO PUBLICITÁRIO

Da mesma forma como o Código de Defesa do Consumidor é plenamente aplicável às formas de desvio publicitário detectadas na internet, sendo suficiente para a sua adequação como condutas violadoras dos direitos atribuídos aos consumidores, também é possível reprimir, corrigir e punir essas condutas por meio da aplicação das normas nele contidas.

Assim, a aplicação de multas, a determinação de cessação da conduta, a imposição de contrapublicidade e outras sanções administrativas (artigos 55 a 60 do CDC), penais (61 a 80) e judiciais de toda espécie (artigos 83 e 84) são perfeitamente aplicáveis aos responsáveis pela publicidade patológica (anunciantes, agências, provedores).

Apenas três questões são capazes de oferecer dificuldades na correção do desvio publicitário, sem no entanto obstar sua efetividade:

A primeira delas diz respeito à **identificação do anunciante**.

Não é raro constatar que alguns anunciantes de produtos e serviços não são, propriamente, empresas. Tratam-se muitas vezes de empreendimentos irregulares que realizam vendas clandestinamente, construindo *sites* na internet para esse intento, de forma anônima ou sob dados falsos. Outras vezes tratam-se de empresas que alteram sua identidade para figurar na Internet como se outra pessoa jurídica (ou mesmo física) fossem. Outros fornecedores sequer disponibilizam um *site*, sendo toda a operação tratada por meio de mensagens eletrônicas.

---

[25] Hipótese tão freqüente que já se apurou que praticamente não existe palavra digitada como argumento de pesquisa em mecanismo de busca que não resulte em *links* para *sites* de sexo.

A solução para o desvio publicitário nessa hipótese passa necessariamente pela figura do provedor de presença na internet. É dele a responsabilidade pela conferência ao menos dos dados cadastrais daqueles que utilizam seus serviços para estabelecer presença na internet, a fim de que se possa localizá-los para aplicação da lei. Caso descuide desse dever, passa o provedor a ser responsável pelos atos praticados pelo anunciante que não possa ser localizado.

Com isso tem-se que, publicada ou remetida mensagem publicitária patológica, na impossibilidade de localização do anunciante, deve ser promovida a retirada ou cessação de remessa do material lesivo (ou mesmo a exclusão da presença do anunciante na rede) junto ao provedor do serviço do qual aquele se utiliza para ter acesso à Internet. Desatendendo a determinação administrativa ou judicial de fazê-lo, deve passar o provedor a responder solidariamente pelo evento nas esferas administrativa e civil, além de criminalmente, na pessoa de seu representante legal.

A segunda questão, que não exclui a primeira, é a da **territorialidade**.

Como se sabe, a internet é um instrumento de comunicação global que desconhece fronteiras geográficas. Nem por isso há que se falar que abolidas estão as nações alcançadas pela Grande Rede.

Destarte, quando o anunciante for empresa sediada ou representada no Brasil, hospedada em provedor brasileiro e o país para o qual vende é o Brasil, nenhuma dificuldade se revela, vez que é evidente a aplicação da lei brasileira.

No entanto, há casos em que o anunciante é sediado ou representado no Brasil e vende para consumidores residentes no país, porém, o provedor de que se utiliza é estrangeiro. Nessa hipótese surge o problema de falsidade ou inexistência de identidade do anunciante. Como aplicar a lei brasileira? Já surgem precedentes judiciais apontando para a solução de aplicação de multa diária ao provedor até que o desvio publicitário seja corrigido. Essa multa, por óbvio, necessita de homologação pela nação sede do provedor para que possa ser executada.

Uma terceira possibilidade é a do anunciante estrangeiro, que utiliza provedor igualmente estrangeiro, mas vende seus produtos ou serviços para público residente no Brasil[26].

---

[26] Importante destacar que a maioria das empresas norte-americanas e européias não aceita pedidos de compra originados de outros países ou blocos econômicos.

O grande problema surge quando a legislação do país onde se localiza o anunciante ou o provedor não considera patológica a conduta imputada ao anunciante.

Nesse caso a doutrina diverge, mesmo dentre os juristas brasileiros. A corrente mais benéfica ao consumidor brasileiro (e por isso a que se prefere) é no sentido de que se aplica às relações de consumo a legislação do país no qual se vende, conforme o sentido da Convenção de Roma e das leis do Mercosul.

Por fim, resta a questão **efetividade da publicidade corretiva** imposta (contra-publicidade ou, na expressão adotada pelo CDC, contrapropaganda).

O parágrafo 1º do art. 60 do Código de Defesa do Consumidor determina que a contrapropaganda será veiculada "da mesma forma, freqüência e dimensão e preferencialmente no mesmo veículo, local, espaço e horário".

Seria, porém, ante as peculiaridades da internet, essa veiculação suficiente para cumprir o preceito legal que exige que a publicidade corretiva seja capaz de desfazer o malefício da publicidade patológica?

Em muitos casos, a resposta é negativa.

Em sua maior parte, a publicidade veiculada na internet é efêmera. Como exemplo, pode-se tomar o fato de que um endereço (página ou *site*) visitado hoje pelo internauta muito provavelmente não o será novamente por um largo período de tempo (por vezes o endereço sequer estará ativo numa segunda tentativa de visita), sendo praticamente impossível fazer com que a contrapublicidade atinja os consumidores expostos à mensagem publicitária patológica ali antes exibida.

Por isso é que a expressão "preferencialmente", inserida no dispositivo legal em estudo, deve ser interpretada da forma mais favorável ao consumidor, em consonância com a parte final do parágrafo e com o microssistema do Código: haverá hipóteses em que a mídia tradicional (jornais, revistas, *outdoors*, rádio, televisão), deverá ser utilizada (às custas do infratores, conforme o *caput* do artigo 60) para a divulgação da publicidade corretiva, a fim de buscar a efetiva anulação dos efeitos nocivos da publicidade enganosa ou abusiva.

Pode-se, então, concluir que a legislação brasileira de defesa do consumidor, por adotar o modelo principiológico (abrangente e flexível, pois), é bastante e suficiente para detectar o desvio publicitário, bem como para preveni-lo, coibi-lo, corrigi-lo e suprimi-lo.

Certamente que uma regulamentação específica viria a tornar menos tormentoso o tema, ao pacificar as dúvidas de interpretação e harmonizar os preceitos corporativos (auto-regulamentação) e legais. Essa legislação teria de ser eminentemente principiológica, abrangente e flexível, para fazer frente à velocidade com que surgem, desaparecem e são modificadas as modalidades de publicidade e as mídias que as suportam.

Jean Jacques Erenberg,

procurador do Estado de São Paulo;
professor de Prática Jurídica na Universidade Cidade de São Paulo;
especialista em Interesses Difusos e Coletivos pela ESMP

BIBLIOGRAFIA

ALVIM, Arruda et al. *Código do consumidor comentado.* São Paulo, Revista dos Tribunais, 1991.

BULGARELLI, Waldirio. *Questões contratuais no código de defesa do consumidor*. São Paulo, Atlas, 1999.

CABRAL, Plínio. *Propaganda, técnica de comunicação industrial e comercial*. São Paulo, Atlas, 1986.

CHAISE, Valéria Falcão. *A publicidade em face do Código de Defesa do Consumidor*. São Paulo, Saraiva, 2001.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo, Saraiva, 2000.

CRASWELL, Richard. Interpreting deceptive advertising. *Boston University law review.* Boston, v. 24, no 4, p. 670, 1985.

DE LUCCA, Newton e SIMÃO Filho, Adalberto (coord.). *Direito & Internet - aspectos jurídicos relevantes*. Bauru-SP, Edipro, 2000.

FARIA, José Eduardo. *O direito na economia globalizada*. São Paulo, Malheiros, 1999.

FEDERIGHI, Suzana Maria Pimenta Catta Preta. *Publicidade abusiva.* São Paulo, Juarez de Oliveira, 1999.

FILOMENO, José Geraldo Brito. *Manual de direitos do consumidor*. São Paulo, Atlas, 1999.

GRECO, Marco Aurélio e MARTINS, Ives Gandra da Silva (coord.). *Direito e internet : relações jurídicas na sociedade informatizada*. São Paulo, Revista dos Tribunais, 2001.

GRINOVER, Ada Pelegrini e outros. *Código brasileiro de defesa do consumidor*. Rio de Janeiro, Forense Universitária, 1999.

JUNQUEIRA, Miriam. *Contratos Eletrônicos*. Rio de Janeiro, Mauad, 1997.

MARZOCHI, Marcelo de Luca. *Direito.br : Aspectos jurídicos da internet no Brasil.* São Paulo, LTr, 2000.

MAZZILLI, Hugo Nigro, *Princípios processuais da proteção dos interesses difusos e coletivos*. São Paulo, Escola Superior do Ministério Público, 1998.

NUNES Júnior, Vidal Serrano. *Publicidade Comercial*. São Paulo, Juarez de Oliveira, 2001.

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

PIRATININGA, Luiz Celso de. *Publicidade: arte ou artifício?* São Paulo, T. A. Queiroz, 1994.

STIGLITZ, Gabriel A . *Potección jurídica del consumidor*. Buenos Aires, Depalma, 1990.

TAHARA, Mizuho. *Contato imediato com a mídia*. São Paulo, Global, 1987.

BREVÍSSIMAS CONSIDERAÇÕES SOBRE DELITOS INFORMÁTICOS

Augusto Eduardo de Souza Rossini

BREVÍSSIMAS CONSIDERAÇÕES SOBRE DELITOS INFORMÁTICOS

Augusto Eduardo de Souza Rossini

SUMÁRIO: 1.Introdução – 2. Escorço histórico – 3. Novos paradgmas – 4. Conceito de "delito informático" – 5. Classificação dos delitos informáticos – 6. Bem jurídico – 7. Considerações finais.

1. INTRODUÇÃO

O presente texto tem por escopo trazer à discussão interessante tema que atualmente se estabelece como mais uma preocupação para o Ministério Público, qual seja, os 'delitos informáticos', tendo a Instituição imperiosa necessidade de estabelecer ferramentas e instrumentos para o enfrentamento da questão, criando uma política para o que está para chegar – se é que já não chegou.

Aqui não se traz qualquer solução, mas se apontam temas para debate, a fim de que em futuro muito próximo o assunto não seja uma novidade assombrosa e sim mais um tipo de criminalidade que o Ministério Público terá que ordinariamente enfrentar, como corolário do princípio insculpido no art. 129, inciso I, da Constituição Federal.

Isso porque, com a recente disseminação dos computadores pessoais, o número de acessos ilegais à rede mundial de computadores (internet) aumentou consideravelmente, havendo quem diga que o Brasil se estabelece como 'paraíso cibernético', ante a pouca preocupação com que o assunto é tratado, gerando, como um todo, inquestionável prejuízo econômico, moral etc.

2. ESCORÇO HISTÓRICO[1]

Não é de hoje que o homem se preocupa com a sistematização de informações, visando, com a criação de ferramentas próprias, a diminuição de gastos de energia

[1] PIMENTEL, Alexandre Freire. *O Direito Cibernético: Um Enfoque Teórico e Lógico-Aplicativo*. Rio de Janeiro: Renovar, 2000, p 5/21.

para a realização das tarefas rotineiras. Assim aconteceu com o ábaco, criado na região hoje conhecida como China, por volta de 3.500 a.C. No Oriente Médio arqueólogos encontraram tábuas de argila contendo cálculos matemáticos e tabuadas de multiplicação, que teriam sido criadas por volta de 1.700 a.C. Os Babilônios criaram as atuais unidades de tempo, como hora, minutos e segundos.

O escocês Jonh Napier, em 1614, criou seus "Bastões", que também podem ser considerados como ferramentas para a computação de dados. Os 'Bastões de Napier' evoluiram para os 'círculos de proporção' de William Oughtred.

Blaise Pascal criou em 1642, quando contava com apenas 19 anos, uma máquina calculadora, denominada "Máquina Aritmética de Pascal.

Charles Babbage, em meados de 1822, criou o projeto da 'Máquina Analítica'.

E, em 1880, Herman Hollerith criou a 'Máquina de Recenseamento' para a Agência Americana de Estatísticas, visando a apuração do recenseamento ocorrido naquele país. Interessa destacar que a 'International Business Machines Corporation' foi criada por Hollerith em 1890 e é nada mais do que a atual IBM, empresa transnacional que é de todos conhecida.

Não é pacífica a 'paternidade' do moderno computador, ora se dizendo que fora criado por Howard H. Aiken em 1937, ora se afirmando que fora criado por Atasanoff e Berry em 1940. O que fica, entretanto, é que a evolução dessa tecnologia se deveu ao advento da Segunda Guerra Mundial, que gerou, além de grande desgraça, enorme avanço tecnológico nas mais variadas áreas, inclusive na computação.

É possível se afirmar que há cinco gerações de computadores:

1.ª geração (de 1940 a 1952) – computadores à base de válvulas à vácuo – alimentação por cartões perfurados – uso exclusivamente militar (nessa época surgiu a teoria da 'informática jurídica' desenvolvida por Lee Loevinger).

2.ª geração (de 1952 a 1964) – substituição das válvulas por transistores – maior velocidade – uso administrativo e gerencial.

3.ª geração (de 1964 a 1971) – substituição dos transistores pelos circuitos integrados (surgidos em 1964) – miniaturização dos grandes computadores – evolução dos *softwares* e criação dos '*chips* de memória' – ampliação do uso comercial.

4.ª geração (de 1971 a 1981) – substituição dos circuitos pelos microprocessadores – criação dos *floppy disks*, ou 'disquetes' para o armazenamento de dados – nascimento da telemática.

5.ª geração (de 1981 até hoje) – enorme avanço da computação – criação da inteligência artificial, da linguagem natural e da altíssima velocidade do processamento de dados – principal novidade: disseminação da internet.

Até esse ponto, resumidamente se demonstrou a evolução da 'máquina', do próprio computador, que é, repita-se, mais uma invenção humana com vistas à redução dos gastos nas tarefas de sistematização e uso de dados. É mais uma ferramenta criada pelo gênio humano para enfrentar com menos esforço os percalços que o meio impõe.

Entretanto, corolário da máquina, foi a criação da internet, que estabeleceu e estabelece verdadeira 'revolução copérnica' nos conceitos de comunicação, educação, cultura e economia.

A internet é a rede mundial de computadores, que em última e singela análise, nada mais é do que um grande computador interligado, pois cada pessoa que o acessa, nele se insere e dele passa a fazer parte, naquele momento e através da 'autoria mediata' do provedor ou portal. No momento em que o usuário acessa a internet, se "pluga", sua máquina compõe o "Grande Computador" e na medida em que endereços são digitados, novos contatos se estabelecem, para qualquer finalidade.

Dessa forma, a internet, que também é uma ferramenta para o desenvolvimento do gênio humano, para o alcance do bem comum, passou também a compor o instrumental de pessoas que de qualquer forma agem contra o estamento, contra a maioria. Socorrendo-me da singeleza das definições infantis: não só pessoas 'do bem' utilizam a internet, mas também as 'do mal'... E são estas que nos preocupam, dada a potencialidade lesiva do que fazem (ou deixam de fazer) no âmbito da Rede.

Interessa, neste ponto, destacar que a internet também tem sua história[2].

A idéia de uma rede interligada surgiu em 1962, durante a "Guerra Fria", e foi imaginada para proteger a rede de computadores do governo norte-americano após um ataque nuclear. Planos detalhados foram apresentados em 1967, tendo sido criada a ARPANET em 1968, estabelecendo-se o germe do que é hoje a internet.

Somente em 1969 houve a interligação, via *backbones*, de quatro *hosts*: os *campi* da Universidade da Califórnia, em Los Angeles e Santa Bárbara; a Universidade

---

[2] Estudo LAFIS. Brasil – Serviços de Telecomunicações : Internet. 20/Nov/2001.

de Utah; e o SRI de Stanford. Em 1971, a rede cresceu e foram abrangidas agências governamentais e militares norte-americanas, incluindo a NASA.

Em 1972 foi lançado o primeiro programa de correio eletrônico (*e-mail)* e, em 1973, foram estabelecidas as primeiras conexões internacionais, interligando-se Estados Unidos da América, Reino Unido e Noruega.

Em 1974 foi lançado o primeiro serviço comercial de transmissão de dados, nada mais do que uma versão comercial da ARPANET.

Em 1976 foram incorporadas conexões de rádio e satélite e em 1979 foi criada a Usenet, que era uma rede descentralizada de grupos de notícias.

Enquanto que nessa época (final dos anos 70 e início dos 80), nos Estados Unidos, tal cultura restringia-se praticamente às áreas militar e universitária, surgiu na França a Rede Minitel, que foi verdadeiramente o primeiro sistema telemático de uso comercial (lembrando-se que a internet somente entrou em efetivo uso comercial em 1994). Na França, foi a “France Telecóm” a empresa responsável pela criação do referido sistema, o qual utilizava a rede de telefonia para atingir um grande número de usuários, oportunidade em que outros usos foram estabelecidos, v.g. transmissão de mensagens, jogos etc. Contudo, a experiência francesa não saiu de seu território, dadas as peculiaridades técnicas (incompatíveis com o resto do mundo) e o grande custo que disso derivava.

Essa experiência européia evidenciou a enorme demanda de tal modalidade de serviços, o que veio a efetivamente ocorrer na década de 90. Entretanto, foi na década de 80 que ocorreu a transição da citada ARPANET para o que atualmente se denomina internet.

Em 1982 foi estabelecido o padrão IP/TCP, até hoje usado na rede, tornando-se obrigatório em 1983 e, somente nesse momento, se pôde conceituar a internet como um conjunto de redes interligadas.

Interessa destacar que nessa mesma época surgiu o conceito de *hacker*, a denominação Ciberespaço – usado no romance de William Gibson ‘Neuroromancer’ e tantas outras terminologias até hoje usadas. Evidencia-se, pois, que alguns conceitos que surgiram nesse momento histórico são até hoje usados por milhões de pessoas e foram aproveitados pelo próprio Direito Penal.

Em 1984 a ARPANET foi dividida em duas redes: a Milnet (Militar) e a Arpanet (acadêmica), ambas sob o controle do Departamento de Defesa dos Estados Unidos.

Nesse mesmo ano foi criado o sistema de nomes e domínios, que substituiu o sistema numérico, permitindo-se, dessa maneira, o acesso mais rápido a outros servidores, sem a necessária memorização de grandes códigos numéricos.

Em 1985 foi criada a NSFNET e foram estabelecidos cinco centros de supercomputação, o que permitiu uma explosão de conexões, notadamente nas universidades, permitindo-se, nesse momento, o desenvolvimento da estrutura do que hoje é a internet.

Em 1988, Dinamarca, Finlândia, Canadá, Islândia, França, Suécia e Noruega foram interligados a NSFNET e tais conexões restringiam-se ao campo universitário, podendo-se afirmar que nesse instante se estabeleceu o núcleo da atual internet.

Em 1989 aderiram a NSFNET Austrália, Alemanha, Israel, Itália, Japão, México, Holanda, Nova Zelândia, Reino Unido e Porto Rico. Nesse ano, o número de servidores chegou a cem mil e ocorreu a primeira experiência de correio eletrônico comercial.

Em 1990 a Arpanet foi desativada pelo Departamento de Defesa, sendo substituída pelos *backbones* da NSFNET e foi criado um sistema de hipertexto com o auxílio do CERN. Nesse ano, o Brasil também foi conectado à NSFNET, bem como Argentina, Áustria, Bélgica, Chile, Grécia, Índia, Irlanda, Coréia do Sul, Suíça e Espanha.

Em 1991 o governo norte-americano criou a NREN (National Research and Education Network), com a função de conduzir o tráfego de alta velocidade para fins de pesquisa, sem qualquer finalidade comercial. Redes privadas foram conectadas à Internet. Nesse mesmo ano, praticamente todos os países da Europa Ocidental também se integraram à rede, o mesmo ocorrendo com Hong Kong, Portugal, Cingapura, África do Sul, Taiwan, Tunísia, Croácia, República Checa, Hungria e Polônia. E surgiram os grandes provedores da internet.

Em 1992 foi implementada a primeira ferramenta de busca e se integraram à rede Venezuela e Equador.

Em 1993 muitos *sites* importantes foram criados, v.g. o da Casa Branca, o das Nações Unidas e o do Banco Mundial. Aderiram à rede, Costa Rica, Peru, Colômbia, Nicarágua, Panamá, Uruguai, Rússia, Ucrânia e China.

Em 1994 surgiram serviços de entrega pela rede (Pizza Hut), o primeiro banco *on-line* e os primeiros *shoppings* virtuais.

Em 1995 a internet foi privatizada, com o estabelecimento de provedores independentes. No Brasil, a Embratel deixou de ter o monopólio das transmissões.

A Internet Society desenvolveu novos protocolos IP com capacidade de manejo de bilhões de endereços.

O ano de 1996 se caracteriza pela primeira iniciativa de controle oficial do uso da internet: o Congresso Norte-Americano tenta proibir a distribuição de material pornográfico através da rede, tendo, contudo, a Suprema Corte daquele país considerado a lei inconstitucional.

Em 1997 houve a ampliação dos conflitos legais advindos do uso da rede. Nos mais variados lugares ações foram propostas, v.g. empresas telefônicas tentaram impedir a transmissão de voz pela rede; houve grandes embates na defesa de direitos autorais; além de outras lides. O crescimento do uso da rede é confirmado pelas estatísticas: estima-se que neste ano foram trocados 85 bilhões de *e-mails* em todo o mundo.

Em 1998 a Organização Mundial do Comércio (OMC) avaliou que os negócios na rede atingiram 300 bilhões de dólares; foram criados os *notebooks* e surgiram os provedores gratuitos, praticamente desaparecidos nos dois anos seguintes.

De 1999 até hoje a internet somente cresceu, chegando a bilionários patamares, permitindo-se concluir que já faz parte do cotidiano de uma grande parcela da sociedade moderna.

Em novembro de 2001, influenciada pelos episódios de 11 de novembro de 2001 na cidade de *New York,* a Comunidade Européia editou Convenção sobre o *Cybercrime*, estabelecendo conceitos basilares, quer de direito material, quer de direito processual, sugerindo-se rol de 'tipos-padrão' para os países signatários, evidenciando o interesse de que haja a desejada padronização universal, tendo em vista uma das principais características desse tipo de criminalidade – a transnacionalidade. O desapego a qualquer forma de fronteira faz desaparecer arraigados conceitos de soberania nacional e, conseqüentemente, de tradicionais regras de competência.

3. NOVOS PARADIGMAS

Todo esse quadro demonstra que a sociedade moderna está diante de mais uma forma de criminalidade, da mesma forma como ocorre, a exemplo, com a criminalidade econômica, ambiental, consumerista e financeira, todas caracterizadas

pela enorme complexidade com que se apresentam e com fundamental ponto em comum, qual seja, a ofensa a bens jurídicos de caráter difuso.

Ora, ante o histórico da internet, pode-se perceber que ela nasceu no seio do Estado (para fins militares), passando para a utilização acadêmica, chegando, por fim, ao uso comercial, disseminando-se pelo Globo.

No início de sua última fase, a comercial, acreditou-se na auto-regulamentação. Pensou-se que o próprio mercado conseguiria impedir o seu mau uso por pessoas inescrupulosas. Imaginou-se, sinceramente, que na Rede Mundial de Computadores, o Estado não teria a necessidade de interferir pois os próprios usuários/provedores conseguiriam 'dar conta do recado'.

Contudo, os últimos episódios no mundo – 'Setembro Negro', sistemática invasão de *hackers* e *crackers* a grandes computadores de empresas, disseminação da pedofilia etc. –, fizeram com que a crença na auto-regulamentação caísse por terra, de forma que o ramo do Direito chamado de 'ultima ratio', não outro senão o Direito Penal, fosse instado a interferir. O fato é que o Estado teve que dirigir seus olhos para esse problema a fim de garantir a proteção a bens jurídicos preciosos para a sociedade.

Interessante que tal busca por soluções mais drásticas – típicas do Direito Penal – ocorreu de modo uniforme pelo mundo. A preocupação que inicialmente circunscrevia-se aos Estados Unidos da América passou a ser a de todos os países em que a internet é uma realidade e onde, invariavelmente, há uma gama de delitos praticados no âmbito dessa rede.

Diante dessa inquestionável conclusão, outra não é a alternativa senão apontar alguns critérios para tentar estabelecer um sistema, dentro do Direito Penal, para enfrentar a questão.

4. CONCEITO DE 'DELITO INFORMÁTICO'

Dentro desse sub-tema, é imperioso consignar que ainda não se definiu um conceito uniforme de Delito Informático. Aliás, nem mesmo uma singela denominação se estabeleceu, pois há quem o trate por 'Criminalidade Mediante Computadores'[3],

[3] TIEDEMANN, Klauss. *Poder Económico y Delito*. Barcelona : Editorial Ariel, 1985, p. 120.

Criminalidade do Computador, Delito Informático, Criminalidade da Informática, Delitos Cibernéticos, entre outros.

Ouso denominá-los 'delitos informáticos', pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível 'conexão' à Rede Mundial de Computadores.

Aliás, no âmbito da internet, a denominação seria 'delito cibernético ou telemático'.

'Delitos informáticos', então, seriam gênero, do qual 'delito cibernético' seria espécie. E em razão da recenticidade do assunto, outras denominações podem surgir com o amadurecimento da questão.

Interessa destacar que Tiedemann[4], já em 1985, chegou a definir: "*Criminalidad Mediante Computadoras: se alude a todos los actos, antijuridicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados com el empleo de un equipo automático de procesamiento de datos*".

Mas, o melhor conceito para 'delito informático' é o cunhado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: *"O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados*".

Embora a 'conduta não ética' esteja inserida nesse conceito, tal é incompatível com a cultura jurídica brasileira, mesmo porque parte-se do pressuposto que toda norma penal incriminadora é eticamente indesejável. Aliás, seria um absurdo que tipos penais não tivessem por fundamento a repulsa moral da Sociedade.

5. CLASSIFICAÇÃO DOS DELITOS INFORMÁTICOS

Há os Delitos Informáticos Puros, aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, sendo que a informática é

---

[4] TIEDEMANN, Klauss. Ob. Cit. P. 122.

composta principalmente do *software*, do *hardware* (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. A conduta (ou ausência dela) visa exclusivamente ao sistema informático do sujeito passivo.

São exemplos, atos de vandalismo contra a integridade física do sistema em razão de acesso desautorizado – as condutas dos *hackers* e *crackers* – ainda não tipificadas no Brasil, além de algumas já previstas, como as hipóteses preconizadas na Lei n 9.609/98 (Lei de Proteção de Software).

E há os Delitos Informáticos Mistos, em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático. Alguns de seus exemplos são o estelionato, a ameaça e os crimes contra a honra, podendo imaginar-se, inclusive, homicídio por meio da internet (mudança à distância de rotas de aviões, alterações à distância de medicamentos com o desautorizado uso do sistema informático de um hospital).

6. BEM JURÍDICO

Ante a classificação acima, há que se indagar: há um bem jurídico autônomo identificado neste novo 'ramo' do Direito Penal? Acredito que sim.

Antes, porém, é de bom alvitre se recordar que bem jurídico é "*aquele valor ético-social que o direito seleciona, com o objetivo de assegurar a paz social, colocando sob sua proteção para que não seja exposto a perigo de ataque ou lesões efetivas*"[5]. Wezel, *apud* Assis Toledo, observa que "*a soma dos bens jurídicos constitui a própria ordem social, e por isso, o significado de um bem jurídico não deve ser apreciado isoladamente, mas sim, em conexão com toda a ordem social*".

Imperioso concluir, pois, que o Direito Penal tem por escopo fundamental a proteção de bens jurídicos (e não poderia ser de outra forma em um Regime Democrático de Direito).

Ora, se aqui se aponta a necessidade da intervenção do Direito Penal na Informática, sustentando-se, inclusive, que há Delitos Informáticos, o que exatamente se busca proteger?

---

[5] TOLEDO, Francisco de Assis, *Princípios Básicos de Direito Penal*, São Paulo, Saraiva, 4 ed. 1991.

Se admitirmos a classificação acima, a indicação dos bens jurídicos nos "Delitos Mistos" não é tarefa difícil, pois são classicamente consagrados: no estelionato praticado por meio da internet, o bem jurídico protegido é o patrimônio; nos crimes de calúnia, injúria e difamação cometidos por meio da Rede, o bem jurídico é a honra; e assim com outras modalidades de delitos.

Nos "Delitos Puros" os bens jurídicos a se proteger também não são difíceis de apontar: na ainda atípica conduta do *cracker* (que invade e destrói o que há no computador da vítima) o bem jurídico continua sendo o patrimônio, pois tal conduta não deixaria de caracterizar o 'dano informático'; já na tipificada 'pirataria de *software*', o bem jurídico protegido é a propriedade intelectual.

Mas há um bem jurídico absolutamente permanente que é a Segurança Informática, que existe independentemente dos bens jurídicos individuais e coletivos que possam existir concomitantemente numa conduta típica praticada no âmbito aqui estabelecido (da internet).

Na tríplice classificação proposta por SMANIO[6] e aqui admitida como a melhor[7], trata-se de um bem jurídico-penal de natureza DIFUSA. Isto porque, além de atingir um número indeterminado de pessoas, gera conflituosidade entre o interesse dos usuários da internet (incontáveis), aí incluídos os usuários comuns, além dos *hackers* (pichadores cibernéticos), *crakers* (*punks* cibernéticos) e o das grandes corporações, quer de empresas fornecedoras de bens e serviços, quer de provedores de acesso.

Entretanto, nesse trabalho, o que ora mais interessa é apontar os elementos da Segurança Informática: a) Integridade – a informação deve ser fidedigna e completa e somente o usuário pode mudá-la; b) Disponibilidade – o usuário deve ter a informação

---

[6] SMANIO, Gianpaolo Poggio. *Tutela Penal dos Interesses Difusos* – São Paulo : Atlas, 2000, p. 108

[7] SMANIO, Ob. cit. P 108: "*a) primeiramente, os bens jurídico-penais de natureza individual, que são os referentes aos indivíduos, dos quais estes têm disponibilidade, sem afetar os demais indivíduos. São, portanto, bens jurídicos divisíveis em relação ao titular. Citamos como exemplo, a vida, a integridade física, a propriedade, a honra etc.; b)- os bens jurídico-penais de natureza coletiva, que se referem à coletividade, de forma que os indivíduos não tem disponibilidade sem afetar os demais titulares do bem jurídico. São, dessa forma, indivisíveis em relação aos titulares. No Direito Penal, os bens de natureza coletiva estão compreendidos dentro do interesse público. Podemos exemplificar com a tutela da incolumidade pública, da paz pública etc.; c)- os bens jurídico-penais de natureza difusa, que também se referem à sociedade em sua totalidade, de forma que os indivíduos não têm disponibilidade sem afetar a coletividade. Ocorre que os bens de natureza difusa trazem uma conflituosidade social que contrapõe diversos grupos dentro da sociedade, como na proteção do meio ambiente, que contrapõe, por exemplo, os interesses econômicos industriais e o interesse na preservação ambiental, ou na proteção das relações de consumo, em que estão contrapostos os fornecedores e os consumidores, a proteção da saúde pública, enquanto referente à produção alimentícia e de remédios, a proteção da economia popular, da infância e da juventude, dos idosos etc.*".

no momento em que necessite; e c) Confidencialidade – ninguém, sem consentimento, deve ter acesso ou divulgar a informação.

Na ausência de qualquer um desses elementos, a própria função da internet (sistema informático/telemático) desaparecerá e não alcançará todas as suas possibilidades. Não passará de mais um singelo meio de comunicação, como o rádio ou a televisão.

Inquestionavelmente, o poder da internet é muito maior, pois, repita-se, transformou sobremaneira a interatividade da sociedade moderna e não pode, e nem deve, ficar adstrita a somente uma de suas funções – a comunicação. A Rede Mundial de Computadores não tem limites, desde que não seja tolhida em sua essência.

Somente a título de exemplo, dada a insegurança que atualmente paira na internet, é bem possível que o usuário encontre num *site* de compras um produto que deseja muito adquirir e certamente fará o pedido através de *e-mail*. Ocorre que, muito provavelmente, o pagamento se efetuará por boleto bancário, ante o verdadeiro pavor de ter o número de seu cartão de crédito lançado no 'Ciberespaço'.

Ora, para que serve então a Rede? Somente para fins lúdicos? Ou é possível realizar negócios por meio dela?

Não estaria a livre iniciativa prejudicada se na internet não houvesse a imprescindível segurança para que os aludidos negócios fossem efetivamente estabelecidos?

A resposta a tais indagações passa pela solução do problema proposto no início desse texto, qual seja, o sistemático ataque ao recente tipo de criminalidade que se estabeleceu no âmago da Rede Mundial de Computadores.

Essa questão representa um verdadeiro desafio ao Ministério Público, que além de ser o titular exclusivo da ação penal pública (art.129, I, da Constituição Federal), também tem por função a defesa do regime democrático (art.128, *caput*, da Constituição Federal). E não se pode olvidar que a livre iniciativa é um dos fundamentos da República Federativa do Brasil (art.1º, inciso IV, última parte, da Constituição Federal).

Se de um lado a modernidade traz benefícios inquestionáveis à sociedade, também traz, de outra banda, enormes desafios àqueles que têm por função assegurar a paz social, dentre eles, com relevo, o Ministério Público.

7. CONSIDERAÇÕES FINAIS

Salvo melhor juízo, bases científicas estão postas de forma absolutamente clara: há uma definição do que seja 'delito informático'; há uma classificação; há um bem jurídico e há base legal (tipos penais).

Para começar está bom.

Há, contudo, muitíssimos outros assuntos dentro desse mesmo tema que demandam maior acuidade dos membros do *Parquet*. Há que se definir o que seja 'documento eletrônico', bem como 'correspondência eletrônica'. Há que se estabelecer dogmaticamente o local e o tempo dos delitos eletrônicos para que todas as conseqüências daí advindas ocorram, quer de direito material (v.g. início do prazo prescricional e decadencial), quer de direito processual (v.g. fixação da competência).

O conceito de soberania deve ser revisto, dada a peculiaridade dos delitos dessa espécie, em que é possível a conduta ser praticada em um país, o provedor estar localizado em outro e o resultado ocorrer em um terceiro. Nessa situação, qual seria o juízo competente?

Alguns tipos penais precisam ser criados v.g. invasões do *hacker* e do *cracker*, violação de correspondência eletrônica, dentre muitas outras.

Aspectos processuais merecem trato legal e doutrinário, inclusive no que tange às formas de investigação, v.g. a escuta autorizada de *e-mail*, a apreensão de dados eletrônicos através da 'clonagem' do disco-rígido, além de outras que certamente surgirão dada a velocidade do avanço tecnológico.

Postas todas essas premissas, é permitido se concluir que existem instrumentos jurídicos mais do que suficientes para dar início ao combate à criminalidade informática. Apertemos, então, a tecla *start*, uma vez que as bases dogmáticas já estão lançadas.

Em síntese, aqui se lança um desafio: o operador do Direito não pode ficar alheio ao que ocorre ao seu redor. O anacrônico mundo hodierno gera dificuldades que necessitam ser enfrentadas com sabedoria e determinação.

Augusto Eduardo de Souza Rossini,

promotor de Justiça, coordenador do Centro de Apoio à Execução

“MAILING LISTS” E DIREITO DO CONSUMIDOR

Ciro Expedito Scheraiber

"MAILING LISTS" E DIREITO DO CONSUMIDOR

Ciro Expedito Scheraiber

SUMÁRIO: 1. Introdução – 2. Da necessidade do marketing publicitário – 3. Dos instrumentos e formas do exercício do marketing (*e-commerce*) – 4. Dos bancos de dados de consumo como meios de difusão do crédito – 5. Das técnicas de difusão de endereços eletrônicos – 6. Da forma de arrecadação de nomes e endereços residenciais e eletrônicos. Do *cookie* – 7. Das malas diretas eletrônicas indesejáveis ou não solicitadas (*spams*) – 8. Da aplicabilidade do Código de Defesa do Consumidor no *webmarketing* – 9. Dos requisitos legais dos bancos de dados ou arquivos pessoais e de consumo – 10. As *mailing lists* como bancos de dados pessoais e de consumo – 11. Da violação da privacidade e das comunicações em geral – 12. Da prática comercial abusiva – 13. Conclusões.

1. INTRODUÇÃO

Se o direito do consumidor representou um avanço em termos de poder legiferante na regulação de direitos modernos, os chamados difusos, coletivos e individuais homogêneos, sobressai-se agora a sua aplicabilidade aos mesmos direitos ofendidos pelo fenômeno da *internet*, que a informática proporcionou.

É sabido que as relações de consumo buscam a regulação do mercado, procurando reequilibrar as relações, presente que se faz a vulnerabilidade do consumidor perante o fornecedor, como fenômeno sociológico antes do econômico.

Nesse contexto, e visualizando o consumo como satisfação de necessidades, não há que apartar os protagonistas, o consumidor e o fornecedor. Entre ambos, portanto, ressurge o elemento "relação de consumo", como categoria jurídica passível de tutela.

No campo econômico, em que se insere a relação de consumo, o fornecedor opera na busca da interrelação com atividades necessárias, sem as quais o mercado não se operaria, tais as técnicas de *marketing*.

E no exercício dessas técnicas, os meios utilizados são os mais diversos, ao tempo em que se apresentam os mais evoluídos, devido às necessidades da sociedade de massa, onde a modernidade não prescinde dos meios de comunicação rápidos e eficientes tais como a *internet* e a *intranet*.

Na prática do *marketing* comercial, por meio desses instrumentos (*webmarketing*),[1] novos horizontes aceleram o desenvolvimento, mas, ao mesmo tempo, desafiam a novas e não vislumbradas ofensas aos direitos tutelados, ou que demandam proteção, no âmbito das relações consumeristas.

A tecnologia, apartada do direito, induz ao espargir de seus tentáculos perante novas formas de tutela, onde outros enfoques do direito posto são exigidos.

Emergindo tais circunstâncias, é que se pretende analisar a aplicabilidade do direito do consumidor ao fenômeno das *mailing lists,* que constituem bancos de dados de consumo e que, por intermédio da *internet,* se apresenta como fato jurídico, social e econômico a merecer tutela, dados os abusos de que são alvos, em especial pela utilização de instrumentos e vias técnicas da informática, tais os chamados *cookies* e *spams*, decorrentes da utilização desregrada dos *e-mails* ou correios eletrônicos.

2. DA NECESSIDADE DO *MARKETING* PUBLICITÁRIO

O consumo é mutante, na medida em que as necessidades e os desejos se alteram, variando conforme se incorporem, ao passar do tempo, novas práticas comerciais envolvendo produtos e serviços, decorrente mesmo da evolução da tecnologia e do conhecimento.

Desde os tempos primevos da mera apreensão dos bens naturais e da simples troca, passando pela compra e venda direta (face a face) tendo como referencial um elemento de valor (ouro, moeda, etc), o "consumir" teve como característica a pessoalidade.

Ao depois a *prática comercial* se tornou ato habitual e profissional, itinerante ou estabelecida. As casas de comércio evoluíram para os hoje conhecidos super ou hipermercados, cujas empresas se agrupam em centros (*shopping centers*) e ainda estabelecem, por vezes, condutas uniformes (*dumpings*, *holdings*, cartéis, trustes, etc). Tornou-se impessoal.

---

[1] Segundo anota a EMBRATEL, **www.embratel.com.br *in*** "Marketing na *Internet*", com acesso em 08/08/01: " O que faz com um cliente mantenha os negócios com a sua empresa? É possível listar um sem número de fatores, mas pode-se resumir tudo em uma só palavra: lembrança. É a lembrança que faz com que tudo aconteça. E é essa a melhor definição para o marketing: gerar lembrança na mente do consumidor. Mas como isso é aplicado na *Internet*? Existe um termo recente, como tudo que diz respeito à *Internet*, chamado webmarketing. E o que é isso? 'É o sentido de adaptar e desenvolver estratégias de marketing no ambiente Web' . O trabalho de webmarketing contempla todas as etapas de trabalho de um website, como a concepção, o projeto, a adequação do conteúdo, o desenvolvimento, a manutenção e a divulgação".

O ponto marcante do crescimento comercial e industrial, pós segunda guerra, decorreu da revolução industrial, a partir da qual o crescimento da tecnologia e do conhecimento decolou, contínua e incessantemente. O vertiginoso crescimento populacional e a sofisticação decorrente da evolução social dão sustentáculo ao aperfeiçoamento tecnológico, que serve como elemento de ajustamento dos anseios sociais.

A complexidade da realidade e o atendimento ingente de necessidades similares proporcionaram a chamada produção em série de produtos e a especialização da prestação de serviços. Em decorrência, novos métodos de comercialização, modernamente chamados de *marketing*[2], tornaram-se instrumentos de colocação rápida e eficiente de produtos e serviços, donde a publicidade exerce papel destacado.

A necessidade de consumir, às vezes artificial, inserida no contexto social, é o móvel da indústria e do comércio, dá ensanchas à "sociedade de massas ou de consumo[3]". Para Ada Pelegrini Grinover, em resumo, são características da Sociedade de Consumo: a) número crescente de produtos e serviços; b) domínio do crédito e do *marketing*; c) dificuldades de acesso à justiça[4].

O *marketing*, portanto, constitui a energia imprescindível para a sobrevivência do fornecedor do mercado, pois ele representa a mola propulsora dos seus negócios, pelo qual faz apresentar e oferecer o seu produto ou o seu serviço. Hoje, mais que isso, para que seja eficiente, há que criar necessidades e desejos no contexto do mercado consumidor, a ponto de que necessidades às vezes artificiais se apresentem com caráter de essencialidade, sem cujas satisfações o consumidor teria frustrações insuperáveis[5].

---

[2] O consumidor, mesmo um ser econômico e social, está cada vez mais isolado e necessida mais e mais ser alcançado pela informação acerca dos produtos e serviços e também, por vezes, convencido da conveniência de sua aquisição.

[3] GRINOVER, Ada Pelegrini. " Código Brasileiro de Defesa do Consumidor Comentado pelos Autores do Anteprojeto". 6ª edição, Forense Universitária, Rio de Janeiro, 1999, p. 6.

[4] Consulte-se acerca do acesso à justica, em especial diante da evolução dos sistemas jurídicos, o "Acesso à Justiça" de Mauro Cappelletti e Bryant Garth, tradução de Ellen Gracie Northfleet, Porto Alegre, Ed. Fabris, 1988.

[5] MONTE, Mário Ferreira. "DA PROTEÇÃO PENAL DO CONSUMIDOR. O problema da (des)criminalização no incitamento ao consumo". Livraria Almedina, Coimbra, 1996. O autor luso expõe com riqueza a classificação das necessidades humanas. De acordo com o ensinamento do autor, o consumo vincula-se à satisfação de necessidades. Consumir é o ato de satisfazer necessidades. Pelo só fato da existência do homem, decorrem necessidades inderrogáveis, tais como o ato de comer ou respirar, que pertencem ao grupo das necessidades naturais. São sempre essenciais. Decorrem as necessidades do meio em que o homem se insere, dos desejos tidos como imprescindíveis, sem as quais ele não vive plenamente, tais como os vícios de fumar ou de se vestir, porque é costume enraizado na sociedade. Correspondem às chamadas necessidades artificiais, mas também essenciais. São necessidades supérfluas aquelas artificiais que podem ser dispensadas, e o ser humano, mesmo assim, viverá normalmente, como a de adquirir determinado bem que venha a lhe proporcionar um conforto desnecessário, como, por exemplo, adquirir um bem novíssimo, em detrimento de outro já existente que exerce a mesma função. As necessidades de consumo são inerentes ao ser, e fazem parte indissociável do cotidiano, que integram os atos da vida, que precedem o nascimento, alcançando o pós-morte.

Apesar de eventuais desvios no exercício do *marketing* é bem verdade que ele exerce importante função social, notadamente por constituir importante fator de impulso ao mercado. Assim é que pode servir como fator definidor de preços, desde que inserido numa justa concorrência, bem como apresentar novos produtos e serviços que por vezes são úteis aos consumidores, elevando a qualidade de vida, pelo aperfeiçoamento da tecnologia que, compulsoriamente, é exigida, dado o grau de aprimoramento do mercado. Além do que, por ser atividade econômica, gera empregos diretos e indiretos.

3. DOS INSTRUMENTOS E FORMAS DO EXERCÍCIO DO *MARKETING* (*E-COMMERCE*)

Com o estado da "sociedade de massas" resultante, evidentemente, da revolução industrial, a necessidade de colocação rápida e intensa de produtos e serviços que aparecem no mercado, as técnicas de venda evoluíram para instrumentos eficientes, tais como a tecnologia da informática, que se utiliza de meios de conhecimento (a era do conhecimento) que viabilizam a concretização daquelas demandas, a que eficientemente se insere a chamada "mídia".

Segundo a tabela de identificação da mídia de Karls Elling[6], ela se classifica em mídia direta pessoal (vendedores, telefonistas, relações públicas); direta impessoal (mala direta, material impresso, brindes, catálogos, embalagens); indireta pessoal ("boca a boca", humanização[7]); e indireta impessoal (mídia impressa, mídia eletrônica, *outdoor*, trânsito). Essa classificação bem representa a evolução das técnicas de venda, conforme as necessidades modernas.

Avulta na modernidade a utilização, nas mais diversas atividades econômicas, da informática, em especial pela forma dinâmica e rápida de comunicação e da facilitação do comércio. Dentre os diversos instrumentos, releva o da *internet* que derruba barreiras e divisas, proporcionando um espraiar de conhecimento sobre os diversos produtos e serviços à disposição[8]. Assim que o chamado *e-commerce* tem

---

[6] SANTOS, Fernando Gherardini. "Direito do marketing: uma abordagem jurídica do marketing empresarial". Editora Revista dos Tribunais, São Paulo, 2000, p. 35.

[7] Humanização representa a associação de um produto a uma determinada pessoa, em especial famosa. Cita SANTOS, Fernando Gherardini, ob. cit., p. 35, nota 50, o caso do tênis "Nike" ao atleta Michael Jordan.

[8] A WEBB negócios *on line* em sua cartilha "Webb Fácil 2", p. 5, refere que os efeitos da internet: **interatividade, onipresença e velocidade** proporcionam vantagens competitivas para as empresas. Apresentam a internet como o meio mais eficaz de comunicação, mostrando que ela levou 04 anos apenas para atingir 50 milhões de usuários no mundo, enquanto que o rádio levou 38 anos, o computador 16 anos, a televisão 13 anos e o celular 09 anos.

sido um dos responsáveis pelo fenômeno denominado “globalização”, já que as dificuldades de comunicação nas práticas comerciais restaram superadas.

É certo que “O crescimento da rede, em nível global, iniciou-se por volta de 1995 e, desde então, segue em contínuo e vertiginoso crescimento. Os dados estatísticos, veiculados nos vários setores da mídia, expressam a progressiva representatividade da internet para o comércio mundial (*e-commerce*). Na era da globalização, profetiza-se como sendo, a *World Wide Web*, a ferramenta do futuro. Destarte, as empresas de todos os setores da economia investem maciçamente na divulgação de seus produtos e serviços e na comercialização dos mesmos através da rede mundial de computadores[9]”.

4. DOS BANCOS DE DADOS DE CONSUMO COMO MEIOS DE DIFUSÃO DO CRÉDITO

Evidentemente que a atividade comercial só se viabiliza se os efeitos da publicidade, em suas diversas formas, se concretizarem. E isso ocorre por intermédio da circulação de riquezas, em que a moeda sempre representou o elemento básico. Todavia, com a intensificação das relações comerciais, outro fator tem gerado o incremento do mercado, como conseqüência da economia massificada, qual seja o “crédito”. Se outrora as relações de compra e venda se davam de forma direta, em que o eventual crédito propiciado era favorecido pelo conhecimento pessoal do fornecedor e de seus hábitos de consumo e poder aquisitivo, hoje isso se tornou impossível. Assim é que surgiram os chamados bancos de dados ou cadastros de consumo (genericamente, arquivos de consumo) onde os comerciantes (os fornecedores) dispõem de organizações de listas de informações acerca do comportamento dos consumidores no mercado, que servem de parâmetros para a concessão da venda a prazo, ou o popularmente chamado “fiado”, onde o crédito representa a confiança de que não haverá inadimplência da obrigação.

As associações comerciais organizaram os chamados serviços de proteção ao crédito (SPCs, ou SEPROCs) ou os bancos a SERASA (Centralização de Serviços dos Bancos S/A), dentre outros, como forma de superar o anonimato do consumidor, e concretizar as transações mediante a outorga do crédito.

---

[9] SOUZA, Marcos Antônio Cardoso de, “A legislação e a internet”, *in* **www.direitocriminal.com.br**, 17.02.2001.

Outros, contendo dados objetivos do consumidor, tais como as listas de pessoas que se habilitam à aquisição de serviços públicos, a exemplo do fornecedor de água, energia elétrica ou telefonia, por vezes podem, tal qual os do próprio comércio, proporcionar que tais dados sejam repassados a interessados diversos, com a finalidade do *marketing*, ou seja, de envio de malas diretas por intermédio dos correios convencionais, ou agora por meio dos correios eletrônicos.

5. DAS TÉCNICAS DE DIFUSÃO DE ENDEREÇOS ELETRÔNICOS

Os bancos de dados ou cadastros de consumo se constituem em repositórios de informações acerca de potenciais adquirentes de produtos ou utentes de serviços, os quais são úteis para os que pretendem exercer as atividades de incremento do comércio, no sentido de fazer chegar ao eventual consumidor a oferta e até mesmo a proposta de contratação.

Tradicionalmente, as listas de nomes e endereços dos potenciais consumidores eram repassadas em forma de listas impressas, etiquetas já também impressas ou, quando muito, já na era da telemática, de fornecimento de disquetes para cópia em programas de computador. Nem tanto havia disseminação dessas malas diretas, devido à razoável dificuldade material de remessa pelo sistema tradicional, e com a facilidade encontrada na mídia eletrônica, o *webmarketing* colocou-se como a forma viável de estimulação do consumo[10]. Para isso, repositórios de dados passaram a representar uma forma de comércio, pelo qual seus detentores comercializam essas listas de nomes e endereços, auferindo lucros, pois a venda desses bancos de dados representa um ganho significativo, já que dispõem normalmente de um número elevado de informações.

Segundo matéria do jornal Estadão[11], o custo desses bancos de dados de *e-mails* é relativamente barato, transcrevendo conteúdo de uma dessas ofertas, como exemplo: "1MILHÃO DE E-MAILS - PESSOAS FÍSICAS BRASILEIRAS - R$ 150. 2 MILHÕES DE E-MAILS - PESSOAS FÍSICAS BRASILEIRAS - R$ 250. 200 MIL E-MAILS - PESSOAS

---

[10] EMBRATEL. **In: www.embratel.com.br**, com acesso em 08.08.2001. Segundo estudo "e-Mail", informa a embratel que "Como na *Internet* não se paga nada por cada mensagem enviada, só se paga mesmo pelo tempo que se fica conectado, basta algum esforço para se conseguir enviar uma mala-direta pela *Internet*, com baixíssimo custo se comparadas às enviadas por correio tradicional (não há o custo de impressão, envelopamento e de envio pelo correio e, na verdade, o custo incremental de se enviar uma mensagem para mais uma pessoa, na *Internet*, é essencialmente zero)".

[11] O ESTADO DE SÃO PAULO. ***In* www.estadão.com.br**, de 18/01/2001.

JURÍDICAS BRASILEIRAS - R$ 150. 2.200.000 E-MAILS - PESSOAS FÍSICAS + PESSOAS JURÍDICAS - R$ 300 - PROMOÇÃO!!! Telefone: 0 ## 11 - 3203-1717".

Ou, então, este[12]: "A Promo Web vem por intermédio desta, colocar a sua disposição um cadastro único para você que tem necessidade de divulgar o seu negócio ou web site a nível brasileiro ou muncial: são mais de 17.000.000 (Dezessete Milhões) de e-mails, sendo 6.000.000 brasileiros e 11.000.000 internacionais, tudo isto pelo valor de R$ 400,00. Não perca mais tempo faça o seu pedido ainda hoje e faça bons negócios!

Mais este[13]: "HIPERMAILING. Envie mais de 2 milhões de mensagens pela Internet para divulgar seu produto, de uma maneira simples e rápida. Ligue e ganhe gratuitamente um software freeware que envia 20 mil mensagens por hora! Oferecemos total suporte técnico e podemos instruí-lo com dicas para não incomodar os provedores. SUPER PROMOÇÃO. + de 2 milhões de e-mails de pessoas físicas brasileiras, MAIS 120 MIL E-MAILS de pessoas jurídicas brasileiras .... R$ 100,00".

Como o correio eletrônico é mais barato e de acesso fácil, os endereços virtuais (*e-mails*) passaram a ser colecionados e depositados em bancos de dados também eletrônicos, ou mesmo em CDs ROOMs e ofertados a custos razoavelmente baixos, de forma que o interessado, de posse desses dados, tem importante instrumento de difusão direta, pela via eletrônica, vislumbrando um horizonte largo na comercialização de seus produtos ou serviços.

6. DA FORMA DE ARRECADAÇÃO DE NOMES E ENDEREÇOS RESIDENCIAIS E ELETRÔNICOS. DO *COOKIE.*

É sabido que os bancos de dados podem ser formados por cadastro do próprio consumidor, que fornece voluntariamente os seus dados, visando adquirir um produto ou serviço, ou por determinação do fornecedor interessado nessas informações, ou, ainda, por decisão de um próprio banco de dados.

---

[12] E-mail enviado pela ***promoweb10@yahoo.com*** para o Centro de Apoio Operacional das Promotorias de Justiça de Defesa do Consumidor de Curitiba (caopcon@pr.gov.br), em 06/08/2001.

[13] E-mail enviado pela "*Informativo*"<***MAILER-DAEMON@pr.gov.br***.para o Centro de Apoio Operacional das Promotorias de Justiça de Defesa do Consumidor de Curitiba (caopcon@pr.gov.br), em 07/08/2001.

Fora da *web*, ocorre normalmente a formação quando o consumidor comparece numa loja e preenche uma "ficha cadastral" para financiar uma determinada compra, ou quando o comerciante envia uma informação de inadimplência a um banco de dados de consumo, como o SPC das Associações Comerciais, por exemplo, ou quando um banco de dados resolve formar uma lista de dados de endereços e nomes para uso próprio ou mesmo para repasse a terceiros.

No caso da comercialização de listas de *e-mails*, o mesmo ocorre quando o usuário da *internet* ou o internauta acessa uma página da rede, ou seja, um determinado *site*, e pode ser convidado a fornecer seus dados, voluntariamente, preenchendo espaços próprios, a fim de, futuramente, receber mensagens ou informações. Neste caso, há a deliberada disponibilização desses dados pelo consumidor.

Mas, utilizando-se de recursos da informática, os titulares de domínios[14] na *internet*, ou seja, de *sites*, no momento em que são acessados, implantam um programa (*software*) na memória do computador do usuário, que terá funções de captação de informações e remessa para depósito no banco de dados do *site*, com o objetivo de traçar o perfil desse usuário, no sentido de identificar as suas preferências e práticas comuns no comércio. Esse programa tem a denominação de ***cookie*** e se configura num "espião" dentro da memória do computador, ocupando espaços, o qual não foi permitido ou solicitado. Representa uma apropriação indevida.

Muitas vezes sem que o usuário saiba, tal programa é instalado e passa a exercer uma função comercial, pois informações individuais, suas características e o seu endereço eletrônico ou *e-mail* passam a integrar um banco de dados. Ou como relata Sabbatini[15], "Depois de um certo tempo, esse perfil é bastante sofisticado e completo, e pode ser usado para muitas coisas: ele pode ser vendido, por exemplo, para empresas que buscam informações sobre o comportamento de usuários, tais como as coisas que eles mais compram, ou os sites que mais visitam, ou as informações que mais procuram". Tais informações podem servir para que o proprietário do *site* passe a remeter publicidades ou propagandas ou ofertas de determinados produtos que são do agrado e da preferência daquele usuário, até de forma personalizada. A essa mala direta eletrônica se denomina na rede de *spam.*

---

[14] CORRÊA, Gustavo Testa. "*Aspectos Jurídicos da Internet*". Editora Saraiva, SP, 2000, pp. 10-14. Segundo o autor, o "domínio" é a identificação do *site* ou a página da WWW (World Wide Web) que foi registrado no Comitê Gestor *Internet* do Brasil (Res. 1, de 15/4/1998).

[15] SABBATINI, Renato. "Privacidade e comércio eletrônico". **In: http://www.epub.org.br/correio/cp000310.html,** com acesso em 08.08.2001.

Veja-se como exemplo, o caso citado, ainda, por Renato Sabbatini[16], em "que o usuário costuma visitar artigos sobre tratamento de asma, a próxima vez que ele entrar em um desses *sites*, irá visualizar um anúncio de um novo medicamento para asma, provocando, então (segundo a teoria), um maior desejo de clicar nesse anúncio".

Cita, inclusive, que alguns programas o fazem personalizadamente, pois oferecem produtos ou serviços que são do desejo daquele cliente (consumidor). Há até outros que criam *banners*[17], ou seja, figuras na sua página eletrônica, coloridas, atraentes, oscilativas, oferecendo diretamente o produto, às vezes de forma destacada no canto da tela ou da página.

Interessante, a respeito, o artigo de Roberto Pompeu de Toledo[18] na Revista Veja, onde ele descreve exatamente a conduta do "Tratamento Personalizado" de um modo geral, como forma de quebrar o gelo, em que pessoas desconhecidas se dirigem a outras pelo nome, às vezes referindo-se a dados particulares, como se fossem íntimas e suas velhas conhecidas. Inclusive, narra que essa prática é forte na propaganda comercial, onde o consumidor pode se sentir lisonjeado com tal tratamento e acaba cedendo às investidas e comprando o produto ou serviço. Refere que outro meio utilizado de forma mais agressiva (não fala do endereço eletrônico, ainda) é o telefônico, onde diz haver "intrusão da intimidade das pessoas", perguntando: "E se a pessoa estiver trabalhando? E se estiver em pleno ato amoroso? Doente? Com um parente morrendo no quarto ao lado? Mesmo que não esteja em nenhuma dessas situações, que contrato social, que ética autoriza que se venha a perturbar-lhe a intimidade dessa forma?". Termina referindo que pode significar a técnica do "tratamento personalizado" uma reação ao anonimato da massificação, mas também pode representar o "massacre" da pessoa.

Pois bem, há outros que vão depositando os endereços eletrônicos dos usuários de computadores, quer sejam acessados por meio de *cookies* ou mesmo por autorização dos usuários (às vezes sem conhecer qual o uso dos seus dados), e formam listas ou ***mailing lists*** com finalidade de repassar aos fornecedores no

---

[16] SABBATINI, Renato. Idem.

[17] A definição de ***banner*** segundo se extrai do *site* **http://members. nbci.com** é a seguinte: "Banda Ilustrada, imagem gráfica usada para veicular anúncios em home pages, normalmente são clicáveis fazendo link com o site do anunciante". Ou, segundo o vocabulário no **www.amem.org.br/vocab/** é simplesmente: "**Banner** - Faixa publicitária na Web".

[18] TOLEDO, Roberto Pompeu de. "Tratamento personalizado, um perigo destes tempos. ***Veja,*** São Paulo: Abril, n. 18, p. 166, 05 maio de 1999.

mercado de consumo, para envio das referidas malas diretas, quando não se propõem eles próprios, utilizando-se desses dados, prestar serviços de envio de correspondências comerciais (malas diretas ou *spams*), na perspectiva do incremento do consumo de bens e serviços.

As listas de endereços eletrônicos proporcionam um volume inimaginável de malas diretas, na ordem de 25 bilhões de dólares ao ano nos EUA, conforme os dados trazidos no seu importante artigo, por Demócrito Reinaldo Filho[19]. Refere que as empresas que fazem intermediação de *mailing lists*, denominadas de *list-brokers* podem vender ou alugar as listas, oferecendo entre 60 a 125 dólares para cada mil nomes que aluguem. E o volume é tal que exemplifica: "Sob o título de "mailing lists", as páginas amarelas do Boston Globe incluem mais de 40 companhias que oferecem acesso a quase onze mil diferentes listas, cobrindo 100 milhões de consumidores"[20].

7. DAS MALAS DIRETAS ELETRÔNICAS INDESEJÁVEIS OU NÃO-SOLICITADAS (*SPAMS*)

A título de mala direta via *e-mail* os fornecedores ou titulares desses banco de dados ou *mailing lists,* passam a remeter, em massa, milhares ou milhões de propagandas comerciais que ao chegarem ao destinatário entopem o seu endereço eletrônico ou *e-mail* de forma até a causar-lhe problemas técnicos, além de lhe proporcionar importante dispêndio de tempo para examinar tais mensagens, a fim de selecionar aquilo que é proveitoso e o que não é, fazendo com que o seu computador deixe de lhe ser útil.

Essa desmedida e desregrada remessa de *spam*[21] (tido como lixo eletrônico) tem sido objeto de preocupação dos usuários, consumidores de produtos e serviços, pois nem sempre o *spam* se constitui num benefício. Às vezes, além das publicidades

---

[19] REINALDO FILHO, DEMÓCRITO. "O comércio de "mailing lists" e a privacidade do consumidor". **In: www.estacio.com.br**., Boston, 14.08.99.

[20] REINALDO FILHO, DEMÓCRITO. Idem.

[21] RIPARDO, Sérgio. "Monty Python difundiu a palavra spam; veja origem do termo". **In: www.uol.com.br/folha//dinheiro/ult9lu20570.shl**, do Jornal Folha de São Paulo, de 30/04/2001. Segundo a matéria, o termo SPAM resultou de uma das produções do grupo humorístico Monty Python, que para impedir a comunicação em um bar, repetem irritantemente o termo "Spam, Spam, Spam". Como alguém se irritou com a repetição de correspondências comerciais em seu e-mail, associou o termo "Spam" ao fato e o fenômeno comercial passou a se chamar assim. Outra versão, extraída da Webopedia, é o de que o termo associa-se ao nome da carne de lata, "com o argumento de que spam é um tipo de coisa que ninguém pede e ninguém engole".

comerciais, são oferecidas correntes de riqueza, remessa de piadas, palavras de baixo calão, que só têm o objetivo de emulação[22].

E tal atividade é conseqüência dessa descompromissada comercialização de *mailing lists* desautorizadas, que acaba causando essa ordem de transtornos.

Devido a isso, no seio da informática, os *cookies* e os *spams* têm sido objeto de grande discussão, envolvendo, como não poderia deixar de ser, o meio jurídico, objetivando vislumbrar as regulamentações aplicáveis, no sentido de reprimir tais condutas. E aí se se depara com uma certa ausência de legislações específicas. Mas o poder legiferante, mesmo assim, tem se manifestado, já havendo uma série de leis que materializam certa proteção, quando não específica, de forma genérica ao uso da informática. Uma gama de projetos de lei que ensaiam atender a essas questões, embora tais providências, se comparadas às de países onde a telemática está mais avançada, como os EUA, as medidas de cá vêm na rabeira das de lá[23].

8. DA APLICABILIDADE DO CÓDIGO DE DEFESA DO CONSUMIDOR NO *WEBMARKETING*

É sabido que o sistema de tutela do consumidor se aplica quando há uma relação de consumo[24], decorrente de uma relação jurídica entre um fornecedor de um lado e um consumidor de outro. A prática comercial ou contratual, no contexto de uma relação de consumo, está sob a égide do sistema de proteção ao consumidor, cuja principiologia se concretiza no seio da Lei 8.078/90, o Código de Defesa do Consumidor, e se espraia a todas as demais normatizações de consumo extravagantes. Dentre os princípios, o da especialidade, também em decorrência da característica de "ordem pública e interesse social" declinado no artigo 1º do Código. Pela especialidade, a tutela do consumidor se aplica de forma obrigatória, mesmo quando não invocada por qualquer interessado.

---

[22] O ESTADO DE SÃO PAULO. "Piadas e Correntes irritam usuários". **In: www.estadão.com.br**, de 26/03/2001. A matéria refere as diversas formas de um usuário ser incomodado com mensagens inúteis e até ofensivas, além dos *spammers* que provocam irritação.

[23] Veja o *site http://www.cyberlaws.com.br/legis/* que traz informações da legislação aplicável direta ou indiretamente à informática.

[24] A conceituação aprovada pelo Grupo Mercado Comum do Mercosul, no MERCOSUL/GMC/RES 123/96, de "relação de consumo" no Anexo, ìtem III, é a seguinte: "Relação de Consumo é o vínculo que se estabelece entre o fornecedor que, a título oneroso, fornece um produto ou presta um serviço e quem o adquire ou utiliza como destinatário final. Equipara-se a esta o fornecimento de produtos e a prestação de serviços a título gratuito, quando se realizem em funções de uma eventual relação de consumo". **In: Revista de Direito do Consumidor n. 23-24,** julho/dezembro 1997, Ed. RT, pp. 512/513.

Dessa forma, em quaisquer meios de comunicação em que a prática consumerista se apresente, quer direta ou indiretamente, estará ele sob o manto do Código de Defesa do Consumidor. É por isso que as normatizações dessa estirpe não podem revogar ou derrogar o princípio específico de "defesa do consumidor", o qual tem foro de constitucionalidade (v. artigo 5.º, XXXII e 170, V da Constituição Federal).

Se relevam de importância os meios modernos e atuais de comunicação, no exercício do *marketing*, em especial aquele exercido pelo *webmarketing*, como já salientado, tais relações devem observar e cumprir os requisitos de quaisquer práticas nas relações de consumo consideradas tradicionais, e que estão previstas no CDC. Assim, mesmo que legislações específicas existam ou que venham a se estabelecer, de caráter genérico na utilização da informática, elas não derrogarão os princípios específicos que ensejam direitos básicos dos consumidores (vejam-se os artigos 4.º e 6.º do CDC).

Bem retrata essa circunstância Angela Bittencourt Brasil[25], membro do Ministério Público do R.J., quando refere que os contratos entre fornecedores e consumidores levados a efeito "fora do estabelecimento" comercial proporcionam a possibilidade de desistência no prazo de 07 dias, conforme dispõe o artigo 49 do CDC. Diz ela: "As relações *on line* não se afastam do preceito acima estabelecido pelo Código do Consumidor, posto que o contrato, por sua característica de livre forma de contratar, é perfeitamente adaptável à aplicação analógica das normas ora existentes às peculiaridades apresentadas pelos contratos eletrônicos".

9. DOS REQUISITOS LEGAIS DOS BANCOS DE DADOS OU ARQUIVOS PESSOAIS E DE CONSUMO

Considerando que devido à necessidade de tutela do consumidor, os Bancos de Dados mereceram pelo Código de Defesa do Consumidor regulamentação especial no Capítulo das Práticas Comerciais, há de se fazer análise dos requisitos para registro de endereços e nomes em tais bancos de dados ou arquivos pessoais e de consumo.

---

[25] BRASIL, Angela Bittencourt. "Aplicação do Código de Defesa do Consumidor na *Internet*". **In: www.ibdi.hpg.com.br/artigos/ /angela_brasil/001.html**, com acesso em 08.08.2001. Conclui a autora que o direito de desistência imotivada feita por *e-mail* passa a contar do momento em que há a "descarga do arquivo" no computador "daquele a quem é feita a desistência, isto é, quando o provedor puder comprovar que o e-mail foi enviado e recebido".

De três formas podem ser abertos os arquivos[26]: a) *por solicitação do próprio consumidor*; b) *por determinação do fornecedor interessado* na realização do negócio de consumo; e c) *por decisão espontânea de um banco de dados*.

O Código de Defesa do Consumidor regulou, no artigo 43 e parágrafos, os direitos básicos dos consumidores, nos bancos de dados e cadastros de consumidores, destacando-se, dentre eles, os direitos de comunicação, acesso e correção de dados.

Pelo direito de informação ou comunicação por escrito, o consumidor deve conhecer, em prazo razoável (não fixado pelo CDC), que deve ser de, no mínimo, 05 dias, por analogia ao artigo 43, § 3º, previamente à incorporação ao arquivo da entidade, de todos os dados registrados[27].

O dispositivo do artigo 43, § 2º do CDC dispõe que "A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele". A abertura, por conseqüência, não poderá prescindir da comunicação por escrito. Infere-se, outrossim, que deverá ser prévia, porque a *mens legis* é no sentido de prevenir eventuais ofensas a direitos do consumidor, cujo titular poderá evitar o registro indevido.

É da doutrina especializada o ensinamento no mesmo sentido, tal qual Antônio Herman V. Benjamin[28], que ensina que "A comunicação deve ser feita antes da colocação da informação no domínio público. É preliminar a tal. Visando a prevenir futuros danos ao consumidor, é de todo recomendável "que a comunicação seja realizada antes mesmo da inscrição do consumidor no cadastro de inadimplentes, a fim de evitar possíveis erros... Agindo assim, estará a empresa tomando as precauções para escapar de futura responsabilidade".

Já pelo direito de acesso, o consumidor tem direito de verificar todas as informações de consumo sobre ele registradas, quer estejam em arquivos abertos pelo próprio fornecedor, quer seja por um banco de dados. Inclusive sobre as fontes dos arquivos, seja com a finalidade de melhor investigação no caso de contestação da informação, quer seja para o exercício de reparação por perdas e danos. Finalmente, pelo direito de retificação, havendo incorreção nos dados, deverá haver retificação

---

[26] BENJAMIN, Antônio Herman de Vasconcellos e. "Código Brasileiro de Defesa do Consumidor Comentado pelos Autores do Anteprojeto". Ed. Forense Universitária, 6ª ed., RJ, 1999, pp. 393/394.

[27] A comunicação prévia foi ampliada de 05 para 10 dias, no SPC da Associação Comercial do Paraná, e de forma prévia ao registro dos dados, em decorrência de Compromisso de Ajustamento de Conduta assinado com o Ministério Público do Estado do Paraná em 2001, em Curitiba.

[28] BENJAMIN, Antônio Herman Vasconcelos. "Código de Defesa do Consumidor...", p. 397.

imediata e comunicação em 05 (cinco) dias úteis aos destinatários das informações incorretas. O arquivista deverá fazer a prova positiva da veracidade dos dados, quando, então fenece o direito de retificação, logo após tenha os dados que confirme a incorreção, devendo suspender qualquer atendimento de pedido de informação, ante a contestação do consumidor, ou enquanto dure o processo de verificação.

Os bancos de dados são, pelo art. 43, § 4.º do CDC, considerados de caráter público, com a finalidade precípua da utilização do *habeas data*, regulado pela Lei 9.507, de 12 de novembro de 1997, que possui base Constitucional (art. 5º, LXXII da C.F.).

10. AS *MAILING LISTS* COMO BANCOS DE DADOS PESSOAIS E DE CONSUMO

As *mailing lists,* como já informado anteriormente, constituem-se em organização e registro de dados de endereços eletrônicos (*e-mails*), podendo conter outros dados, mesmo pessoais, referentes aos consumidores, com o objetivo do exercício do *marketing*, na modalidade de venda por intermédio de comunicação direta pela via do correio eletrônico.

Como estão inseridas numa relação de consumo, em especial na prática de ofertas publicitárias, todos os princípios norteadores se aplicam às *mailing lists*, conforme regulados no Código de Defesa do Consumidor.

Segundo definição de Bertram Antônio Stürmer[29], "Tendo em vista o previsto no art. 29 do CDC, de que as normas sobre bancos de dados se aplicam a todas as pessoas determináveis ou não, expostas a serem cadastradas, que as equipara como consumidores e, também, em razão de que o art. 3.º qualifica como fornecedor toda a pessoa física ou jurídica, pública ou privada, inclusive entes despersonalizados e, ainda, no art. 2.º inclui, ao lado da pessoa física a pessoa jurídica como consumidora quando adquire ou utiliza produto ou serviço como destinatário final, podemos concluir que bancos de dados, para fins do Código do Consumidor, é toda reunião de dados pessoais ou de consumo, gerais ou específicos sobre débitos, feita por pessoa física ou jurídica, privada ou pública, sob a forma de fichas, registros ou cadastros, por processo manual, mecânico ou

[29] STÜRMER, Bertram Antônio. "Banco de Dados e "Habeas Data" no Código do Consumidor". **In:** Revista de Direito do Consumidor, Ed. RT, São Paulo, 1992, Vol. I, p. 62.

eletrônico, para uso próprio ou fornecimento a terceiros, independentemente da finalidade do dado ou informação e está, portanto, sujeito às regras daquele Código."

Não se pode considerar, portanto, que as *mailing lists* organizadas e armazenadas em bancos de dados escapem ao crivo do direito do consumidor, já que, pelo artigo 29 do CDC, são consumidores equiparados quaisquer que "determináveis ou não", estejam "expostos às práticas comerciais ou contratuais".

É inegável que as pessoas titulares de *e-mails* tenham seus endereços eletrônicos expostos a terceiros, onerosa ou gratuitamente, e com o objetivo de que potenciais fornecedores estimulem práticas relacionadas ao consumo, quer pelo exercício da publicidade comercial de si (*marketing*), quer pelas contratações que resultem delas, seja por contratos eletrônicos mesmos (compra e venda pelo *e-mail*, por exemplo), quer por outras formas.

E os organizadores desses bancos são fornecedores no sentido real do texto do CDC, pois mesmo pessoas físicas ou "entes despersonalizados", o são, desde que exerçam atividades econômicas (produção, montagem, comercialização etc.) conforme o artigo 3.º *caput*, relacionado a produto "material ou imaterial" - artigo 3.º, § 1.º - ou serviço - artigo 3.º, § 2.º , todos do CDC.

Protegido que está o consumidor, há que o titular de banco de dados eletrônicos, para poder utilizá-lo, que proceder a prévia e necessária comunicação por escrito ou por *e-mail,* sob pena de tornar o arquivo de consumo ilegítimo.

Noticia-se que a *internet* "é um verdadeiro faroeste" conforme diz Sabbatini[30], de modo que dados privativos do usuário da rede são armazenados de forma que ele não saiba de que forma e nem onde, sendo alterados, vendidos, cedidos ou mesmo roubados constantemente. Relata que, nos EUA, a Federal Trade Commission (FTC), regulamentadora das atividades comerciais, apurou que apenas 8% dos *sites* de comércio eletrônico têm um "selo de privacidade". Acrescentou: "A FTC deseja que os *sites* tenham quatro normas básicas: aviso, escolha, acesso e segurança. Em outras palavras, o *site* deve avisar claramente ao usuário qual informação está sendo coletada sobre ele, e como é usada; dar opção para que ele escolha como a informação será usada, dar acesso às informações já coletadas sobre ele, para fins de verificação, correção e apagamento, e tomar as medidas necessárias para proteger os dados de acesso por terceiros".

---

[30] SABBATINI, Renato. "Privacidade e comércio eletrônico". **In http://www.epub.org.br/correio/cp000310.html** com acesso em 08.08.2001.

Em resumo, aquilo que o CDC já prevê como necessária para a regularidade dos Arquivos de Consumo ou Bancos de Dados, é a devida comunicação prévia, para que se legitime eventual comercialização dessas *mailing lists*.

11. DA VIOLAÇÃO DA PRIVACIDADE E DAS COMUNICAÇÕES EM GERAL

A privacidade e o sigilo das comunicações telegráficas, telefônicas, *de dados* e das correspondências são invioláveis, exceto por determinação judicial, conforme o artigo 5.º, incisos X e XII da Constituição Federal.

A ofensa a tais direitos implica em sanções de naturezas diversas, tais como administrativa, civil e penal.

A transferência de informações desautorizadas por parte de detentores de dados listados e organizados em cadastros ofende os preceitos constitucionais, erigidos à categoria de "Direitos e Garantias Fundamentais" do cidadão.

Para efeito de verificação de violações ao direito de sigilo nas operações financeiras e para finalidades de investigação de ilícitos, mediante decreto judicial, há expressa regulamentação em lei, qual seja, a Lei Complementar 105 e Decreto 3724, ambos de 10 de janeiro de 2001, onde se apresenta a necessidade de estrita confidência dos dados investigados, com absoluta restrição às partes envolvidas.

Se a rigorosa regulamentação legal estabelece rígidos sistemas de controle, com finalidades de apuração de fatos graves, notadamente ilícitos criminais, isto significa que uma invasão de dados pessoais, por qualquer forma, também representa violação da privacidade. É certo que a divulgação em massa de dados (milhões de endereços eletrônicos) poderá ensejar uma série de conseqüências pelo mau uso ou uso indevido, já que não há forma de controle eficiente, em especial pela agilidade do sistema informativo *on line.*

A legislação referida também visa impor controles aos órgãos legais investigativos, tais como a Polícia, o Ministério Público e as Comissões Parlamentares de Inquéritos.

Nesse contexto é que a OAB, por intermédio da Comissão Especial de Informática Jurídica - Seção de São Paulo , desenvolveu anteprojeto de lei cuidando, dentre outras coisas (documento eletrônico e assinatura digital), também de operações comerciais

no mundo virtual (*e-commerce*), dispondo no artigo 5.º: "O ofertante somente poderá solicitar do destinatário informações de caráter privado necessários à efetivação do negócio oferecido, devendo mantê-las em sigilo, salvo se prévia e expressamente autorizado a divulgá-las ou cedê-las ao respectivo titular". No mesmo projeto, art. 12, impõe a necessidade de ordem judicial para dar acesso aos dados, determinando o "segredo de justiça" ao procedimento[31]. No que se refere à autenticidade, integridade e validade jurídica de documentos em forma eletrônica, visando transações seguras no meio virtual, o Poder Executivo editou a MP 2200, de 28 de junho de 2001, já reeditada, em que instituiu a *Infra-Estrutura de Chaves Públicas Brasileira - ICP-BRASIL*, cujas normas já estavam estabelecidas no Decreto nº 3.587, de 05.09.2000.

Por sua vez, os projetos de lei n.º 84/99 e 1713/96, respectivamente dos deputados Luiz Piauhylino e Cassio Cunha Lima, que tratam de crimes cometidos na área de informática, estabelecem a necessidade de autorização prévia para a transmissão de dados pessoais, erigindo a violação do sistema à natureza de crime, conforme o comentário de Gustavo Testa Corrêa[32].

Portanto, a comunicação ou autorização prévia são necessárias já pela legislação de defesa do consumidor, bem como faz parte de diversos projetos de lei específicos acerca do comércio pelo meio eletrônico.

12. DA PRÁTICA COMERCIAL ABUSIVA

Se por um lado a instituição de *mailing lists* representa violação a preceito constitucional que assegura a inviolabilidade de dados privativos e pessoais, bem como do sigilo de correspondências e comunicações eletrônicas, tal prática perante o Código de Defesa do Consumidor configura forma de abusividade.

O artigo 39 do Código de Defesa do Consumidor estabelece rol exemplificativo de práticas comerciais abusivas que podem ensejar medidas repressivas administrativas, civis e penais. O rol é aberto, permitindo que novas práticas sejam incorporadas àquelas. Até porque faz parte da Política Nacional das Relações de Consumo a ser materializada pelo Sistema Nacional de Defesa do Consumidor (v. arts. 4.º e 105 e 106 do CDC) a

---

[31] BRUNO, Gilberto Marques. "O sigilo de dados e a privacidade *on line*. Anteprojeto de lei do comércio eletrônico". **In: www.jusnavegandi.com.br**, de fevereiro de 2001.

[32] CORRÊA, Gustavo Testa. "*Aspectos Jurídicos da Internet*". Editora Saraiva, SP, 2000, pp. 85 e seguintes.

edição periódica de rol de novas práticas comerciais ou contratuais abusivas no mercado, a cargo do DPDC (Departamento de Proteção e Defesa do Consumidor) vinculado à Secretaria de Direito Econômico do Ministério da Justiça. Assim é que quatro portarias do DPDC trazem o rol de diversas outras práticas consideradas abusivas no mercado.

Extrai-se das lições de Benjamin[33]: "Comumente há aí bem caracterizada prática abusiva, nos termos do art. 39, do CDC, que é norma aberta, do tipo cláusula geral. Sem falar na violação da garantia constitucional da privacidade. A abusividade é praticada de forma solidária, tendo, de um lado, o banco de dados que coleta as informações cadastrais e, do outro, a empresa que adquire uma 'mala direta' em particular".

A comercialização de quaisquer produtos ou a prestação de quaisquer serviços violam os princípios da boa-fé e eqüidade (v. artigos 39 e 51 do CDC), tais como o de listas eletrônicas desautorizadas, em especial quando têm objetivo de auferir lucro.

13. CONCLUSÕES

a) As listas de endereços eletrônicos (*mailing lists*) configuram bancos de dados pessoais e/ou de consumo que estão sob a égide do sistema de tutela do consumidor.

b)A transmissão onerosa ou gratuita das *mailing lists* só poderá ocorrer quando o lançamento dos dados se der mediante autorização do consumidor ou prévia comunicação, de acordo com o artigo 43 e §§ 1.º e 2.º do CDC.

c) O estabelecimento de *mailing lists* mediante técnicas de informática não autorizadas (*cookies*) configura invasão de privacidade, ofendendo preceito constitucional.

d) A prática do *webmarketing*, ou envio de malas diretas eletrônicas (*spams*) decorrente das *mailing lists* não-autorizadas, configura prática comercial abusiva, na forma do artigo 39 do Código de Defesa do Consumidor.

Ciro Expedito Scheraiber

promotor de Justiça do Consumidor em Curitiba – Paraná

[33] BENJAMIN, Antônio Herman de Vasconcellos e. "Código Brasileiro de Defesa do Consumidor Comentado pelos Autores do Anteprojeto". Ed. Forense Universitária, 6ª ed., RJ, 1999, p. 356.

CONDUTAS ILÍCITAS NA SOCIEDADE DIGITAL

Marco Antonio Zanellato

CONDUTAS ILÍCITAS NA SOCIEDADE DIGITAL

Marco Antonio Zanellato

1. INTRODUÇÃO

1.1. Internet: da passagem do mundo analógico (dos átomos) para o digital (dos *bits*)

A humanidade, como muito bem sublinhado por TERCEIRO, vem "medindo seu progresso historicamente, em termos de tecnologia, com o resultado de que cada era tem passado mais rapidamente do que as anteriores"[1]. A partir da revolução industrial, que se estendeu desde o princípio do século XVIII até o final do século XIX, surgiram três eras, verdadeiramente revolucionárias em termos de tecnologia, uma mais curta do que a outra, embora muito convulsivas: a *era eletrônica*, que durou quarenta anos (desde a Segunda Guerra Mundial até o início dos anos oitenta), em que surgiu e se massificou o PC (*Personal Computer*); a *era da informação* (do princípio dos anos oitenta até os primórdios dos noventa), em que os PCs, já integrados, inclusive no âmbito doméstico, começaram a interconectar-se em redes

[1] J. B. TERCEIRO. *Sociedad digital*, Madrid, 1996, p. 29.

da informação; por último, a em que estamos, a chamada *era digital*, caracterizada pela normalização de todo tipo de redes informáticas e pela aparição de uma nova sociedade, a digital, com uma *cyber* cultura, que, no dizer do filósofo francês PIERRE LEVY[2], "encarna a forma horizontal, simultânea, puramente espacial, da transmissão".

A propósito dessa nova revolução de natureza tecnológica por que estamos passando, muito interessantes revelam-se algumas observações de M. AURÉLIO GRECO[3] - certamente inspiradas em NEGROPONTE[4] -, pelo que nos permitimos aqui reproduzi-las:

> "A atual revolução tecnológica pode ser resumida no reconhecimento de que estamos passando "dos átomos para os *bits*"[5]. O que isso significa?
>
> Os átomos serviam de meio físico para transporte e comunicação de mensagens no sentido de que 'contrato' tanto significava o vínculo jurídico como o documento redigido em papel (ou pergaminho) revestido de certas formalidades. Os átomos do papel eram o meio físico para transmitir a mensagem 'jurídica' da criação das relações, obrigações etc.
>
> Uma nova civilização está em criação; nesta, o conceito relevante não é mais o de átomo, mas sim o de *bit*, o que traz profunda alteração na estrutura das relações e na relevância dos objetos, pois *a mensagem se desatrela do meio físico passando a ter vida própria* independente de estar superposta a átomos.
>
> O 'virtual' passa a ter valor próprio, independente do seu suporte físico, a mensagem ou a informação têm valor independente de um suporte em que se apóia ou de um meio para sua transmissão. Os interesses jurídicos e, conseqüentemente, os direitos e deveres daí decorrentes passam a ter como objeto a própria mensagem ou informação e não mais o meio em que se apresentam (não interessa o disquete, mas sim o *software* que nele se encontra). A mensagem em si passa a ter um valor próprio, independente dos átomos do seu meio físico.

---

[2] PIERRE LEVY. Sobre a cibercultura, em *Revista do Ocidente*, n.º 206, Madrid, 1998, p. 31.

[3] MARCO AURELIO GRECO. Transações eletrônicas. Aspectos jurídicos, in *Revista de Direito Bancário do Mercado de Capitais e da Arbitragem*, São Paulo: Ed. Revista dos Tribunais, v. 8, abr.-jun. de 2000, p. 65-69.

[4] NICHOLAS NEGROPONTE. *Vida digital*. 2ª ed. - Trad. de Sérgio Tellaroli, São Paulo: Companhia das Letras, 1999.

[5] Observe-se que o computador não guarda, na memória, letras, algarismos, imagens ou sons. Ele armazena apenas *bits.* O vocábulo *bit* corresponde à abreviação da expressão inglesa ***BI****nary digi****T*** (dígito binário). O termo *byte*, por sua vez, é uma unidade formada por oito *bits* (cf. ADAM OSBORNE. *An introduction to microcomputers*, California, Osborne/Mc Graw-Hill, 1980, *apud* MARCO AURELIO GRECO. Transações eletrônicas. Aspectos jurídicos, cit., p. 68, nota 8, e p. 69.

Esta é a grande mudança. O valor não está mais atrelado necessariamente às características físicas das coisas. As informações, mensagens, dados, instruções, *softwares* etc. adquiriram valor próprio, independente dos átomos de que é formado seu meio físico. Até mesmo objetos que originalmente tinham natureza física, passaram a ter feição virtual; é o caso das ações de sociedades anônimas que até certo tempo atrás eram apresentadas em papel, geralmente coloridas, numeradas, assinadas etc. e que hoje em dia foram substituídas pelas 'ações escriturais' que nada mais são do que um 'registro' (conjunto de *bits*) na memória de um computador.

Em suma, o *meio* deixou de ser o referencial único ou básico de valor. Os valores (econômicos, patrimoniais, financeiros etc.) passam a apoiar-se ou a ser dimensionados pelos *bits* que estão embutidos num determinado meio.

O valor dos *bits* não está neles mesmos, mas sim na *utilidade* que eles podem proporcionar a alguém. Quanto maior a utilidade que deles pode ser extraída, maior será o valor que terão. Ou seja, os *bits* trazem uma *utilidade* para o usuário, seja na facilidade de funcionamento de uma máquina, seja na velocidade de transmissão de dados, seja na facilidade de armazenamento ou segurança de informações, etc. Enfim, sempre uma utilidade.

Na medida em que se acrescenta uma utilidade, acrescenta-se um valor ao que antes existia. Daí dizer-se que o elemento chave num mundo informático é o conceito de 'valor adicionado'. Vale dizer, os bens informáticos não valem pelo que eles são, mas sim pelo valor que eles adicionam à vida de alguém, de uma empresa, do Poder Público, etc. Ou seja, o valor está atrelado à utilidade agregada, que se adiciona ao processo. Daí a noção 'valor adicionado'. Note-se que este conceito está ligado à *utilidade* fornecida e não ao seu preço, nem ao trabalho desenvolvido para realizar ou produzir o serviço.

A idéia de valor adicionado resulta nítida quando se imagina a linha telefônica que, originariamente, surgiu trazendo apenas a utilidade de viabilizar conversas entre pessoas. Hoje, à tal utilidade foram acrescidas outras, como a transmissão de dados, a conexão a computadores centrais para fins de *home-banking*, a transmissão de imagens via Internet, a transmissão de documentos escritos etc."

Na mesma direção é a lição de ESTHER MORÓN, ancorada na doutrina de NEGROPONTE, FERNÁNDEZ ESTEBAN e CASTAÑARES:

> "Para poder apreciar as vantagens e conseqüências de 'ser digital', deve aconselhar-se refletir sobre a diferença entre átomos e *bits*. Como já se afirmou, a maior parte da informação nos chega em forma de átomos: livros, periódicos, revistas. O mundo é feito de átomos. Um *bit* não tem cor, tamanho nem peso. É o DNA da informação. É tão-somente um número, cuja representação mais elementar é uma seqüência de zeros e uns. Os *bits* sempre foram o elemento básico da informação. Nos últimos vinte e cinco anos logrou-se digitalizar cada vez mais tipos de informação, auditiva e visual, por exemplo, reduzindo-os de igual maneira a números.
>
> Digitalizar significa converter em números o que se quer transmitir. A digitalização permite que distintos tipos de dados e de informação, como textos, voz e imagens possam converter-se em números, ser tratados do mesmo modo e transmitidos pelas mesmas linhas. O fenômeno multimídia ou hipermídia é o resultado da digitalização de todos os tipos de sinais.
>
> A digitalização da informação é um conceito chave para entender as novas tecnologias e sua generalização tem operado uma divisão radical entre o analógico e o digital. O mundo digital é o mundo da informação convertida em dígitos e o mundo analógico é o restante."

Essa nova dimensão de *cyberspace*, a *digitalidade*, "conduz a uma reinterpretação de nosso modo de entender a técnica, uma vez que nesse novo mundo o real pode converter-se em falso, o original, em cópia e o ser, em identidade virtual"[6]. No ciberespaço, "cada indivíduo é potencialmente um emissor e um receptor em um meio qualitativamente diferenciado, em que todos se comunicam com todos. Os internautas não se localizam principalmente por seu nome, posição social ou situação geográfica, mas a partir de centros de interesses. É um mundo virtual segregado pela comunicação"[7].

---

[6] ESTHER MORÓN LERMA, Internet y Derecho Penal: "hacking" y otras conductas ilícitas en la red, in *Revista de Derecho y Processo Penal*, Pamplona: Aranzadi Ed., n.º 1, 1999, p. 79.

[7] ESTHER MORÓN LERMA, *op. cit.*, p. 80. Esta autora cita a seguinte observação de RODOTÀ: "Non ci sono privilegi el comunicare, anche la piùricca delle strutture di tipo tradizionale, le televisioni dei 500 canali, non hanno le potenzialità di rottura dello schema gerarchico che abbiamo conosciuto, perché non tutti possono nello stesso tempo assumere il ruolo de produttori e consumatori delle informazioni" (*Libertà, opportunità, democrazia, informazione*, Conferência introdutória apresentada no *Congresso Internet e privacy. Quali regole?*, em Roma, maio de 1998).

1.2 Internet: origem

ESTHER MORÓN, baseada em informação sobre a origem da Internet, colhida em FERNÁNDEZ ESTEBAN[8] e TERCEIRO[9], explica que a Internet surge em torno da tecnologia militar norte-americana, em plena guerra fria, com o objetivo de estabelecer uma rede de telecomunicações o menos vulnerável possível a um ataque atômico soviético. Em meados dos anos sessenta, o Governo dos Estados Unidos promove, por meio da ARPA (*Advanced Research Projects Agency*), uma rede experimental, ARPANET, a fim de facilitar a comunicação entre investigadores situados em lugares longínquos, adotando uma configuração que garantisse seu funcionamento, mesmo quando se avariassem suas partes. O objetivo era criar uma rede ampla de computadores em que a informação pudesse ser transmitida de uns a outros através de vias distintas, por um caminho ou outro, de maneira que, se uma área fosse atacada em uma ação bélica, a informação chegaria intacta a seu destinatário. A chave desse sistema residia na inexistência de um centro nevrálgico que controlasse a rede, pois este seria um ponto vulnerável do sistema. Durante os anos setenta e oitenta, a ARPANET cresceu, incorporando serviços e unindo-se a outras redes que utilizavam a mesma linguagem, denominadas protocolo TCP/IP (*Transmition Control Protocol/Internet Protocol*). Este permite transmitir a informação por partes, dividindo cada mensagem em pequenos pacotes de dados. Em 1988, a *Net* (como se costuma designar a Internet) introduziu-se no ARPANET, que deixa de existir em 1990[10].

1.3 Internet: a rede das redes

O conceito de Internet revela-se, de certa forma, polissêmico. Com efeito, muitas são as definições de Internet encontradiças na literatura especializada[11]. Uma que

---

[8] M. L. FERNÁNDEZ ESTEBAN. *Nuevas tecnologias, Internet y derechos fundamentales*, Madrid, 1998, p. 24.

[9] J. B. TERCEIRO. *Sociedad digital*, cit., p. 91 *et seq.*

[10] *Op. cit.*, p. 95-96.

[11] ESTHER MORÓN LERMA afirma que "resulta inabarcavel toda a literatura que surgiu em torno da Internet" (Internet y Derecho Penal: "hacking" y otras conductas ilícitas em la red, in *Rev. de Derecho y Processo Penal*, cit., p. 95). À guisa de exemplificação, dentre muitos outros escritos, ver os seguintes: Vários autores. *Internet para todos.* Barcelona, 1996; CEBRIÁN. *La red.* Madrid, 1998; LÓPEZ. *Internet, la red con mayúsculas*. Sevilha, 1997; PARRERAS. *Internet y derecho*. Barcelona, 1998; Autores diversos. *L'Internet professionnel*, CNRS éditions, 1995; BAUCHE. *Tout savoir sur Internet*, Arléa, 1996; BENSOUSSAN. *Internet, aspects juridiques*, Hermès, Paris,1996; DUFOUR. *Internet*, PUF, 1996; PIETTE-COUDOL et BERTRAND. *Internet et la loi*, Dalloz, Paris, 1997; TORTELLO et LOINTIER. *Internet pour les juristes*, Dalloz, Paris, 1996; THEMENS. *Internet et la responsabilité* civile, Les éditions Yvon Blais Inc., Québec, 1998; SHAPIRO e VARIAN. *Information rules – A strategic guide to the network economy*, Harvard Business School Press, 1999; Autores vários. *Cyberfutures*, Zianddin, Sardar & Ravetz, 1996; LLOYD. *Information technology law*, Butterworths, 1993; REED. *Computer law*, Blackstone Press, 96; Autores vários. *Direito y Internet – Aspectos jurídicos relevantes* (coords. Newton De Lucca e Adalberto Simão), São Paulo: EDIPRO, 2000; LORENZETTI. Informática, cyberlaw, e-commerce, in *Direito & Internet – Aspectos jurídicos relevantes*, cit., p. 419-446; PAESANI. *Direito e Internet: liberdade de informação, privacidade e responsabilidade civil*, São Paulo, Atlas, 2000.

nos parece aceitável é a que considera a Internet uma cadeia mundial de redes de computadores públicos ou privados, ligados uns aos outros por equipamentos informáticos heterogêneos e que fornecem os mais variados serviços. Em sentido assemelhado, podem ser mencionadas as seguintes definições de Internet: "uma ampla reunião de redes de computadores que trocam informações por meio de uma seqüência de protocolos de redes chamada TCP/IP"[12]; e "uma cadeia de redes que convida à troca de diferentes tipos de dados e à prestação de serviços variados no mundo inteiro, a todas as pessoas equipadas de um computador munido de um *modem*"[13].

Em um computador de rede podem concentrar-se os principais arquivos. Tal computador é conhecido como "servidor" e os computadores que estão conectados ao servidor são seus "clientes". O servidor de rede pode conectar-se ao servidor de qualquer outra rede, formando-se, assim, redes de redes ou inter-redes. A rede que enlaça e interconecta um maior número de redes denomina-se *Internet*.

ESTHER MORÓN apresenta conceito semelhante aos antes referidos: "A Internet caracteriza-se por ser um meio universal de comunicação de baixo custo. É composta por um conjunto de redes interconectadas, que permitem a comunicação entre milhões de usuários de todo o mundo, gerando um imenso grupo de recursos de informação, em forma de imagens, textos, gráficos e sons"[14].

Hoje, os integrantes da "aldeia global"[15] comunicam-se navegando pelas *superautopistas*[16] da informação existentes no espaço virtual. As autopistas de informação, no dizer de ORTIZ CHAPARRO, "seriam meios de comunicação universal surpreendentemente baratos, porque seus integrantes principais, a informática e a comunicação, estão cada dia mais acessíveis. Porém, a navegação por elas, de maneira que se consiga obter o máximo de suas capacidades potenciais, requer um

---

[12] GILLES BAUCHE, cit. por CRISTINE RIEFA. *Le consommateur et l'Internet*. Tese apresentada à Universidade de Montpellier I e Perpignan, sob a orientação do Prof. Jean Calais-Auloy, 1997.

[13] PIERRE LAFFITTE. *La France et la société de l'information*, Rapport de l'office parlementaire d'Évaluation des Choix Scientifiques et Technologies, n.º 213 (335), du 7 févier 1997: http://cubitus.senat.fr/rap/o213-2_toc.html.

[14] ESTHER MORÓN LERMA. *Internet y Derecho Penal: "hacking" y otras conductas ilícitas en la red*, cit., p. 95.

[15] Expressão cunhada por MARSHALL MACLUHAN, em 1962, para aludir a uma comunidade cujos integrantes relacionavam-se entre si por intermédio dos meios de comunicação de massa.

[16] Referindo-se às autopistas de informação ou infopistas no *cyberspace* ou na comunidade virtual, ESTHER MORÓN assinala que foi AL GORE, ex-vice-presidente norte-americano, quem cunhou o termo *superautopista da informação*, no final da década de oitenta, concretamente em 1988.

aprendizado e uma prática. E, sobretudo, a destra utilização das ferramentas intermediárias, fundamentalmente o computador"[17].

É a Internet, de fato, uma *superautopista* (*superhighway, superautoroute*) da informação que "pode ser definida como um conjunto de computadores interconectados entre si através de redes[18]. Dita interconexão efetua-se mediante *hardware* e *software.* A comunicação entre vários computadores é possível com um *modem*, cuja função é converter os dados e transmiti-los por meio da linha telefônica"[19] (hoje, pode ser por ondas eletromagnéticas ou por cabos de fibras óticas; veja-se, por exemplo, o provedor *Ajato*).

Qualquer que seja a definição adotada, constata-se que três elementos caracterizam a Internet: (a) é uma cadeia de redes (*réseau de réseaux*); (b) em escala mundial; (c) cujos equipamentos informáticos expressam a mesma linguagem e utilizam as mesmas técnicas para fazer circular a informação.

A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, idéias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos. É um novo meio de consumo. Abre uma nova era para o consumidor. Permite, por meio de suas aplicações, notadamente a *World Wide Web* (*WWW ou W3*), consumir tanto informações quanto produtos e serviços. Gera uma clientela mundial, cria novos mercados.

A *Net* (como é comumente designada a Internet) propicia o chamado comércio eletrônico (*e-commerce*)[20]. Em sentido estrito, este pode ser definido como aquele que se limita à noção de transação *on-line*: uma troca comercial eletrônica implica uma compra, um consumo e/ou pagamento efetuado por meio de uma rede. Em sentido amplo, a noção de comércio eletrônico engloba todas as funções que integram

---

[17] F. ORTIZ CHAPARRO. Los impactos sociales de las autopistas de la información, em *Actualidade Informática Aranzadi*, n.º 17, 1995, p. 9, *apud* ESTHER MORÓN, "Internet y Derecho Penal ..., cit., p. 86, nota 163.

[18] A propósito, cumpre esclarecer que quando vários computadores se unem através de uma rede e estão no mesmo edifício (sem necessidade de usar telecomunicações), denomina-se *Intranet* a rede de área localizada; por outro lado, se para conectar os computadores é necessário empregar telecomunicações (a rede de telefone, por exemplo), denomina-se rede de área ampla (WAN – *Wide Area Net-work*).

[19] *Op. cit.*, p. 90-91.

[20] Para um maior aprofundamento no tema comércio eletrônico, que não é objeto do presente escrito, consulte-se NEWTON DE LUCCA, Títulos e contratos eletrônicos: o advento da informática e seu impacto no mundo jurídico, in *Direito & Internet: aspectos jurídicos relevantes*, Bauru-SP: EDIPRO, p. 21-100, 2000. Referido autor introduziu essa matéria no Curso de Pós-Gradução da Universidade de São Paulo, no âmbito do que denominou *Direito no espaço virtual*, o que revela pioneirismo no estudo do tema no meio acadêmico brasileiro.

o processo de venda, da simples informação sobre produtos e serviços oferecidos até os serviços pós-venda. O ato de consumo efetua-se à distância e *online*; as partes não se encontram para trocar seus consentimentos. Por isso, a Internet deve ser considerada como uma técnica de comunicação à distância, o que faz com que as vendas praticadas na *Web* sejam vistas como vendas à distância, a merecer tratamento legal especial (aplica-se aos contratos celebrados por meio eletrônicos o prazo de reflexão de sete dias, em que o consumidor pode exercer o direito de arrependimento ou de desistência do negócio, previsto no artigo 49 do Código de Defesa do Consumidor). Daí a Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000 (Diretiva sobre comércio eletrônico)[21] e as leis sobre comércio eletrônico que estão sendo editadas nos Estados-Membros da União Européia, em cumprimento a tal diretiva[22].

É importante observar que o considerando n.° 10 da Diretiva sobre comércio eletrônico deixa claro que ela "não prejudica o nível de proteção, designadamente, da saúde pública e do consumidor, estabelecido por instrumentos comunitários: nomeadamente a Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, relativa a *cláusulas abusivas nos contratos celebrados com os consumidores,* e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho, de 20 de maio de 1997, relativa à *proteção dos consumidores em matéria de contratos à distância*, que constituem um elemento essencial da proteção do consumidor em matéria contratual. Essas diretivas aplicam-se igualmente na sua integralidade aos serviços da sociedade da informação".

Referido considerando ainda estatui que "fazem igualmente parte desse acervo a Diretiva 84/450/CEE do Conselho, de 10 de setembro de 1984[23], relativa à *publicidade enganosa e comparativa*, a Diretiva 87/102/CEE do Conselho, de 22 de dezembro de 1986[24], relativa à *aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros relativas ao crédito ao consumo* (...) a Diretiva

---

[21] Dentre os conceitos previstos na Diretiva sobre comércio eletrônico estão os de: *prestador de serviços* ("qualquer pessoa, física ou jurídica, que preste um serviço no âmbito da sociedade da informação"); *destinatário do serviço* ("qualquer pessoa, física ou jurídica, que, para fins profissionais ou não, utilize um serviço da sociedade da informação, nomeadamente para procurar ou para tornar acessível determinada informação"); *consumidor* ("qualquer pessoa física que atue para fins alheios à sua atividade comercial, empresarial ou profissional"); e *comunicação comercial* ("todas as formas de comunicação destinadas a promover, direta ou indiretamente, mercadorias (produtos), serviços ou a imagem de uma empresa, organização ou pessoa que exerça uma profissão regulamentada ou uma atividade de comércio, indústria ou artesanato").

[22] A Diretiva sobre comércio eletrônico estabelece, no artigo 22.°, alínea 1, que "os Estados-Membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva, até 17 de janeiro de 2002". Esse prazo já decorreu e, como se sabe, nem todos os países da UE transpuseram a diretiva para os seus ordenamentos.

[23] Diretiva alterada pela Diretiva 97/55/CE do Parlamento Europeu e do Conselho.

[24] Diretiva com a última redação que lhe foi dada pela Diretiva 98/7/CE do Parlamento Europeu e do Conselho.

98/6/CE do Parlamento Europeu e do Conselho, de 16 de fevereiro de 1998, relativa à *defesa dos consumidors em matéria de indicações dos preços dos produtos oferecidos aos consumidores*, a Diretiva 92/59/CEE do Conselho, de 29 de junho de 1992, relativa à *segurança geral dos* produtos, a Diretiva 94/47/CE do Parlamento Europeu e do Conselho, de 26 de outubro de 1994, relativa à *proteção dos adquirentes quanto a certos aspectos dos contratos de aquisição de um direito de utilização a tempo parcial de bens imóveis*, a Diretiva 98/27/CE do Parlamento Europeu e do Conselho, de 19 de maio de 1998[25], relativa às *ações inibitórias em matéria de proteção dos interesses dos consumidores*, a Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985[26], relativa à *aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente de produtos defeituosos*, a Diretiva 1999/44/CEE do Parlamento Europeu e do Conselho, de 25 de maio de 1999, relativa a *certos aspectos da venda de bens de consumo e garantias conexas*, a futura diretiva do Parlamento Europeu e do Conselho relativa à *comercialização à distância de serviços financeiros junto dos consumidores*, a Diretiva 92/28/CEE do Conselho, de 31 de março de 1992, relativa à *publicidade dos medicamentos para uso humano*".

Deixa consignado, por fim, o mesmo considerando, que a Diretiva sobre comércio eletrônico é complementar dos requisitos de informação fixados nas diretivas citadas, e em especial na Diretiva 97/7/CE, relativa, como já se mencionou, à *proteção dos consumidores em matéria de contratos à distância.* Idêntico raciocínio deverá ser aplicado na interpretação e aplicação da futura lei do comércio eletrônico brasileira: ela será complementar às normas de proteção e defesa do consumidor existentes no ordenamento jurídico brasileiro. Existe, aliás, no Substitutivo aprovado pela Comissão Especial da Câmara dos Deputados, disposição nesse sentido. É o artigo 30, *in litteris*: *"Aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor vigentes no País.*

A propósito dos negócios eletrônicos, RÉGIS DE QUEIRÓZ, calcado em LANDOLFI e ROHRMANN, sublinha que "a nova fronteira dos negócios virtuais divide-se em três grandes categorias: o fornecimento de produtos ou a prestação de serviços na própria *Internet*, como, por exemplo, os serviços de notícias, de corretagem, de

---

[25] Diretiva com a última redação que lhe foi dada pela Diretiva 1999/44/CEE.

[26] Diretiva com a última redação que lhe foi dada pela Diretiva 1999/34/CE.

venda de programas, etc.; o fornecimento de produtos ou serviços a serem entregues ou prestados fora da Rede e, por fim, a transferência de valores. Além disso, a *Internet* serve de vitrine para todo tipo de propaganda, financiando o desenvolvimento de produtos e serviços gratuitos, incentivando a adesão de potenciais parceiros econômicos e consumidores, num círculo virtuoso, ampliando a sua inserção na vida das pessoas, das empresas e dos Governos"[27].

A Internet pode ser vista como *objeto de consumo* ou como *meio de consumo*. Exemplo da primeira hipótese: contratos celebrados com provedores de acesso; exemplo da segunda: contratos de venda à distância concluídos na Internet.

O considerando n.° 18 da Diretiva sobre comércio eletrônico dá um panorama geral dos serviços da sociedade da informação, todos prestados *on-line*: abrangem uma grande diversidade de atividades econômicas, como a celebração de contratos *on-line*; serviços que não são remunerados pelo respectivo destinatário, como os que consistem em prestar informações *on-line* ou comunicações comerciais, ou ainda os que fornecem ferramentas de pesquisa, acesso e descarregamento de dados; serviços de transmissão de informação por meio de uma rede de comunicações, de fornecimento de acesso a uma rede de comunicações ou de armazenagem de informações prestadas por um destinatário do serviço; os serviços fornecidos ponto a ponto, como o vídeo a pedido ou o envio de comunicações comerciais pelo correio eletrônico[28].

É freqüente a insuficiência de informações essenciais ao consumidor por parte dos provedores de acesso, normalmente sobre a prestação do serviço ofertado, o preço do serviço, informações de ordem técnica sobre os produtos ou serviços, etc. Isso equivale a dizer que as ofertas de acesso à Internet carecem de *transparência*, que, no sistema positivo brasileiro, foi elevada à condição de um dos princípios basilares da defesa do consumidor (CDC, art. 4.º, *caput*).

---

[27] RÉGIS MAGALHÃES S. DE QUEIRÓZ. Assinatura digital e o tabelião virtual, in *Direito & Internet – aspectos jurídicos relevantes*, Bauru-SP: EDIPRO, 2000, p. 374.

[28] O considerando n.º 18 aponta algumas atividades que não são serviços da *sociedade da informação*: a radiodifusão televisiva, na acepção da Diretiva 89/552/CEE, e a radiodifusão, dado não serem prestados mediante pedido individual; a utilização do correio eletrônico ou de comunicações comerciais equivalentes, por exemplo, por parte de pessoas físicas agindo fora de sua atividade comercial, empresarial ou profissional, incluindo a sua utilização para celebrar contratos entre essas pessoas; e as atividades que, pela sua própria natureza, não podem ser exercidas à distância e por meios eletrônicos, tais como a revisão oficial de contas de sociedades ou o aconselhamento médico, que exija o exame físico do doente.

1.4 Internet: ambiente de um novo modelo de sociedade, a sociedade da informação (ou da "comunicação rápida"[29]), em que o poder é ostentado por quem sabe abastecer-se de informação e dela dispor

Na atualidade, a *informação*, indiscutivelmente, ostenta um valor econômico, diferenciando-se do saber (incorporado ao homem), da cultura (incorporada ao grupo) e dos dados, que podem ser formalizados, constituídos em repertório, normalizados e objetivados, como assinala LECLERQ[30]. A informação hoje é vista como um recurso autônomo, gerador de riqueza e poder.

Diferenciando-se da primeira revolução industrial, que dependia de recursos finitos e que se organizava em torno da energia, a sociedade pós-industrial organiza-se em torno da *informação* e se alimenta do abastecimento inesgotável de conhecimentos. Nos países industrializados, fundamentalmente nos Estados Unidos, Japão e Comunidade Européia, existe uma onda de opinião dominante, cuja característica fundamental é que a matéria e a energia passam para um segundo plano e a informação e o conhecimento convertem-se no novo objeto formal da ciência e da tecnologia, a ponto de a economia, cultura e bem-estar social dependerem, cada vez mais, do nível alcançado no âmbito das altas tecnologias da informação[31].

O modelo cultural de uma sociedade descansa, também, sobre sua memória, cujo domínio condiciona em grande medida a hierarquia dos poderes. O acesso a fontes de informação outorga poder, nascendo com isso uma nova classe, a dos *possuidores de informação*. Na atualidade, a discriminação não se radica somente em armazenar conhecimentos, mas na habilidade de buscá-los e utilizá-los. A nova classe nasce com o emprego das telecomunicações. Trata-se de saber acessar e manejar a informação. As ferramentas que as modernas redes de telecomunicações facilitam ao

---

[29] A expressão é do filósofo francês PIERRE LEVY, para quem um novo conceito de produção do saber é a chave do futuro; é preciso uma democracia conveniente à sociedade da *comunicação rápida*, "que nos faça ver a vitalidade da invenção e do pensamento coletivo", *in* Cultura traz intelectuais de olho no futuro, *O Estado de S. Paulo*, 24.12.2000, Caderno Telejornal, p. T6.

[30] P. LECLERQ. *Ensayo sobre el estatuto jurídico de las informaciones*, em A. MADEC. *El mercado internacional de las ideas*, Madrid, 1984, p. 131. *Apud* ESTHER MORÓN, *op. cit.*, p. 85-86, notas 159 e 160.

[31] Assim, L. DÍEZ-PICAZO. Cambio social y evolución jurídica en la sociedad de la información, em *Implicaciones sociojurídicas de las tecnologías de la comunicación*, Madrid: Citema, p. 18-19; S. DORMIDO BENCOMO. Tecnologias de la información: reflexiones sobre el impacto social y humanístico, em *Informática y Derecho*, núms. 19-22, Mérida, 1998, p. 57; A. E. PÉREZ LUÑO. *Nuevas tecnologías, sociedad y derecho*, Madrid, 1987, p. 34-35. *Apud* ESTHER MORÓN, *op. cit.*, p. 86, nota 161.

usuário não somente lhe permitem acessar à informação, como também lhe proporcionam um serviço de manejo e de enriquecimento dela. Daí que a tutela material, social e jurídica (seja em sede penal ou não) da informação venha colocando-se em termos novos: protege-se o valor da "informação sobre a informação" (a informação como valor econômico em si mesma), isto é, a que permite acessar à informação pertinente e a que permite conhecê-la[32].

COUSIDO sublinha que uma das qualidades inerentes ao direito da informação é sua universalidade, a partir de três perspectivas: "as mensagens atravessam as fronteiras (universalidade geográfica); difundem-se através dos meios de comunicação (universalidade dos meios); e é um direito de todos os indivíduos (universalidade subjetiva) [33]".

Hodiernamente, as redes de informação apresentam-se como instrumento e causa da sociedade da informação. Com efeito, como se viu, sendo a Internet uma rede de computadores criada para unir um conjunto de computadores, ela se afigura, hoje, o principal procedimento tecnológico de tratamento automatizado em torno do qual se articulam a transmissão e a difusão da informação.

"A conjugação da tecnologia da telecomunicação com a informática, denominada de *telemática*, converge para a formação de uma extensa malha que, em um futuro muito próximo, interligará virtualmente todo tipo de informação disponível nas sociedades modernas, em um único e gigantesco banco de dados, possibilitando a comunicação e a realização de negócios entre comerciantes, particulares e entidades governamentais"[34].

2. INTRUSÃO INFORMÁTICA

Parafraseando trecho da reportagem *Privacidade*[35]*,* podemos afirmar que em nenhum lugar do mundo é tão difícil ter vida privada quanto na Internet. A cada clique

---

[32] NORA Y MINC. *La informatización de la sociedad*, FCE España, Madrid, 1980, p. 182 e ss., e ROMEO CASABONA. *Poder informático y seguridad jurídica*, Madrid, 1987, p. 15-33. *Apud* ESTHER MORÓN, *op. cit.*, p. 86-87..

[33] P. COUSIDO. *Derecho de la información (I). Sujetos y medios*, AA. VV., Madrid, 1992, p. 121 e ss., em ESTHER MORÓN, *op. cit.*, p. 87.

[34] RÉGIS M. S. de QUEIRÓZ. Assinatura digital e o tabelião virtual, cit., p. 375-376.

[35] *Revista Info-Exame*, São Paulo: Ed. Abril, ano 15, nº 171, Junho/2000.

do *mouse*, as pessoas são marcadas, seguidas, encaixadas em estatísticas anônimas – ou nem tanto – graças a tecnologias cada vez mais invasoras e onipresentes. Estaríamos, assim, sob o domínio do mal na *World Wide Web*? Nada mais absolutamente falso. Essas tecnologias, ao tomar conta das informações pessoais na *Web,* melhoram incrivelmente a nossa vida, com *sites* personalizados, *banners* que parecem feitos sob medida para nós, ofertas de comércio eletrônico irresistíveis etc. O desafio, a esta altura, é traçar os limites entre o que é aceitável e o que é abuso de privacidade na Internet.

No limiar do século XXI, a metáfora do *Big Brother*, o grande irmão, espionando o menor movimento das pessoas, referido no livro *1984*, de George Orwel, está obsoleta, presa nos pesadelos do século XX. Com efeito, hoje não é o Estado totalitário (praticamente desaparecido após a queda do Muro de Berlim) quem mais espreita a vida privada. "São empresas, milhares de empresas, conhecidas ou anônimas, que fazem essa vigilância 24 horas por dia. Somos filmados nos estacionamentos, identificados digitalmente na entrada dos escritórios, 'escaneados' a cada embarque num avião, monitorados por circuitos de tevê na entrada dos prédios, seguidos nos mínimos cliques na Internet. Monumentais bancos de dados garantem que informações desse tipo sejam acumuladas. Na *Web*, entre senhas e *cookies*, esse controle chega ao ápice. Qualquer coisa que respire, tenha um nome e movimente um *browser* entra nesse jogo, voluntária e involuntariamente. Quem quiser escapar terá de virar um eremita".

Com a Internet, veio a facilidade de monitorar cada um dos passos *on-line* das pessoas e integrar as informações dispersas, inclusive juntando as pegadas da *Web* com as fichas pessoais dos grandes bancos de dados convencionais das seguradoras, das escolas, das empresas de assistência médica, dos bancos, etc. É aí que mora o perigo e se acende uma imensa zona de sinal vermelho. Imaginem se as grandes corporações começarem a checar os arquivos médicos das pessoas antes de contratá-las. Ou seus históricos escolares.

"Sem que o internauta perceba, cada clique do *mouse* vai espalhando pela *Web* rastros sobre seus hábitos de compra, seus interesses, suas preferências, seu *status* conjugal, a idade dos filhos ou as doenças dos pais**.** No Brasil, 49% dos 100 *sites* mais populares em 1999 usam *cookies*, segundo testes do INFOLAB – isto é, abrem caminho até o disco rígido do internauta e armazenam ali um arquivo de texto

que identifica o seu computador com um número único. Com os *cookies,* pode-se reconhecer quem entra num site, de onde vem, com que periodicidade costuma voltar"[36].

3. PRÁTICAS ILÍCITAS NA *WEB*

3.1 Considerações gerais

Como pontifica MORALES PRATS, Professor Catedrático de Direito Penal da Universidade Autônoma de Barcelona, "o fenômeno Internet suscita um enxame de questões jurídicas de fundo, cuja elucidação requer que se opere em várias direções"[37]. Pela sua precisão e íntima relação com o tema objeto do presente ensaio, permitimo-nos reproduzir, aqui, outras observação do grande penalista espanhol:

> "A eclosão da Internet suscita um âmbito de tensão cifrado na necessidade de tutelar a *privacy* do usuário (traduzida num direito ao anonimato) *versus* segurança pública e segurança nacional como interesses coletivos. Porém, acima deste primeiro âmbito de tensão, situa-se outro mais amplo; a Rede nasce como uma nova autopista da informação, sob a égide da anomia, porquanto a ausência de regulação jurídica e, portanto, de limites de controle definem a Internet**.** Sem embargo, a rápida evolução desta autopista de informação revelou a necessidade de elaborar um estatuto jurídico; a difusão e identificação de conteúdos e condutas ilícitas na Rede e o anseio de converter esta num novo mercado virtual impõe ao poder público a necessidade desenvolver mecanismos jurídicos e institucionais que controlem a Internet. Em definitivo, estamos ante uma nova esfera de tensão entre segurança jurídica e liberdade, todavia mais complexa do que a que gerou, nos anos 70, a eclosão da informática e das redes telemáticas, tensão que, há mais de vinte anos, obrigou os Estados e a classe jurídica a criar soluções para resolver a tensão ou o conflito entre tecnologia e liberdade.
>
> Esther Morón, (...) adverte sobre a necessidade e complexidade de uma regulação jurídica para a Rede, destacando as linhas de política adequadas,

---

[36] *Revista Info-Exame*, cit.

[37] FERMÍN MORALES PRATS. Prólogo à obra de ESTHER MORÓN LERMA, *Internet y Derecho Penal: "hacking" y otras conductas ilícitas na red*, cit., p. 15.

que em nenhum caso deverão desconhecer os princípios da proporcionalidade e racionalidade das respostas jurídicas, porquanto o enxame de interesses contraditórios que estão subjacentes na nova autopista da informação pode converter-se em infrutuosas e inadequadas soluções jurídicas simplistas, porque unidirecionais.

(...)

Na presente obra efetua-se uma exposição geral de fenômenos informáticos que faz supor novos perigos para a intimidade do cidadão, neste caso o usuário da Rede, traduzindo-se na necessidade de tutela de uma nova faceta da privacidade, convertida agora no direito ao anonimato na consulta e vista da informação que oferece a Internet. A partir dessa expectativa garantista, analisam-se fenômenos como o *spamming*, os *sniffers* ou a recepção de *cookies*. Mas a intimidade e outros interesses do usuário são postos também em perigo na medida em que a Rede se converte em novo âmbito de comunicação interpessoal, que deve garantir a confidencialidade entre os comunicantes, o que suscita, por sua vez, a necessidade de gerar novos mecanismos técnicos a serviço de tal interesse, como, por exemplo, os *anonymous remailers*, como objetivo de preservar a intimidade entre remetente e destinatário de mensagens.

Não obstante, a preservação da intimidade, assim como a tutela de outros interesses não estritamente individuais na Rede, frente a condutas ilícitas na mesma Rede, reclama o esclarecimento do estatuto jurídico dos *providers*, pois, sem a fixação dos deveres jurídicos dos provedores de serviços na Rede, toda proposta de regulação jurídica estará fadada ao fracasso.

Assim, o desenvolvimento de comunicações pessoais e comerciais na Internet suscitou a aparição de novos mecanismos técnicos para preservar aquelas. Em particular a *criptografia*, que, como técnica de código de mensagens, é operativa neste âmbito, junto com a denominada *firma digital*[38]. Não obstante, o desenvolvimento ilimitado destas técnicas pode chegar a pôr em perigo interesses coletivos da Rede e, em particular, as faculdades de controle dos Estados frente à introdução de conteúdos ilícitos e à articulação de novas formas de criminalidade organizada na Rede.

---

[38] Sobre o tema assinatura digital, ver REGIS MAGALHÃES SOARES DE QUEIRÓZ, Assinatura digital e o tabelião virtual, in *Direito & Internet – aspectos jurídicos relevantes*, cit., p. 371-415.

Todas essas questões foram abordadas com lucidez e rigor por Esther Morón em sua obra, que, ademais, ingressa nas condutas ilícitas padrões na Rede e no seu possível enquadramento jurídico-penal no CP espanhol de 1995. Neste sentido, os denominados fenômenos *cracking*, *cyberpunk* e *sniffers* são analisados em profundidade como condutas ilícitas que encontram adequada subsunção típica no CP vigente. No que respeita à conduta denominada *spamming*, como forma de envio não consentido de mensagens publicitárias por correio eletrônico, na obra se conclui, com razão, que as respostas jurídicas devem dar-se fora da legislação penal.

Não obstante, a conduta que reclama maior reflexão é a denominada ***hacking***, como manifestação da intrusão informática. Neste ponto, Esther Morón aborda com profundidade as dúvidas existentes em torno da necessidade de criminalizar tal conduta, quando não vem acompanhada de um fim ilícito específico agregado ao mero desejo de curiosidade e de demonstração de perícia informática pelo *hacker*. Na obra especula-se sobre o possível enquadramento típico da intrusão informática no delito de utilização abusiva de equipamentos terminais de comunicação (art. 256 CP), no delito de dano do art. 264.2 CP ou nos delitos contra a propriedade intelectual (art. 270 CP), para concluir que o *hacking* em sentido estrito constitui uma conduta atípica, que, em todo o caso, deve encontrar resposta jurídica extramuros do Direito Penal. Com efeito, a questão é complexa e coloca no penalista a necessidade de refletir sobre os limites da intervenção penal a respeito das condutas ilícitas na Rede. Em suma, o debate não é outro senão o relativo à necessidade de ultrapassar a barreira da intervenção penal para tipificar a conduta do *hacker* como delito autônomo de mera atividade. A opção por uma proposta criminalizadora poderia vulnerar, como assinala a autora, o princípio da intervenção mínima e o caráter de *ultima ratio* do Direito Penal. Sem embargo, convirá refletir, no futuro, sobre a necessidade de que a legislação penal enfrente uma nova manifestação de intrusão, agora em versão informática e sobre a Rede, mediante técnicas de tipificação que preser-vem o princípio da ofensividade e afastem, de *lege ferenda*, problemas que suscitariam a criação de um delito de perigo abstrato pela falta de determinação e conteúdo ilícito material"[39].

3.2. Espécies de ilícitos informáticos

3.2.1 *Cookies*

Os *cookies*, assim como os arquivos de *log*, de acordo com a NRPOL - Norma de Referência da Privacidade OnLine – Versão 1.0, de junho de 2000, são considerados

[39] FERMÍN MORALES PRATS. Prólogo à obra de ESTHER MORÓN LERMA, *Internet y Derecho Penal ...,* cit., p. 15-18.

meios não-explícitos de coleta de informações on-line[40], usados pela empresa para interagir, registrar ou monitorar as atitudes de usuários em visita a seu *website*[41], para quaisquer finalidades (item 5.10).

Os *cookies*[42], os famosos biscoitinhos da *Web*, têm dado dor de cabeça aos usuários, preocupados com sua privacidade. São pequenos arquivos de textos que são gravados no computador do usuário, pelo *browser*[43], quando ele visita determinados *sites* do comércio eletrônico. Têm por escopo guardar alguns dados, como nomes e senhas, para que, quando o usuário retorne a determinados *sites*, não precise digitar tudo novamente. Para as páginas comerciais, outra é a utilidade dos *cookies* que elas distribuem. Utilizam-nos para direcionar os anúncios com base nos interesses e no comportamento do usuário. As informações coletadas pelos *cookies* são chamadas de "seqüência de cliques" ou "rastreamento de cliques", que também podem descrever quais páginas o usuário visitou em cada loja do vendedor. É o que se extrai da notícia jornalística intitulada *Avanço tecnológico também abre portas para malfeitores* [44]. Na mesma reportagem está ainda consignado o seguinte:

---

[40] Ao contrário, de conformidade com a NRPOL, são considerados *meios explícitos de coleta de informações online* "os formulários de cadastramento de pedidos de informações adicionais, de participação em concursos ou promoções, de compras online, etc. O usuário tem pleno conhecimento de que está fornecendo informações pessoais identificáveis e decide se deseja ou não fornecê-las para a Organização ou a terceiros" (item 5.9).

[41] *Website,* de acordo com a NRPOL, é uma localização na Internet que pode ser visitada e com a qual se pode estabelecer uma comunicação, obtendo ou fornecendo dados. O *website* pertence e é gerenciado por uma Organização ou indivíduo para a realização de suas atividades na Internet. O usuário, de seu turno, é definido, pela mesma Norma ética, como o "indivíduo que tem acesso ao *website* da Organização. Este indivíduo fornece ou tem suas informações pessoais ou de sua empresa coletadas para qualquer finalidade, desde o simples acompanhamento de sua sessão no ambiente online até o preenchimento de formulários para realização de compras ou para obtenção de serviços" (item 5.25).

[42] Curioso assinalar que os *cookies*, em França, são conhecidos pela expressão "témoins de connexion" (testemunhas de conexão, ao pé da letra). "Un témoin de connexion (cookie) c'est cela: une suite très peu claire de lettres et de chiffres, qui est envoyée sur votre ordinateur, le plus souvent à votre insu, par le site que vous consultez. Si vous utilisez régulièrement internet vous trouverez sur votre ordinateur une multitude de fichiers du type votrenom@www.nomdusite.txt, de taille généralement inférieure à 1 Ko, soit n'ayant aucune date d'expiration, soit em ayant une très lointaine (2010, 2037). À quoi servent ces 'témoins'? "Les 'temoins' permettent au site qui les envoie de stocker sur votre propre ordinateur, et non sur son serveur, des informations que constituent la mémoire de vos relations. Ils peuvent done être utilisés soit pour faire gagner du temps à l'internaute, soit pour mieux le connaître et lui proposer des produits personnalisés" ("Uma testemunha de conexão (cookie) é isto: uma seqüência muito pouco clara de letras e dígitos, que é enviada ao seu computador, mais freqüentemente sem o seu consentimento, pelo site que você consulta. Se você utiliza regularmente a internet, encontra no seu computador uma multiplicidade de arquivos do tipo votrenom@www.nomdusite.txt., de tamanho geralmente inferior à 1 Kb, ora não tendo nenhuma data de expiração, ora tendo uma mais distante (2010, 2037). A que servem estas "testemunhas"? As testemunhas permitem ao site que os envia armazenar em seu próprio computador, e não no seu servidor, informações que constituem a memória de sua relação. Eles podem, pois, ser utilizados seja para fazer o internauta ganhar tempo, seja para melhor o conhecer e lhe oferecer produtos personalisados"). Cf. *Le publipostage électronique et les communications commerciales non sollicitées: comment s'en protéger?*: http://www.finances.gouv.fr/cybercommerce/conseils/protec.htm.

[43] *Browser* é todo e qualquer programa que busca páginas na Internet e as apresentam na tela. Os mais utilizados são o *Netscape Navigator* e o *Internet Explorer.*

[44] *O Estado de S. Paulo*, 4.9.2000, p. I7.

"Mas eles (*cookies*) podem capturar números de cartões de crédito? Teoricamente sim, diz Paulo Vianna, diretor de tecnologia da Alladin. 'Mas lembrem-se que os números de cartões não são armazenados na máquina. Eles moram no servidor do *site* onde faz compras. O *cookie* apenas avisa ao servidor que aquele cliente específico chegou para comprar mais coisas', explica Vianna.

Os anúncios têm gerado tanta desconfiança dos usuários que as novas versões dos *browsers* (navegadores) Internet Explorer 5.5 e Netscape 6.0 já vêm com tecnologia para um controle rígido dos *cookies*. Claro que já há programas específicos que fazem isso. O *IDcide Privacy Companion* é gratuito e pode ser pego em http://www.idicide.com/download. Com ele você pode ver quais *sites* estão-lhe espionando e definir o nível de controle da privacidade. Outra opção é o *Cookie Viewer*, que permite ler e apagar os *cookies* armazenados no micro. O download está em http://www.winmag.com/scripts/download.pl/karen/ptcookie-setup.exe".

Há diversos programas com a função de detectar e "deletar" os *cookies* do computador do usuário. Um deles é o Burnt Cookies v1.006, baixado do site http://www.andersson-design.com. No *Netscape Communicator*, selecione "Editar-Preferências" e clique em "Avançado". Em "Cookies", há opções de "Desativar cookies" e "Avisar-me antes de aceitar um cookie" ou "Aceitar somente cookies que forem enviados de volta ao servidor de origem". Os diálogos de alerta de *cookie* informam de onde ele vem e tempo que vai durar.

É bom lembrar, todavia, que há sites que não são exibidos caso o recebimento de *cookies* seja rejeitado, o que torna inúteis todas as providências acima referidas para se prevenir contra a recepção de *cookies* indesejados.

Os *cookies*, realmente, podem ser lidos e apagados pelo usuário. Todavia, ao desabilitá-los, o usuário paga caro pela sua navegação anônima no oceano virtual chamado *Web*. Com efeito, mergulha num mundo de senhas, preferências que precisam ser renovadas a cada visita ao *site*, páginas que não abrem sem a presença dos terríveis "biscoitos". Segundo a matéria jornalística intitulada *Privacidade*[45], os portais latino-americanos *Star Media* e *O Site* simplesmente barram a entrada de qualquer pessoa sem *cookies*. Participar de um bate-papo do *UOL*, o maior provedor de acesso e conteúdo brasileiro, com cerca de 700.000 assinantes? Impossível. Ali os "sem-cookies" não entram. Cada um dos cem *sites* brasileiros mais populares deixa até catorze *cookies* num PC.

---

[45] Publicada na *Revista Info-Exame*, cit., p. 33.

Interessante notar que, de acordo com a mesma reportagem, "mesmo sem *cookies* os sites podem saber muita coisa de quem o visita: os *browsers* entregam boa parte do serviço. Eles dizem quem são e qual a sua versão, qual é o sistema operacional instalado na máquina usada pelo internauta e a última URL visitada por ele. O protocolo http fornece outros dados adicionais, como o endereço IP".

Aponta, ainda, que os *spammers*, "com suas baterias de e-mails indesejados, costumam usar um truque sujo para acompanhar os passos das pessoas na rede. Eles anexam um *cookie* com um número único aos e-mails em HTML e a partir daí espionam clique por clique dos destinatários, sem que eles sequer desconfiem do que está acontecendo (...). Para ter uma idéia do alcance desse perigo, basta dizer que listas brasileiras com 100.000 endereços de e-mails são oferecidas pela Internet a três por quatro, a qualquer pessoa, por 50 reais".

Noutra matéria jornalística, intitulada *De olho nos cookies (criados para facilitar a navegação, estes arquivos podem estar sendo usados como espiões)* e assinada pelo jornalista Eli Monteiro[46], são tecidas interessantes considerações sobre os *cookies*. Merecem destaque alguns trechos:

> "Mocinho ou vilão. O *cookie,* arquivo remetido pelo servidor de rede de *Websites* ao disco rígido do internauta, desperta discussões acaloradas no Brasil e no exterior sobre a privacidade na internet. Em tempos de personalização de serviços e páginas na rede, o temido arquivinho que muita gente nem conhece vem sendo acusado de espionagem. Ele estaria sendo inserido cada vez mais em HDs (discos rígidos) alheios pelos *websites* (provedores), para monitorar hábitos de navegação**.** Mas, afinal de contas, para que servem os famosos biscoitos da era digital?
>
> Toda vez que acessa um *site*, o visitante recebe 'de brinde' este arquivinho, encaminhado automaticamente ao diretório *c:**windows**cookies*, para quem usa o *browser* Internet Explorer, e *c:**arquivosdeprogramas**netscape**users*, para usuários do Netscape. Muitos sites não usam *cookies*, mas alguns mais espertinhos chegam a colocar mais de 15 biscoitos de uma só vez. (...) Depois de instalado no disco rígido, o *cookie* serviria teoricamente para facilitar a vida do navegante. Ele agiria como um tíquete de entrada,

---

[46] *Jornal do Brasil,* 21.9.2000, p. 2.

> permitindo o acesso sem barreiras, como formulários e senhas, ao conteúdo da página. Isso teoricamente. Apesar das boas intenções, o biscoito pode servir também para facilitar a vida, mas das empresas. A intenção mais singela seria descobrir os hábitos de navegação do internauta. A mais perniciosa, porém, é conseguir dinheiro repassando a terceiros os dados obtidos.
>
> Esse tipo de comércio já acontece na vida dos consumidores há algum tempo e usa a internet apenas como meio mais fácil e rápido. Quem nunca recebeu mala-direta sem que tivesse idéia de como as empresas tomaram conhecimento de sua existência? Simples. O cartão de crédito, a lista telefônica, os cadastros feitos em loja, a assinatura de publicações e muitas outras fontes estão aí à disposição de quem está ávido por uma *mailing list* e tem dinheiro para pagar.
>
> Para Carlos Cabral, coordenador do Programa Selo de Privacidade *On-Line* da Fundação Vanzolini, entidade sem fins lucrativos ligada à Universidade de São Paulo (USP**),** o *cookie* se torna preocupação a partir do momento em que é usado sem o controle e o conhecimento de usuário. **'**Ele tem uma função séria de reconhecer o visitante, mas nem sempre quem está por trás dos bancos de dados das empresas tem boas intenções**'**, analisa Cabral.
>
> (...) O diretor chama a atenção para uma questão que ultrapassa a fronteira da privacidade. O cruzamento de bancos de dados seria uma praga mais perigosa ainda. 'Se você é usuário cadastrado de um *site* de bebida alcoólica, por exemplo, pode um dia ter um seguro de saúde recusado', alerta".

Na mesma reportagem, Jason Catlett, presidente da *Junkbusters Corporation*, *site* americano que atua na defesa da privacidade *on-line*, "considera que os *cookies* só devem ser usados com autorização explícita dos usuários. 'Eles deveriam ser administrados pelos fabricantes de *browsers*, mas eles também têm interesse comercial em seguir a navegação dos usuários, critica'". Assinala, ainda, que "ficar esperando a boa vontade da indústria é perda de tempo". Para ele, "uma lei específica para regular o uso de *cookies* é fundamental".

Outro trecho da aludida notícia que merece relevo está assim vazado:

> "Será que alguém, em sã consciência, abriria seus dados na internet mesmo ignorando seu destino? Por incrível que pareça, sim. *Sites* de

> prêmios, provedores de acesso gratuito e lojas de comércio eletrônico 'oferecem' formulários a serem preenchidos pelo internauta interessado em participar de promoções. O que estas empresas ganham em troca? Dados preciosos. Na era da tecnologia da informação, a identidade é a moeda de troca com maior valor. Preferências, horários de navegação e perfil social valem mais do que o internauta imagina e, para encher os bancos de dados, estão sendo trocados por moeda real. Especula-se que o lote com cerca de 100.000 *e-mails*, por exemplo, saia pela bagatela de R$ 50.
>
> (...) A saída que algumas empresas pontocom conseguiram para conquistar a confiança dos internautas se chama Marketing de Permissão. O nome pomposo nada mais é do que pedir a permissão do internauta para a inclusão de seu nome em *mailing lists* e malas-diretas**.** Assim, ao preencher cadastros, o usuário responde se as informações podem ser repassadas. Desta forma, a empresa dá ao internauta a chance de escolher se quer ou não ser vítima de uma enxurrada de correspondência em sua caixa postal. (...) Mas nem todas as empresas oferecem escolha. Espalham seus pequenos espiões no HD (disco rígido) e ficam à espreita".

No *site* www.br-business.com.br./brb/*cookies*.htm, podem ser obtidas as seguintes informações sobre os *cookies*, todas relacionadas com sua utilidade (o *site* não se preocupa em mostrar os riscos que eles representam à privacidade e à segurança do usuário):

> *Cookies* podem ser definidos como pequenos textos (de geralmente 1 Kb), colocados no disco rígido do microcomputador do internauta por alguns *sites* que ele visitou. Contêm informações que o próprio internauta ofereceu ao *site*, como *e-mail*, preferências, o que ele comprou, seu nome, endereço, data de nascimento, etc. Se ele apenas entrou no *site* e não digitou nenhuma informação, então o *cookie* não conterá informação nenhuma.
>
> Alguns *sites* de comércio eletrônico colocam os *cookies* no *hard disk* (disco rígido) do usuário com o objetivo de personalizar os próximos atendimentos. Por exemplo, o usuário entrou em uma livraria virtual e comprou o livro *O Grande Chefão*, de Mario Puzzo. Pagou com cartão de crédito e forneceu seu nome e mais alguns dados para que a compra pudesse ser realizada. Em seu próximo acesso a esse *site*, ele receberá uma mensagem em sua tela dizendo: "Bom dia Fulano de Tal, que tal conhecer *O Grande Chefão II."* Isto significa que o atendimento foi personalizado para tal usuário. Ele

> foi reconhecido e um livro, provavelmente de seu agrado, foi-lhe oferecido.Tal exemplo mostra que, em razão do uso dos *cookies* o cliente pode ser atendido de acordo com o seu perfil e suas preferências, e o site terá uma maior probabilidade de vender-lhe outro livro. Esse tipo de operação envolvendo *cookies* e personalizando o atendimento visa a criar um vínculo com o cliente com o objetivo de que este volte outras vezes ao *site.*
>
> A grande utilidade dos *cookies* é fornecer informação sobre o número, freqüência e preferência dos usuários para que se possa ajustar a página de acordo com o gosto de cada um deles.

Ainda sobre os *cookies*, o mencionado *site* revela, além de seu poder de captação de dados, outra utilidade:

> "Nos sites de comércio eletrônico, os *cookies* também são utilizados para criar os carrinhos de compras. Digamos que o usuário esteja num site fazendo compras e de repente, por algum motivo, cai sua conexão. Acontece que ele já encheu seu carrinho com um monte de coisas. Será que o site vai perder esta venda? Pois, mesmo que o cliente volte, será que ele terá paciência para comprar tudo outra vez?
>
> Graças aos *cookies* está tudo bem. Se o cliente retornar ao *site* e quiser continuar de onde parou, os *cookies* 'lembrarão' o que tinha dentro do carrinho e o cliente não precisará começar tudo de novo".

Esclarece que "os *cookies* não transmitem vírus e podem ser lidos apenas por aqueles que o colocaram no *hard disk* do usuário, evitando o tráfego aberto de informações pela rede". Omite, todavia, a possibilidade de venda dos dados captados para empresas interessadas em *mailing lists*, normalmente para fins de envio de publicidade, por *e-mail* ou mala-direta, aos usuários.

Segundo a notícia jornalística intitulada *Softwares espiões monitoram os computadores*[47], os *cookies* levam informações dos usuários para os *sites*. "Entretanto, são dados fornecidos pelo próprio internauta, digitados nos formulários da página (...). Os *cookies* ficam arquivados no disco rígido e servem como um cartão de identificação do usuário para a próxima visita. Por si só, os *cookies* são inofensivos. O problema surge quando essas informações são fornecidas ou vendidas a outras empresas sem o

[47] De autoria de KÁTIA ARIMA, *O Estado de S. Paulo,* 30.10.2000, Caderno de Informática.

consentimento do internauta. Agências de publicidade, por exemplo, fazem cruzamentos de dados para levantar perfis de consumidores e realizar propaganda direcionada (...)".

3.2.2 *Spywares*

Spywares são programas espiões que enviam informações do computador do usuário da rede para desconhecidos. Até o que é digitado no seu teclado pode ser monitorado por eles. Alguns têm um mecanismo que faz uma conexão com o servidor do usuário sempre que ele fica *on-line.* Outros enviam informação via *e-mail*.

Os *spywares* são conhecidos como os primos-irmãos dos *cookies*. Todavia, destes se distinguem, pela forma como são deixados no PC do usuário. Enquanto os *cookies* são plantados por um *website*, os *spywares* são introduzidos por um programa *freeware*[48].

Como os *softwares* espiões "roubam" informações do PC (*Personal Computer*) do usuário? A resposta a esta indagação pode ser obtida mediante o seguinte esquema: (a) o usuário baixa um programa, quem vem com arquivo executável do *spyware* (este acompanha o pacote); (b) normalmente, o usuário não sabe o que é esse arquivo (*spyware*) e o instala; este pode obter tanto informações que estão no microcomputador como as que passam por ele – por exemplo, as digitadas no teclado; (c) alguns *spywares* tentam fechar a comunicação com o servidor do usuário toda vez que ele que ele fica *online*, estabelecendo uma conexão direta; utilizam um método de conexão proprietário com o servidor, o mesmo usado pelos comunicadores instantâneos; (d) o *sofware* espião também pode atuar usando o gerenciador de *e-mail* para enviar as informações para um endereço determinado.

Segundo a matéria jornalística *Livre seu micro dos spywares e cookies*[49], há *softwares* gratuitos que eliminam os *spywares* do micro do usuário da rede. O programa *Output* pode ser baixado no site da Gibson Research Association (http://www.grc.com).

---

[48] AMARO MORAES ensina que os "*freewares*, como o próprio nome noticia, são *softwares* disponibilizados gratuitamente, tanto na *Web* como fora dela. Contudo, o atrativo do 'é grátis!' pode custar muito caro para a sua privacidade, haja vista que praticamente todos esses programas trazem com eles um código conhecido como *spyware*, um verdadeiro Cavalo de Tróia que, uma vez instalado em seu computador, passa a rastrear suas informações para, na seqüência, noticiá-las ao fabricante (ou patrocinador) do gracioso *freeware*. Afinal ... por que uma empresa (não um homem comum) desenvolveria produtos para não lucrar com eles? Diz ainda que "a mais famosa empresa que se vale desses métodos é a RADIATE, responsável por centenas de programas *freeware* que rodam em dezenas de milhões de computadores. Coleta esses dados na condição de intermediária para que sejam personalizados os *banners* a serem apresentados ao espionado" (*Privacidade na internet*: *um enfoque jurídico*. Bauru, SP: EDIPRO, 2001, p. 86-87).

[49] Publicada no jornal *O Estado de S. Paulo*, 30.10.2000, Caderno de Informática.

O *AD-Aware* v.3.61 também encontra e "deleta" *spywares*[50]*.* Pode ser baixado no endereço http://www.lavasot.de/free.htm.

Segundo André Ptkoviski, gerente de *marketing* da *Trend Micro*, "os programas específicos para eliminar *spywares* não são necessários", pois "há antivírus atualizados que realizam esse trabalho". Já Marcos Machado, diretor geral do *site Anti-Hackers*, recomenda aos usuários que confiem apenas nas produtoras de *softwares* responsáveis, com rígidas leis de proteção à privacidade e declarações aprovadas, e por regulamentadoras, como a *Trust-e*.

3.2.3 Uso perigoso do *browser*

Browser é todo e qualquer programa que busca páginas na Internet e as apresentam na tela. Os mais utilizados são o *Netscape Navigator* e o *Internet Explorer*. À evidência, o uso devido do *browser* não contraria o Direito. Ao reverso, o seu uso indevido, perigoso ou nocivo caracteriza conduta antijurídica.

Segundo a Cartilha de Segurança para a Internet, elaborada pelo Comitê Gestor da Internet no Brasil, o *browser* pode ser perigoso de várias maneiras. Por meio de: (a) programas *Java* e *JavaScript*; (b) programas ou controles *Active X*; e (c) *downloads* de programas hostis em *sites* não confiáveis.

Consoante a mesma Cartilha, *Java* é uma forma de fazer programas, desenvolvido pela empresa *Sun Microsystems*. O programa é feito de modo a poder ser utilizado em diversos tipos de computadores e aparelhos. Na verdade, quem "roda" os programas *Java* é um outro programa chamado *Máquina Virtual Java*. Praticamente, todos os *browsers* possuem uma máquina virtual dessas embutida[51] e como não existe diferença entre uma máquina virtual de um *browser* e de outro, basta fazer um única versão do pro-grama em *Java.* Esses programas aparecem dentro das páginas da Internet e podem ser desde simples "programinhas" de efeitos especiais até pacotes de escritórios completos, com editor de texto, planilha de cálculo etc.

Um programa *Java* normalmente é seguro, explica a Cartilha. Existem, todavia, os programas *Java* hostis, suscetíveis de causar dano no computador. Para se

---

[50] AMARO MORAES afirma que os *spywares* não são identificados por programas antivírus ou firewalls, "por uma básica razão: os *spywares* são nativos do *freeware*, qual seja, suas linhas de programa são parte ativa do próprio *software*". Sustenta que programas como o *ad-ware* podem minimizar o problemas, mas não soluciona-lo (*op. cit.*, p. 87).

[51] A Cartilha explica que existem máquinas virtuais independentes, o que permite que os programas *Java* rodem sem a necessidade do *browser.*

proteger contra tais programas hostis, pode-se desligar o *Java* no *browser* em que ele está instalado. No entanto, se o uso do *Java* for absolutamente necessário, ele deve estar ligado para que as páginas de um *site* possam ser vistas, como ocorre, por exemplo, com as páginas de *home-banking*. Disso se infere que nem sempre é possível proteger-se contra os *Java* hostis. A Cartilha também esclarece que alguns dos programas antivírus mais atuais possuem a capacidade de detectar os programas *Java* hostis enquanto o *browser* está "baixando" pela internet.

O programa *JavaScript*, segundo a Cartilha, é uma versão enxuta do *Java*, que é muito mais utilizado em páginas que este, de tal sorte que, se aquele for desligado, muitas páginas deixarão de funcionar. Aconselha a desligar o *JavaScript* quando visitar uma página desconhecida e religá-lo depois, caso seja necessário.

Por outro lado, ainda segundo a Cartilha, os programas feitos em *ActiveX* funcionam de maneira similar aos programas feitos em *Java*, mas só podem ser "rodados" em máquinas com *windows*. Diferentemente dos *Java,* os programas *ActiveX* podem fazer de tudo no computador do usuário, até instalar programas em máquinas. Explica que pode ser verificada a procedência de tal programa por meio de um esquema de certificados digitais (algo parecido com o reconhecimento de firma nos documentos por cartório), de tal sorte que, aceitando-se a certificação, o programa será rodado no computador. Deve-se evitar a aceitação desses programas quando se ingressa em *sites* desconhecidos, de reputação duvidosa. Alguns programas de antivírus são capazes, segundo a Cartilha, de identificar e bloquear programas *ActiveX* maliciosos ou hostis.

3.2.4 *Spamming*

Spamming consiste na conduta de enviar mensagens não solicitadas, geralmente publicitárias, por correio eletrônico, a uma massa de usuários da rede. Tais mensagens são conhecidas, na linguagem informática, como *spams*. Normalmente, têm por objetivo promover determinado produto ou serviço e entopem a caixa de correio de muitos usuários[52]. São anúncios de produtos para emagrecimento, aumento de potência sexual,

---

[52] MARIA CLARA MAUDONNET conceitua o *spam* com bastante precisão: "spam corresponde ao envio não solicitado e não autorizado de mensagens pelo correio eletrônico, visando à divulgação de propagandas de produtos ou de serviços, assim como de quaisquer informações, com ou sem natureza comercial, de interesse da pessoa divulgadora. Assemelha-se muito a uma mala-direta eletrônica via Internet, atrativa para o divulgador, dado o seu custo reduzido, a facilidade e a rapidez de transmissão" (Invasão da Privacidade, in *Revista Consultor Jurídico*, www.conjur.com.br, 24.04.02).

venda de diplomas universitários, mensagens pornográficas etc. Essa avalanche de comunicações comerciais não solicitadas, mais comumente denominadas *spamming* - juntamente com a recolha selvagem de dados pessoais, constituição de grandes bases de perfis, comércio descontrolado de informação, multiplicação de práticas desleais, graves atentados à vida privada das pessoas, vírus no sistema informático e outras condutas ilícitas praticadas na rede - afigura-se um desafio cada vez mais preocupante ligado ao desenvolvimento da Internet e do comércio eletrônico.

SERGE GAUTHRONET e ÉTIENNE DROUARD[53], consultores do gabinete ARETE, da Comissão das Comunidades Européias, descrevem muito bem a forma de desenvolvimento do *spamming*, valendo a pena expô-la aqui. Assinalam que "o *spamming* manifesta-se por meio da existência de uma oferta de produtos (*spamware*) e serviços, que emana, a maior parte das vezes, de pequenas empresas. Podem distinguir-se duas categorias de *spamware*, os instrumentos de *pull*, ou seja, a aspiração de endereços, e os instrumentos de *push*, também conhecidos por envio de mensagens em massa. Os programas de recolha são, sobretudo, relativamente fáceis de utilizar. Funcionam segundo o princípio de uma navegação automatizada em *sites* da Web e nos espaços públicos da Usenet, utilizando uma lista de URL especificados à partida ou por palavras-chave submetidas a motores de pesquisa que permitirão constituir uma lista de URL pertinentes. O programa realiza, seguidamente, uma recolha sistemática de todos os endereços de correio eletrônico encontrados nas páginas desses *sites* ou nos *newsgroups*. Todos estes programas se gabam de poder enganar os *spam-trap* (armadilhas para detectar *spams*). Os instrumentos de *push* são motores que permitem realizar envios em massa sem passar por um servidor de correio eletrônico específico ou próprio de um ISP (fornecedores de serviços na Internet). Os produtos que se encontram normalmente no mercado permitem ao computador em que são instalados comportar-se como um verdadeiro servidor de correio, sem correr o risco, em princípio, de serem acusados de saturar a banda de passagem do ISP de que o *spammer* é assinante. Esses motores são mais ou menos poderosos para quebrar os filtros anti-*spam* dos servidores de correio e manter uma falsificação perfeita dos cabeçalhos das mensagens. Paradoxalmente, esses produtos podem encontrar-se livremente no mer-cado, comercializados por distribuidores aparentemente oficiais, sabendo que uma parte das suas funções corresponde a modalidades de desvio de tráfego na Internet, atualmente proibidas, cada vez mais, em Estados norte-americanos".

---

[53] *Comunicações comerciais não solicitadas e proteção dos dados – Síntese das conclusões do estudo – Janeiro de 2001*, http://europa.eu.int/index_pt.htm, 16.07.2002.

Os mesmos autores dizem ainda que “a oferta de serviços apresenta-se, esquematicamente, em duas grandes categorias de prestações: o serviço que alberga a campanha, a que poderíamos chamar *host-spamming*, e a corretagem de ficheiros de endereços eletrônicos. Os servidores oferecem uma prestação de serviço completa para a organização de campanhas de *spamming*; várias pequenas empresas fazem-no abertamente na Net; as tarifas variam entre 5 e 1.000 dólares por um envio e entre 20 e 1.000 dólares, se o cliente também pretende obter os endereços. Algumas têm como especialidade oferecer um serviço ‘à prova de bala’, isto é, capaz de escapar, em princípio, às ações repressivas dos ISP. Quanto aos corretores de endereços, são numerosos; várias empresas propõem ofertas de adesão que compreendem três fórmulas de assinatura de listas de endereços. Primeira fórmula: 300.000 endereços por semana, a 19,95 dólares por mês; segunda fórmula: 500.000 endereços por semana, a 29,95 dólares por mês; terceira fórmula: um milhão de endereços por semana, a 39,95 dólares por mês (...). As múltiplas propostas de listas de endereços eletrônicos levam, inevitavelmente, a que se coloque a questão da qualidade dos próprios endereços e da sua validade, para já não falar do nível de autorização real com que eles são obtidos. As listas direcionadas são apresentadas, quase sempre, de forma bastante vaga; os critérios de seleção mais correntes são o país, o Estado, a cidade de residência, o sexo, os interesses, a profissão e o domínio de atividade. Os interesses repartem-se por cinqüenta segmentos correntes que fazem lembrar a estrutura dos grandes domínios da Usenet”[54].

Finalizam, pontificando que, “no que toca aos *spammers*, que persistem num caminho perigoso e condenado por toda a comunidade, a sua prática continua a ser de amadorismo ou de oportunismo, tentando comercializar uma má idéia na Web. Vários casos recentes de *spamming* foram estudados de perto e os poucos casos conhecidos na Europa mostram que estamos em presença de operadores poucos escrupulosos, freqüentemente insensíveis aos avisos da justiça, mas que correm o risco certo de condenação ao pagamento de grandes multas por danos e interesses; esta fórmula, não sendo satisfatória do ponto de vista do direito à proteção dos dados pessoais, não é menos eficaz e pode, a curto prazo, ajudar a erradicar o fenômeno”[55].

Como se viu, o *spammer* (aquele que envia *spams*) geralmente recolhe grande quantidade de endereços eletrônicos de fontes as mais diversas e os utiliza para

---

[54] *Ibidem.*

[55] *Ibidem.*

enviar mensagens publicitárias a grande quantidade de usuários. Segundo GIUSEPPE BELLAZZI, "o envio de grande quantidade de *e-mail* não solicitada, além de provocar o protesto dos usuários, pode influir sobre a própria prestação de serviço dos sistemas de Internet Service Providers (ISP), que podem crescer assustadoramente (...). Por tal razão os ISP geralmente 'filtram' o tráfego bloqueando as mensagens provenientes das comunicações dos spammers; uma lista de indicações de casos de 'spamming' é mantida pela Naming Authority Italiana"[56].

Reiterando, aqui, o que foi consignado quando da análise dos *cookies*, os *spammers*, com suas baterias de *e-mails* indesejados, costumam usar um truque sujo para acompanhar os passos das pessoas na rede. Eles anexam um *cookie* com um número único aos *e-mails* em HTML e, a partir daí, espionam clique por clique dos destinatários, sem que eles sequer desconfiem do que está acontecendo. Para ter uma idéia do alcance desse perigo, basta dizer que listas brasileiras com 100.000 endereços de *e-mails* são oferecidas pela internet, a qualquer pessoa, por 50 reais.

Em França, o *spam* é conhecido pelo termo "polluriels". É visto como uma das formas de postagem pública eletrônica: "ele consiste em endereçar massivamente correios eletrônicos, geralmente comerciais, não solicitados, a pessoas com as quais o expedidor jamais teve contato, mas de quem obteve o endereço em fóruns de discussão, catálogos, listas de difusão, pirateando sites na Internet, ou comprando listas de endereços"[57] (*mailing lists*).

O interesse do profissional recorrer a este modo de anúncio, em França como em qualquer outro país, está no seu custo, insignificante[58]. É sobre o internauta que pesam os custos dessa publicidade que ele não procura: é ele quem paga o custo da conexão correspondente ao carregamento dessas mensagens. A CNIL avaliou, assim, em 90.000 francos o custo global dos "polluriels" (*spams*) que recaíram sobre os assinantes da *AOL (American OnLine)* em 1999[59].

---

[56] GIUSEPPE BELLAZZI, *Lo 'spamming' nel diritto italiano*: http://www.iusseek.com/civile/spamming.htm.

[57] V. *Le publipostage électronique et les communications commerciales non sollicitées: comment s'en protéger?*: http://www.finances.gouv.fr./cybercommerce/conseil/protec.html.

[58] DEMÓCRITO REINALDO FILHO observa que "o envio de panfletos com propagandas e mensagens publicitárias não solicitadas para as casas das pessoas já era prática conhecida e há muito vinha sendo utilizada – o chamado marketing direto. Mas, agora, o baixo custo das comunicações eletrônicas que permite a qualquer um que tenha uma conta de acesso à Internet enviar mensagens em número ilimitado, dimensionou o problema; sem contar que nos ambientes eletrônicos os remetentes muitas vezes se valem de técnicas de 'anomização', o que lhes permite encobrir a verdadeira identidade" (O Can-Spam Act, in *Revista Consultor Jurídico*, www.conjur.com.br, 21.06.2002).

[59] *Ibidem.*

Merece ser transcrito, aqui, o inconformismo de AMARO MORAES com a atitude antiética dos *spammers*:

> "Porque não apagar, pura e simplesmente, o *spam*.
>
> Por quê?
>
> Porque não é possível apagá-lo sem arranhar nosso espírito cívico, haja vista que o desprezível *modus operandi* dos *spammers* transfere os custos de sua publicidade para milhões de destinatários.
>
> Apagá-lo é, de certo modo, aprovar a atitude do *spammer*; é renunciar ao direito à privacidade, à tranqüilidade. É autorizar que tipos aéticos se locupletem à custa da sociedade. É compactuar com o que discordamos.
>
> Os centavos que nos forçam gastar podem parecer pouco. Entretanto bilhões de centavos passam a ter um outro significado.
>
> (...) E tudo isso em nome de um baixo custo para a divulgação de informações de pequenas, médias e grandes corporações . Baixo custo para elas, alto custo para nós, cibernautas comuns.
>
> E mesmo sendo enorme o prejuízo que os *spammers* causam, cinicamente eles tentam nos convencer de que esse prejuízo é menor que aquele frenético pó que dança nos ares."

Matéria jornalística publicada sob o título *Usuário desiste de conta devido a spam – entulho eletrônico chega na forma de listas, correntes e ofertas de empresas e amigos*[60], bem ilustra a prática de envio de *spams*, por meio do depoimento de dois usuários. Um deles, um estudante, afirma que, para cada mensagem útil, recebe quatro *spams*, mesmo com o uso de filtros, sendo que a maioria dos *spams* recebidos é americana. Outro deles, também estudante, assevera que desistiu de uma conta de *e-mail* porque recebia doze *spams* por dia. Diz, ainda, que a maioria das mensagens – até dos próprios amigos – é *spam*. Escreveu um *e-mail* para todos os amigos, manifestando-se contra o *spam*. Para sua surpresa, essa mesma mensagem tornou-se uma espécie de *spam*, sendo repassada para outras pessoas e retornando para sua própria caixa de correio. Um terceiro usuário afirmou que nem abre mais seu *hotmail*. "Não dava mais para administrar, mesmo com o filtro que usava, disse. Pelo menos dez *spams* por dia chegavam a sua caixa, anunciando empréstimos, sites de sexo e promoções".

---

[60] Jornal *O Estado de S. Paulo*, 13.11.2000, Caderno de Informática.

Realmente, o envio de *spams* é deveras perturbador da vida privada do usuário. Segundo a provedora de soluções para correios eletrônicos *Brightmail*, os números que registram o crescimento dos *spams* são impressionantes: em comparação com o ano passado (1999), as tentativas diárias de envio de *spams* e/ou *junk mail* (mensagem lixo) cresceram 400%. A empresa afirmou que está interceptando 4,9 mil tentativas de *spamming* por dia, em média. A *Ferris Research*, que realiza pesquisas, constatou que 10% das mensagens de *e-mail* enviadas são *spam*. Até 2005, estima-se que crescerá para 40% [61]. Uma organização anti-*spam* britânica, *Spamhaus Project*, conseguiu provas de que duas das maiores fornecedoras de infra-estrutura à Internet, *AT&T e PSINet*, tinham contratos com companhias *spammer*, que enviavam *e-mails* comerciais não-solicitados. A mesma empresa inglesa divulgou uma cópia de um contrato da *PSINet* com uma empresa chamada *Cajunnet*, *spammer*. A *PSINet* reconheceu a existência do contrato, justificando que eles foram assinados por empregados inexperientes e cancelados assim que descoberta a atividade de *spammer*. A *AT&T* também cancelou o contrato com a empresa *spammer*, depois de denunciada publicamente[62].

"*Spam* é um problema que se agravou violentamente", constatou o presidente da Associação Brasileira dos Provedores Internet (ABRANET-SP), Roque Abdo. A associação está elaborando uma proposta de código de ética anti-*spam* para ser apresentada brevemente para o Comitê Gestor da Internet. Por enquanto, cada provedor segue sua política com relação ao *spam*. O *Yahoo! Brasil* e o *iG*, por exemplo, não permitem o envio de mensagens com muitos destinatários. Para obter seu *e-mail* gratuito, o *iG* está solicitando e checando o número de CPF do usuário. O *Iconet* não permite receber *e-mail* de provedores que estão em listas negras de organizações anti-*spam*, como a RBL[63]. Embora seja uma medida polêmica, foi a única forma que encontrou de proteger o usuário. Tomou tal medida em virtude de acordo firmado com a *NIC BR Security Service*, órgão que cuida da segurança na Internet no Brasil[64].

Ainda para Roque Abdo, o *spam* gera muitos custos, já que congestiona os servidores de *e-mails*. "Todo mundo perde com o spam: é um marketing burro, custa caro para o provedor e ninguém agüenta mais receber *e-mails* inúteis, disse"[65].

---

[61] Vide notícia jornalística intitulada *Spam vira praga e entope caixas de e-mail*, publicada no jornal *O Estado de S. Paulo*, 13.11.2000, Caderno de Informática.

[62] Ver reportagem *Spam vira praga e entope caixas de e-mail*, cit.

[63] *Ibidem*

[64] Ver reportagem *Administrar e-mail fica cada vez mais difícil – spam torna-se grande problema na Web, mas cada provedor tem uma política diferente*, jornal *O Estado de S. Paulo*, 13.11.2000, Informática.

[65] Cf. *Administrar e-mail fica cada vez mais difícil* ..., cit.

Segundo a Cartilha de Segurança para Internet, do Comitê Gestor da Internet no Brasil, o *spam* não é oficialmente proibido, mas é considerado uma falta de ética descabida. Acrescemos que, além de antiética, a técnica de *spam* inscreve-se na esfera do ilícito, das condutas contrárias ao Direito, de sorte a merecer a adequada resposta jurídica.

Interessante matéria jornalística, intitulada *Spam com HTML ameaça privacidade*, por guardar inteira relação com a prática consistente no envio de *spams* ao usuário sem o seu consentimento, merece, à guisa de ilustração, ser aqui reproduzida:

> "O marketing na Internet está cada vez mais bisbilhoteiro. Um novo truque adotado por empresas nos EUA permite descobrir quantas pessoas leram uma mensagem de *e-mail*, ou mesmo se elas foram repassadas ou ignoradas. A informação ajuda a construir relatórios completos sobre a eficácia do *spam* – o envio indiscriminado de e-mail pela rede.
>
> O truque baseia-se em um recurso simples: o *e-mail* HTML, presente em programas como o Outlook e Netscape Messenger. Os *e-mails* publicitários são enviados nesse formato, como se fossem páginas Web, e trazem um elemento gráfico composto de um ponto único e imperceptível – que é, na verdade, um link para um gráfico no site do vendedor.
>
> Quando o e-mail é lido pelo usuário, o Outolook ou o Netscape têm de consultar o *site* do vendedor para mostrar o tal ponto – que, na verdade, serve apenas de isca. É nessa hora que o dono do *site* registra a leitura da mensagem, guardando os dados do micro do usuário"[66].

Um dos casos mais famosos relacionados com a prática de envio indiscriminado de *spams* a usuários da rede envolveu a agência de publicidade *DoubleClick*, responsável pela veiculação de 1,5 bilhão de anúncios por dia em 13.000 *sites* em todo o mundo. No ano passado, essa empresa comprou uma gigante no ramo de cadastros, a *Abacus Direct*, e pretendia confrontar os dados dessa empresa com os que ela obtém ao monitorar os anúncios. O objetivo seria, além da obtenção do nome, endereço, número de documentos, renda e outros dados comuns às fichas cadastrais do mundo real (*off line*), coletar outros dados dos usuários da rede, como, por exemplo, se ele estaria interessado em seguros de carros ou se estaria planejando fazer uma

---

[66] Jornal *O Estado de S. Paulo*, 11.12.2000, Informática, p. I 3.

viagem. Todavia, em virtude da reação da sociedade – grupos de proteção da privacidade - contra essa manifesta intrusão informática, a empresa recuou.

Sem margem para dúvidas, a conduta de envio de *spams*, um fenômeno novo, que eclodiu e se intensificou com o próprio desenvolvimento da Internet, necessita de regulação legal, pois representa o exercício abusivo de um direito, na medida em que perturba o usuário da rede e invade a sua privacidade. Pode ser vista como uma prática abusiva, nos termos do artigo 39 do Código de Defesa do Consumidor, que traz um rol meramente exemplificativo de práticas comerciais abusivas. O *spamming* seria abusivo por violar dois princípios basilares do Código de Defesa do Consumidor: o princípio da transparência pela informação eficiente (art. 4.°, *caput*) e o princípio da boa-fé objetiva (art. 4.°, III), que impõe deveres colaterais de conduta em todo o processo negocial, como o de lealdade na execução das práticas comerciais. Mas tais normas, embora importantes, na prática são insuficientes para inibir o *spamming*.

Nos Estados Unidos da América do Norte, para combater o envio indiscriminado de *spams*, foi apresentado, no mês de março de 2001, um projeto de lei que tem por objetivo regular essa matéria, denominado *Can-Spam Act*, abreviatura de *Controlling the Assault of Non-Solicited Pornography and Marketing*.

DEMÓCRITO REINALDO FILHO[67], em sucinta análise feita a esse projeto de lei, destacou os seus principais pontos: o projeto impõe uma série de exigências para o envio de *e-mail* com finalidade comercial e estabelece várias penalidades para o descumprimento dessas exigências, que vão desde a aplicação de multa até a imposição de pena de prisão; traz algumas definições para permitir sua melhor interpretação e aplicação, entre elas a de *spam*: *"unsolicited commercial eletronic mail message"*, isto é, qualquer mensagem comercial eletrônica enviada ao destinatário sem prévio consentimento, que pode ser *afirmativo* ou *implícito*. O consentimento afirmativo verifica-se quando o destinatário solicita ou autoriza o envio de uma mensagem de *e-mail* pelo remetente (*Section3,1*). Há uma solicitação ou autorização prévia que legitima o envio do *spam*. De outra parte, o consentimento implícito "é aquele que provém da circunstância de o destinatário manter com o remetente algum tipo de transação comercial (que pode ser simplesmente o fornecimento de informações, mesmo de forma gratuita), no período de cinco anos após o recebimento da primeira mensagem".

---

[67] *Op. et loc.* citados.

O *Can-Spam Act* tipifica criminalmente a conduta consistente em enviar, pelo correio eletrônico, mensagem comercial contendo informação falsa, fraudulenta ou de qualquer forma enganosa, cominando-lhe pena de multa ou de prisão, não superior a um ano (*Section 4*). No Brasil, tal conduta encontra perfeita subsunção no artigo 67 do Código de Defesa do Consumidor, que define como crime contra as relações de consumo a publicidade enganosa ou abusiva. DEMÓCRITO observa que o projeto usa a expressão "header information" no sentido de que "a falsidade ou caráter enganoso que caracteriza o crime ocorre quando ela disfarça a fonte, o destino ou retransmissões, que são informações que vêm no começo de qualquer mensagem eletrônica, incluindo o nome de domínio ou endereço eletrônico do remetente originário"[68]. Essa conduta também é tida pelo Projeto como ilícito civil, assim como aquela consistente em enviar um *e-mail* comercial com o campo do *subject* (assunto) contendo título enganoso em relação ao real conteúdo da mensagem (*Section 5*).

Por outro lado, o Projeto impõe que "todos os *e-mails* comerciais incluam um endereço eletrônico que permita ao destinatário indicar seu desejo de não receber futuras mensagens. Isso significa que adotou o sistema do 'opt out', ou seja, o envio de mensagem eletrônica comercial não será considerado *spam* se o remetente fornece meios ao destinatário de evitar o recebimento de futuras mensagens. É um sistema diferente e menos rígido do que o 'opt in', que requer que o destinatário envie uma resposta manifestando seu interesse em continuar a receber mensagens da fonte originária. Enquanto não obtiver essa resposta, o remetente fica impedido de enviar novas mensagens. No sistema do 'opt out', o remetente pode enviar as mensagens umas atrás das outras, até receber uma resposta negativa do destinatário".[69] DEMÓCRITO observa, ainda, que, no Projeto em questão, o remetente não fica obrigado a cessar incontinenti o envio das mensagens, "pois o reenvio delas só se torna ilegal se ultrapassar 10 dias do recebimento da objeção do destinatário (*Section,* a, 4)"[70]. Por fim, assinala que, além da exigência de o remetente incluir no *e-mail* comercial um endereço eletrônico para resposta do destinatário, o Projeto "prevê a obrigatoriedade de o remetente incluir na mensagem uma identificação de que se trata de uma publicidade comercial, além de seu endereço postal físico (*Section*, a, 5)"[71].

---

[68] *Ibidem*

[69] *Ibid.*

[70] *Ibid.*

[71] *Ibid.*

De se consignar, ainda, sobre o *spamming* nos Estados Unidos, que, adiantando-se à administração federal, mais de vinte Estados americanos adotaram, a partir do ano 2000, legislação repressiva em relação a essa prática abusiva. Alguns desses textos legais "já foram utilizados no quadro dos processos abertos contra os *spammers*; note-se que vários desses diplomas cobrem, simultaneamente, a comunicação comercial por fax. As principais disposições desses textos consistem em impor a presença de um dispositivo de *opt-out* (registro de opção negativa), bem como que se tenha efetivamente em conta a retirada de uma pessoa que manifeste o seu interesse nesse sentido; proíbem, obviamente, o que é intrínseco ao *spam*, ou seja, o endereço falso e a maquiagem dos cabeçalhos da mensagem ou do seu assunto; alguns impõem a presença de uma etiqueta no cabeçalho, indicando que se está perante uma mensagem publicitária (ADV) ou de um anúncio respeitante a um *site* reservado a adultos (ADLT); um terço destas leis define o *spamming* como o envio de mensagens a utilizadores da Internet, sem que tenha havido um pedido expresso da parte destes"[72].

Pode afirmar-se que as disposições regulamentares americanas, não sendo obviamente perfeitas, têm a capacidade de condenar os *spammers* a pesadas multas; a média é de 10 dólares por *bulk-mail* (envio em massa), com um máximo de 25.000 dólares por dia; tratando-se de pequenos operadores que disponham de recursos financeiros limitados, pode-se considerar que se trata de um meio de dissuasão relativamente eficaz e, em certos casos, mesmo radical[73].

Segundo SERGE GAUTHRONET e ÉTIENNE DROUARD, o *spamming* foi a doença infantil do *marketing* por correio eletrônico. Dizem que o *spamming*, na forma como o conheceram, "em meados dos anos 90, principalmente no Estados Unidos, está em recessão. Basta consultar as diferentes listas negras de *spammers*, acessíveis *on-line*, para constatar que se trata de um fenômeno que conheceu a sua idade de ouro entre 1995 e 1998 e que os registros nessas listas negras têm tido tendência a diminuir, de há dois anos a esta parte". Asseveram que quatro fatores explicam essa evolução recente: (a) a ação dos ISP (fornecedores de serviços na Internet), que adquiriram um bom controle dos fluxos nos serviços de correio e de notícias e que se dotaram de meios de reação rápidos; (b) as disposições regulamentares americanas, que, como acima se afirmou, têm capacidade de condenar os *spammers* a pesadas multas; (c) a ação das organizações e das associações profissionais, principalmente a da AIM, filial independente

[72] SERGE GAUTHRONET e ÉTIENNE DROUARD, *op. cit.*, p. 3-4, nota 3.

[73] *Ibidem.*

da poderosa DMA, que, com base em estudos pragmáticos, afirma uma oposição resoluta e inequívoca ao *spamming*; (d) a contracultura do *e-marketing*, que se apóia cada vez mais nas teses do *permission marketing* em reação à publicidade em massa que satura e semeia a confusão entre o público.

"A *permission marketing* consiste em se comunicar com os consumidores, com base no voluntariado, construindo, pouco a pouco, uma relação de interesse e, posteriormente, de confiança: à medida que a confiança aumenta, o consumidor, estimulado por promessas claramente adaptadas e, claro, cumpridas (*incentive marketing*), fica motivado no sentido de dar cada vez mais autorização para a recolha de outros dados sobre o seu estilo de vida, os seus passatempos, interesses, etc.; autorização para ser consultado sobre novas categorias de produtos ou serviços, autorização para receber pontos-brinde ou milhas, uma amostra, uma assinatura temporária, etc. É assim que, aos poucos, se constrói esse intercâmbio, o indivíduo anônimo torna-se contato, cliente potencial, depois cliente e, finalmente, cliente fiel. A criação dessa relação necessita do tempo e da freqüência e, se possível, dentro de um mecanismo de custos aceitável; que outro meio seria melhor que a Internet para proporcionar essa interatividade e essa progressividade? Que contexto de autorização poderia ser mais favorável que esse que assenta na inscrição voluntária em listas de *opt-in*? As despesas de encaminhamento são extremamente reduzidas, os resultados dos testes de campanha são quase instantâneos, as taxas de resposta são quinze vezes superiores, a relação com os clientes potenciais pode ser contínua, sem afetar os orçamentos de comunicação dos anunciantes, nem o da relação de serviço com os consumidores, desde que se saiba industrializá-lo o suficiente, e a impressão é gratuita. Toda essa tese é extraordinariamente bem ilustrada por Seth Godin, vice-presidente da Yahoo, e os profissionais do *marketing* ou do comércio *on-line* estão cada vez mais conquistados pela revelação do *permission marketing*: descobrem a eficácia do novo conceito de campanhas dirigidas a voluntários que tenham dado o seu consentimento. Hoje em dia, nos Estados Unidos, já só se fala de *opt-in e-mail marketing* (*marketing* por correio eletrônico com opção positiva)"[74].

O envio de *spams* também não passou despercebido na Proposta de Diretiva do Parlamento Europeu e do Conselho relativa *ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas*, COM (2000) 385 de

---

[74] *Op. cit.*, p. 4-5.

12 de julho de 2000, como se verá adiante. Referida proposta destina-se a substituir a Diretiva 97/66/CE, relativa *ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações*, que foi adotada pelo Parlamento Europeu e o Conselho em 15 de dezembro de 1997 e devia ser transposta em 24 de outubro de 1998, o mais tardar. Na aludida proposta, as definições de serviços e redes de telecomunicações da Diretiva 97/66/CE serão substituídas por *definições de serviços e redes de comunicações eletrônicas*[75], de modo a adaptar a terminologia à diretiva proposta, que estabelece um quadro comum para os serviços e redes de comunicações eletrônicas.

Conforme consta da exposição de motivos dessa proposta de diretiva, o artigo 12 da Diretiva 97/66/CE, em vigor, protege os assinantes contra chamadas não solicitadas para efeitos de comercialização direta. No entanto, dado que o termo "chamada" foi interpretado no sentido estrito, algumas das legislações nacionais de transposição apenas criaram uma proteção contra chamadas não solicitadas de telefonia vocal para efeitos de comercialização direta, excluindo mensagens de comercialização direta por correio eletrônico ou outras novas formas de comunicação. Para tornar o artigo tecnologicamente neutro, o termo "chamada" é substituído pelo termo "comunicação". Além disso, o correio eletrônico para efeitos de comercialização direta que não tenha sido solicitado pelo assinante (o chamado *spam*), será abrangido pelo mesmo tipo de proteção que existe para os faxes. Isto significa que *o envio de correio eletrônico não solicitado fica proibido*, exceto para os assinantes que tenham indicado que querem receber mensagens não solicitadas para fins de comercialização direta.

Consta, também, da mesma exposição de motivos, que quatro Estados-membros já dispõem de proibições relativamente a correio eletrônico comercial não solicitado e outro está prestes a adotar medidas semelhantes. Na maioria dos restantes Estados-membros, existem sistemas de rejeição (*opt-out*). Na perspectiva do mercado interno, esta situação não é satisfatória. As empresas que praticam comercialização direta (*marketing* direto) em países com sistemas de *consentimento prévio* (*opt-in*) não podem dirigir a sua comunicação comercial não solicitada a endereços de correio eletrônico no seu próprio país, mas podem continuar a enviar correio eletrônico

---

[75] A proposta de diretiva prevê cinco novas definições importantes, intimamente relacionadas com o ambiente virtual. Vejamos três delas: *utilizador* ("é qualquer pessoa física que utilize um serviço de comunicações eletrônicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço"); *dados de tráfego* ("são quaisquer dados tratados durante ou para efeitos de transmissão de uma comunicação através de uma rede de comunicações eletrônicas"); e *comunicação* ("é qualquer informação trocada ou transmitida entre um número finito de partes através de um serviço de comunicações eletrônicas publicamente disponível").

comercial não solicitado para países com um *sistema de rejeição* (*opt-out*). Além disso, dado que os endereços de correio eletrônico freqüentemente não indicam o país de residência dos seus titulares, um sistema de regimes divergentes dentro do mercado interno é, na prática, inviável. Este problema pode ser resolvido com base num sistema harmonizado de rejeição (*opt-out*).

A proposta de diretiva, ao reverso do *Can-Spam Act*, adota o sistema de consentimento prévio (*opt-in*), conforme se deduz claramente de seu artigo 13, 1, *in verbis*: "A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio eletrônico para fins de comercialização direta *apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio*" (itálicos nossos).

No Brasil, o deputado Ivan Paixão apresentou, em 05.03.2002, o Projeto de Lei n.º 6.210/2002, que dispõe sobre as limitações ao envio de mensagens eletrônicas não solicitadas (*spam*), por meio da Internet, originadas ou destinadas a computadores instalados no País.

Esse projeto define a mensagem eletrônica não solicitada (*spam*) como a "recebida por meio de rede de computadores, sem consentimento prévio do destinatário, e que objetive a divulgação de produtos, marcas, empresas ou endereços eletrônicos, ou a oferta de mercadorias ou serviços, gratuitamente ou mediante remuneração". Tal conceituação praticamente encampa a já existente, sobre o tema, na doutrina e na legislação alienígena (constituída e *in constituendo*).

É bem clara a limitação imposta pelo aludido PL ao envio de *spams*, conforme se deduz de seu artigo 3.º, *in verbis*:

> *Art. 3.º - Toda mensagem eletrônica não solicitada deverá atender aos seguintes princípios:*
>
> *I – a mensagem poderá ser enviada uma única vez, vedada a repetição a qualquer título sem o prévio consentimento do destinatário;*
>
> *II – a mensagem deverá conter, no cabeçalho e no primeiro parágrafo, uma identificação de que se trata de mensagem não solicitada;*
>
> *III – o texto da mensagem conterá a identificação do remetente e um endereço eletrônico válido; e*
>
> *IV – será oferecido um procedimento simples para que o destinatário opte pelo não recebimento de outras mensagens do mesmo remetente.*

Parágrafo único. É vedado o envio de mensagem eletrônica não solicitada a quem tiver se manifestado ao remetente contra seu recebimento.

O PL em comento parece ter-se inspirado no *Can-Spam Act*, anteriormente abordado, pois institui o sistema de rejeição *a posteriori* da mensagem eletrônica não solicitada - também conhecido como sistema *opt-out* -, ou seja, depois de recebida a primeira mensagem, como se depreende do inciso I do artigo 3.°. Mas o *spammer* (o que envia *spams*) só pode enviar uma primeira mensagem, sem o consentimento prévio do destinatário, se cumprir as exigências descritas nos incisos II a IV do mesmo artigo, quais sejam, identificar, no cabeçalho e no primeiro parágrafo da comunicação, que se trata de mensagem não solicitada (inc. II); fizer constar, do texto da mensagem, a sua identificação e um endereço eletrônico (*e-mail*) válido (inc. III); e oferecer um procedimento simples (de fácil operacionalização) para que o destinatário opte pelo não recebimento de outras mensagens dele (inc. IV).

O mesmo projeto veda expressamente que o remetente envie mensagem eletrônica não solicitada ao destinatário que já realizou a opção de não mais recebê-la, a teor da norma do parágrafo único do artigo 3.º, punindo a violação desse dever de não fazer (*non facere*) com pena de multa de até oitocentos reais por mensagem enviada, acrescida de um terço na reincidência (artigo 5.°).

Cumpre chamar a atenção do leitor para a não menos importante norma do artigo 4.°, § 1.°, de referido projeto de lei, que confere o direito subjetivo ao destinatário de "exigir do seu provedor de acesso ou de correio eletrônico, ou do provedor do remetente, o bloqueio de mensagens não solicitadas, desde que informado o endereço eletrônico do remetente". Para o descumprimento de tal obrigação é imposta a mesma sanção pecuniária estabelecida para a não-observância do dever previsto no artigo 3.° do mesmo PL (artigo 5.°). O provedor de acesso ou de serviço de correio eletrônico só não será responsabilizado pelo recebimento indevido de mensagem eletrônica – que ocorre na hipótese do parágrafo único do artigo 3.° - se houver, de boa-fé, feito uso de "todos os meios a seu alcance para bloquear a transmissão ou recepção da mensagem" (artigo 4°, § 3.°).

3.2.5 *Hoaxes*

De acordo com a Cartilha de Segurança para Internet, *hoaxes* são comuns na Internet e são *e-mails* que possuem conteúdos alarmantes ou falsos, geralmente

apontando como remetentes empresas importantes ou órgãos governamentais. Em geral, se o usuário ler atentamente esses *e-mails*, notará que seus conteúdos são absurdos, sem sentido. Essas mensagens podem, ainda, estar acompanhadas de vírus.

Dentre os *hoaxes* típicos temos as correntes ou pirâmides[76], pessoas ou crianças que estão prestes a morrer de uma doença grave, um produto alimentício que é suscetível de causar câncer etc. Histórias desse tipo são criadas para espalhar desinformação pela Internet. Esse tipo de *e-mail*, ainda segundo a Cartilha, foi inventado para entupir as caixas postais dos grandes provedores. Outro objetivo de quem escreve esse tipo de mensagem é verificar o quanto ela se espalha pelo mundo e por quanto tempo ela continua a ser espalhada, o que corresponde, mais ou menos, aos objetivos de quem programa vírus. Tais mensagens propagam-se muito em razão da boa vontade e solidariedade de quem as recebe e, por isso, é praticamente impossível eliminá-las da Internet.

Quem repassa esse tipo de mensagem para os amigos ou conhecidos, de acordo com a Cartilha, acaba endossando ou avalizando indiretamente o que está escrito, e as pessoas que recebem os *e-mails* do usuário acabam confiando em sua pessoa e não verificam a procedência nem a veracidade da história. É possível encontrar, no endereço http://HoaxBusters.ciac.org uma lista de *hoaxes* que estão circulando pela Internet com seus respectivos textos.

3.2.6 Sniffers

Os *sniffers* pertencem ao gênero dos programas espiões. Assemelham-se aos *spywares*, anteriormente descritos. São programas rastreadores, que costumam ser usados para penetrar no disco rígido (*hardware*) dos computadores conectados à rede, buscando certo tipo de informação. Sem dúvida, constituem um modo de invasão particularmente insidioso da vida privada, merecendo, assim, ser combatido.

O uso de *sniffers* permite o controle não autorizado do correio eletrônico na rede. Com efeito, lançado no *cyberspace*, um *sniffer* reconhece os *e-mails* que por ele circulam e permite seu controle e leitura. Tal ato deve reputar-se como grave atentado contra a privacidade, a exemplo das práticas ilícitas descritas anteriormente.

---

[76] Estas caracterizam crime contra a economia popular, previsto no artigo 2.°, inciso IX, da Lei n.º 1.521/51 (Lei de Economia Popular).

3.2.7 *Cavalos de Tróia (Trojan Horses)*

A expressão *Cavalo de Tróia* foi emprestada da mitologia grega. Homero, no clássico *Ilíada*, narra que houve uma guerra que envolveu as cidades de Atenas e Tróia. Esta era considerada inexpugnável. Para invadi-la e dominá-la, os atenienses adotaram a seguinte estratégia: construíram um enorme cavalo de madeira e o rechearam de centenas de soldados, com o objetivo de introduzi-lo na cidade de Tróia, que era cercada por muros instransponíveis. Ofereceram-no de presente aos troianos, que o aceitaram e abriram os portões da cidade para a sua recepção. Uma vez introduzido nos domínios de Tróia, durante a noite, os soldados gregos dele saíram e dominaram a cidade. Daí as expressões *Cavalo de Tróia* e *Presente de Grego* (esta muito utilizada na linguagem do dia-a-dia no mundo *off line*).

Cavalo de Tróia, no mundo digital, pós-moderno, bem distante dos tempos da mitologia grega, passou a ter um significado essencialmente técnico, intimamente relacionado com a intrusão informática. *Cavalo* é um programa espião, enquanto a cidade de *Tróia* passou a ser o computador do usuário da Internet. Os programas *Cavalos de Tróia*, nos termos da Cartilha de Segurança para a Internet, "são construídos de tal maneira que, uma vez instalados nos computadores, abrem portas em seus micros, tornando possível o roubo de informações (arquivos, senhas, etc.)".

Ainda de acordo com a Cartilha, o computador pode ser infectado com um tal programa da seguinte forma: o usuário recebe o *Cavalo de Tróia* como um presente (de grego). Embora o usuário possa recebê-lo de várias maneiras, na maioria das vezes ele vem anexado a algum *e-mail*. Este vem acompanhado de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Uma vez aberto o arquivo anexo, o *Trojan Horse* se instala no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos *hackers* o controle total da sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado. É um verdadeiro procedimento de invasão informática.

O computador normalmente é infectado com um *Cavalo de Tróia* sem que o usuário perceba, de tal sorte que, quando se dá conta da sua presença na máquina, já é tarde demais, os danos já ocorreram. A Cartilha explica que "os programas antivírus normalmente detectam os programas *Cavalos de Tróia* e tratam de eliminá-los como

se fossem vírus. As atualizações dos Antivírus possibilitam a detecção dos *Cavalos de Tróia* mais recentes". Adverte, porém, que, mesmo assim, "a proteção é parcial, uma vez que os *Cavalos de Tróia* mais novos poderão passar despercebidos. O ideal é nunca abrir documentos anexados aos *e-mails*". Informa, ainda, que "existem programas de *Firewall* pessoal que podem ser utilizados para barrar as conexões dos *hackers* com os *Cavalos de Tróia* que possam estar instalados em seu computador. Tais programas não eliminam os *Cavalos de Tróia*, mas bloqueiam seu funcionamento".

3.2.8 *Backdoors*

A Cartilha de Segurança para a Internet explica que "existe uma confusão entre o que é um *Backdoor* e um *Cavalo de Tróia*, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um *Cavalo de Tróia* é um programa que cria deliberadamente um *Backdoor* em seu computador. Programas que usam a Internet e que são de uso corriqueiro, como *Browsers*, programas de *e-mail, ICQ ou IRC* podem possuir *Backdoors*".

Ainda segundo a Cartilha, os *Backdoors* são abertos devido a defeitos de fabricação ou falhas no projeto dos programas. Isto pode acontecer tanto acidentalmente como pode ser introduzido ao programa propositadamente. Exemplo: versões antigas do *ICQ* possuem defeito que abre um *Backdoor* que permite ao *hacker* derrubar a conexão do programa com o servidor, fazendo com que ele pare de funcionar. Por isso, é aconselhável sempre atualizar as versões dos programas instalados no computador. O fabricante *software* com defeito tem o dever de avisar aos usuários sobre a sua existência e promover a substituição do programa por outro em perfeitas condições (CDC, art. 10, § 1°).

A Cartilha orienta o usuário no sentido de sempre visitar os *sites* dos fabricantes de *software* e verificar a eventual existência de novas versões de programas ou de pacotes que eliminem os *Backdoors*. Tais pacotes de correção são conhecidos como *patches* ou *service packs.* Adverte que os programas anti-vírus não são capazes de descobrir *Backdoors*. Já os programas de *Firewall* pessoal podem ser úteis para amenizar, mas não eliminar esse tipo de problema.

3.2.9 *Vírus*

Segundo a Cartilha, "vírus de computador são programas capazes de se reproduzir". A reprodução consiste na capacidade do vírus "de se copiar de um computador para

outro, utilizando-se de diversos meios: através dos disquetes, embutindo-se em documentos de texto ou planilhas de cálculos e, atualmente, distribuindo-se por *e-mail*". A Cartilha ensina que o computador pode ser infectado por vírus de diversas maneiras: (a) através de um disquete esquecido no *drive* A:, quando o micro é ligado; (b) executando um programa desconhecido que esteja em um disquete ou, até mesmo, em um CD-ROM; (c) instalando programas de procedência duvidosa; (d) abrindo arquivos do *World, Excel*, etc.; (e) em alguns casos, abrindo arquivos anexados aos *e-mails.*

A Cartilha explica, ainda, que "os vírus podem fazer de tudo, desde mostrar uma mensagem de 'feliz aniversário' até destruir irremediavelmente os programas e arquivos de seu computador. Praticamente, o vírus passa a ter controle total sobre o computador". O computador é infectado por um vírus sem que se perceba. "A idéia do vírus é permanecer escondido (encubado), reproduzindo-se e infectando outros micros até um evento qualquer acordá-lo. Geralmente os vírus entram em atividade em alguma data específica, como na sexta-feira, dia 13".

Os *vírus* são programas que têm, no mínimo, uma função: reproduzir-se. Já os *Cavalos de Tróia* são programas que se instalam furtivamente no micro. Juntos, são usados por *hackers* experientes e iniciantes para tomar o controle de PCs via Internet e "roubar" dados.

"Qualquer estudante de ensino primário é capaz de aprender a invadir PCs. A Web está infestada de dicas e programas desse tipo. Os mais populares, Back Orifice 2000 e Netbus Pro, contam até com sites dedicados, recheados de dicas. Para capturar presas, basta que o invasor disfarce o programa intruso com um nome inofensivo – como, por exemplo, os usados em cartões de Natal"[77].

"Essa foi a técnica usada pelos criadores do vírus Matrix, ou MTX. O programa, na verdade, tem duas partes: enquanto o vírus se encarrega de espalhar o programa entre usuários, o cavalo de Tróia substitui o programa de envio de e-mail. Dessa forma, pode multiplicar-se por toda a rede em questão de minutos"[78].

---

[77] Cf. ROBINSON DOS SANTOS, "Cartão de Natal virtual pode estragar PC – Mensagens de fim de ano são usadas por hackers para espalhar vírus e cavalos de Tróia", in *O Estado de S. Paulo*, 11.12.2000, Informática, p. I3.

[78] *Ibidem*

3.2.10 *Hacking e Cracking*

O *hacker*[79] é o grande intruso do mundo digital e utiliza várias das condutas ilícitas anteriormente referidas para desenvolver seu processo de ingerência nos computadores dos usuários da rede. As condutas de *hacking* são a forma mais expressiva da delinqüência vinculada às novas tecnologias. Tais condutas circunscrevem-se ao conjunto de comportamentos de acesso ou interferência não autorizados, de forma sub-reptícia, a um sistema informático ou a uma rede de comunicação eletrônica de dados e à utilização deles sem autorização ou além da autorização[80].

O acesso não autorizado a sistemas de informática pode ser levado a cabo pelo *hacker* com o mero (e insaciável) desejo de curiosidade e de demonstração de perícia informática, desacompanhado de um fim ilícito específico, como espiar (ou espionar), defraudar, sabotar, violar a privacidade ou vulnerar a intimidade, descobrir segredos de empresa, causar dano etc. Tem-se, neste caso, a caracterização *stricto sensu* do *hacker*. Por isso, seria incorreto identificar a conduta do *hacker* com a do delinqüente informático com caráter genérico.

A maioria dos *hackers* conhece a fundo os sistemas de informática, as linguagens de programação e os protocolos da Internet (TC/IP). Eles dedicam grande parte do tempo ao estudo da existência de "agulheiros" (portas falsas) e de falhas nos aludidos sistemas e às causas que as provocam[81].

---

[79] AMARO MORAES E SILVA NETO, estudioso dos temas afetos à Internet, buscando a origem do termo *hacker* diz que ele tem sua raiz no verbo inglês *to hack*, que apresenta vários sentidos, que vão de chute ou golpe a manjedoura, passando por táxi e podendo significar tosse. Também é aplicado a todo aquele que se vende (prostitui-se), aluga-se (mercenário) ou faz algo apenas por dinheiro. Fala da existência de histórias a respeito: "conta uma lenda urbana que o termo *hacker* foi atribuído a um indivíduo que conhecia o ponto exato onde dar um chute (*hack*) numa *vending machine* de refrigerantes para obter – sem ter que inserir qualquer moeda para tanto – sua desejada bebida gaseificada. Já uma outra lenda urbana faz referências aos funcionários das companhias telefônicas que prestavam manutenção aos telefones públicos, os quais golpeavam (*hacked*) os *apparati* em pontos precisos para saberem se liberariam as ligações correspondentes sem o devido pagamento (qual seja, a colocação da ficha, da moeda ou do cartão magnético)". Cfr. *Publicidade na internet: um enfoque jurídico*. Bauru, SP: Edipro, 2001, p. 62-63. O A. observa, com pertinácia, que, "em ambos os casos existe algo em comum: tanto o fã de refrigerantes quantos os técnicos das companhias telefônicas conheciam os pontos fracos das máquinas; conheciam seus sistemas, nos quais podiam entrar sem quaisquer autorizações. Eles sabiam aquilo que os conceptores da estrutura ignoravam" (*op. cit.*, p. 63).

[80] ESTHER MORÓN, *op. cit.*, p. 42. Ver, no mesmo sentido, GUTIÉRREZ FRANCÉS. Delincuencia económica e informática en el nuevo Código Penal, em *Ambito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, CGPJ, Madrid, 1996, p. 299-300.

[81] Os *hackers* – conhecidos como os piratas da *web* - "são indivíduos muito bem informados, com conhecimentos muito acima da média (em termos informáticos) e com privilegiada imaginação que os autoriza avaliar as falhas de um sistema operacional qualquer. São pessoas que, mais cedo ou mais tarde, acabarão sendo contratadas por grandes empresas para cooordenarem, na maioria dos casos, seus sistemas de defesa, haja vista que são muito bons e sabem escrever códigos que realmente funcionam". Cfr. AMARO MORAES, *op. cit.*, p. 63.

Uma vez dentro da máquina, podemos afirmar que o *hacker* atingiu seu desiderato. Quando não estão imbuídos de finalidades nocivas (causar danos, defraudar, vulnerar a intimidade, etc), os *hackers* não apagam nada, exceto os arquivos *logs* que se afigurem necessários para fazer desaparecer seus rastros[82]. Daí a dificuldade do descobrimento, persecução e futura repressão de tais condutas.

Atualmente, considera-se que a maior parte de comportamentos ilícitos relativos à informática são desenvolvidos por pessoas ligadas, de algum modo, às empresas, isto é, empregados de confiança, programadores, técnicos, operadores etc.[83]

Cabe fazer uma distinção entre *hacker* e *cracker*, ao menos para efeito de repressão penal de suas condutas, na medida em que as dos primeiro seriam menos nocivas do que as do segundo, de modo a merecerem tratamento legal diferenciado.

No mundo das redes de comunicação como a Internet, as condutas de *vandalismo informático* (v. os chamados *cyberpunks*), como a destruição de arquivos ou de programas, mediante o acesso digital (*online*) a computadores é típico dos denominados *crackers* – uma espécie de *hackers* de segunda categoria, que se caracterizam por terem menor conhecimento dos sistemas informáticos do que os *hackers* e sempre agirem com ânimo de prejudicar.

Os *crackers* dirigem suas ações, habitualmente, à destruição de sistemas informáticos, inserindo neles *vírus*, *Cavalos de Tróia*, *sniffers*, *spywares* etc.[84] São, portanto, mais perigosos do que os *hackers* ou meros intrusos informáticos. Todavia, não se pode olvidar, como têm observado os *experts* em informática, que uma vez descoberta a porta de entrada a um sistema informático pelo *hacker*, dificilmente ele resiste em esgotar as possibilidades que tem ao seu alcance e, em conseqüência, acaba cometendo atentados contra a intimidade, o patrimônio e outros bens jurídicos do usuário, ou contra a informação como valor econômico da empresa etc.[85]

---

[82] Para um estudo mais detalhado da atuação dos *hackers*, consulte-se *Máxima seguridad en Internet*, Madrid, 1998, disponível no site http://andercheran.upv.es/mbenet/hack.vs.crack.html.

[83] ESTHER MORÓN, *op. cit.*, p. 44.

[84] Ver, a respeito de ataques de *hackers* e outros aspectos de segurança na Internet, CONCERINO. Internet e segurança são compatíveis?, in *Direito & Internet* ..., cit., p. 131-154, especialmente p. 133-144.

[85] Para uma visão mais aprofundada sobre a delinqüência informática ou crimes de informática, consulte-se M. L. GUTIÉRREZ FRANCÉS. Notas sobre la delincuencia informática: atentados contra la 'información' como valor económico de empresa, em ARROYO ZAPATERO e KLAUS TIEDEMANN (orgs.). *Estudios de Derecho Penal Económico*, Cuenca, 1994, pp. 205 e ss. Ver, também, no Brasil, IVETTE SENISE FERREIRA. A criminalidade informática, in *Direito & Internet* ..., cit., p. 207-233; SANDRA GOUVÊA. *O Direito na era digital: crimes praticados por meio da informática*, Rio de Janeiro: Mauad, 1997.

4. NECESSIDADE DE REGULAÇÃO DA INTERNET

4.1 Considerações gerais

Como bem observa MORALES PRATS, "a Rede nasce como uma nova autopista da informação sob a égide da anomia, porquanto a ausência de regulação jurídica e, portanto, de limites e de controle definem a Internet (...), a evolução desta autopista da informação com rapidez revelou a necessidade de elaborar um estatuto jurídico; a difusão e identificação de conteúdos e de condutas ilícitas na Rede e o anseio de converter esta num novo mercado virtual impõem ao poder público a necessidade de desenvolver os mecanismos jurídicos e institucionais que controlem a Internet"[86].

Segurança ainda é o ponto mais discutido na Internet, mas, em grande parte dos casos, os problemas, como se extrai das práticas de intrusão anteriormente descritas, resumem-se à *invasão* do computador do usuário, *do site* ou à sabotagem de servidores. Preocupa-nos mais a invasão do computador do usuário da rede, pois tal intrusão atenta contra vários de seus direitos, como a sua *privacidade* (hoje vista como um dos direitos da personalidade e uma dimensão da liberdade do cidadão[87]), seu *patrimônio* e outros bens-interesses jurídicos relevantes, na medida em que ela pode destruir programas, arquivos etc. Estes, como se viu, traduzidos em *bits*, tem um grande valor econômico e, por isso, não podem ser atacados pelos *hackers* ou *crackers*.

Não se pode perder de vista que um dos direitos do "cidadão eletrônico" é o relativo ao segredo de suas comunicações, sob o perfil de que não se rastreie sua navegação e possam ser, em conseqüência, conhecidos os lugares que visita, independentemente de seu objetivo. A técnica do *spamming*, por exemplo, prepara, como ilícito anterior, a monitorização de condutas na rede. Merece, por tanto, ser rechaçada de plano, quando não consentida.

A notícia jornalística intitulada *Softwares espiões monitoram os computadores*, já referida neste estudo, chama a atenção para o fato de que "a legislação brasileira

---

[86] FERMÍN MORALES PRATS. Prólogo à obra de ESTHER MORÓN, cit., p. 15.

[87] A *privacy* "si presenta sempre piú nettamente 'come una dimensione della libertà, un antidoto contro le involuzioni autoritarie e le constrizioni del mercato' e la strada da seguire è quella che deve portarci "dal mercato alla polis, e alla 'nuova cittadinanza nel tempo dell'elettronica". Conclusão de STEFANO RODOTÀ, Presidente del Garante per la protezione dei dati personali, *in* Comunicação à 22ª Conferência Internacional sobre a Privacidade e Proteção dos Dados Pessoais, realizada em Veneza, no período de 28 a 30 de setembro de 2000, que resultou na *Carta de Veneza sobre a Privacidade e Proteção dos Dados Pessoais*, uma declaração subscrita por vinte e sete países, na qual se ratificam princípios e critérios comuns para a proteção dos dados pessoais em nível global. Ver texto da *Carta di Venezia* em http://garanteprivacy.it/garante/prewiew_paragrafo/1,1731,2232,00.html.

ainda não tem norma específica em relação à privacidade *on-line*. O Código do Consumidor é aplicável a esses casos**.** Segundo a advogada Andrea Monteiro Affonso, da Tess Advogados, a tendência no Brasil é a adoção do modelo europeu *Safe Harbor.* De acordo com a resolução que instituiu o *Safe Harbor,* aprovada neste ano pela União Européia, o usuário deve ter a alternativa de limitar o uso ou a revelação da informação. Ele deve ser avisado claramente sobre o propósito da coleta e uso de informações, o perfil de terceiros a quem são reveladas as informações, entre outras exigências."

Diz a notícia, ainda, que "nos Estado Unidos discute-se como conciliar o *Safe Harbor* com a tradição de privilegiar a liberdade contratual e auto-regulamentação de mercados (...). A privacidade do americano, enquanto isso, é desrespeitada".

Na Comunidade Européia, grande tem sido a preocupação com a privacidade e a proteção de dados pessoais dos cidadãos e dos consumidores. Com efeito, sobre o assunto há duas diretivas: a Diretiva 95/46/CE, do Parlamento Europeu e Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, a qual impõe aos Estados-Membros a garantia dos direitos e liberdades das pessoas naturais no que respeita ao tratamento de dados pessoais, nomeadamente o seu direito à privacidade, com o objetivo de assegurar a livre circulação de dados pessoais na Comunidade; e a Diretiva 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor de telecomunicações, a qual traduziu os princípios estabelecidos na Diretiva 95/46/CE em regras específicas para o setor das telecomunicações.

Atualmente, como já foi referido linhas atrás, existe uma Proposta de Diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das *comunicações eletrônicas*[88]. Tal proposta foi apresentada pela Comissão em 25 de agosto de 2000. Consta do *considerando* (3) da proposta que a "Diretiva 97/66/CE[89] deve ser adaptada ao desenvolvimento dos mercados e das tecnologias dos serviços de comunicações eletrônicas, de modo a

---

[88] Tal proposta de diretiva, como já aludimos neste escrito, destina-se a substituir a Diretiva 97/66/CE.

[89] A Diretiva 97/66/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, foi adotada pelo Parlamento Europeu e o Conselho em 15 de dezembro de 1997 e devia ser transposta em 24 de outubro de 1998. A proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no setor da comunicações eletrônicas não pretende criar grandes alterações à substância da Diretiva 97/66/CE, mas apenas adaptar e atualizar as disposições existentes a desenvolvimentos novos e previsíveis nos serviços e tecnologias de comunicações eletrônicas (cfr. Introdução da Exposição de Motivos da Proposta em tela).

fornecer um nível idêntico de proteção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas".

O artigo 1.° dessa proposta de Diretiva estabelece que ela "harmoniza as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrônicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrônicas na Comunidade".

O art. 4.°, relativo *à segurança*, dispõe que "o fornecedor de um serviço de comunicações eletrônicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede de comunicações públicas no que respeita à segurança da rede (...)".

O art. 5.°, dispondo sobre a *confidencialidade das comunicações*, estabelece que "Os Estados-Membros garantirão, na legislação nacional, a confidencialidade das comunicações (e respectivos dados de tráfego) realizadas através de redes de comunicação públicas e de serviços de comunicações eletrônicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceptação ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa (...)". O art. 6° diz que "os dados de tráfego relativos a assinantes e utilizadores tratados para efeito de transmissão de uma comunicação e armazenados pelo fornecedor de uma rede ou serviço de comunicações públicas devem ser eliminados ou tornados anônimos após a conclusão da transmissão".

Por outro lado, no tocante a *listas de assinantes*, o art. 12 prescreve que "O Estados-Membros garantirão que os assinantes sejam informados gratuitamente dos fins a que se destinam as listas de assinantes impressas ou eletrônicas publicamente disponíveis ou que podem ser obtidas através de serviços de informações de listas, nas quais os seus dados pessoais podem ser incluídos (...)". Tal disposição confere aos assinantes o direito de determinarem se querem figurar num lista pública e quais das suas informações pessoais devem nela ser incluídas e ainda de receberem informações completas sobre os fins a que se destina a lista.

O art. 13, já referido neste estudo, trata das *comunicações não solicitadas*. Estabelece que "a utilização de sistemas de chamadas automatizados sem intervenção humana (...), de aparelhos de fax ou de correio eletrônico para fins de comercialização direta apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio". Noutras palavras, concede aos assinantes o direito de recusarem comunicações não solicitadas para efeitos de comercialização direta, em todas as formas de comunicações eletrônicas, inclusive o correio eletrônico.

Na Europa, por outro lado, há espaço, na legislação penal de alguns países, para o enquadramento de condutas ilícitas na *Web*. É o caso, por exemplo, do Código Penal espanhol de 1995[90]. À guisa de exemplificação, no Título X de tal CP, e dentro dos delitos contra a intimidade, a própria imagem e a inviolabilidade do domicílio, há vários artigos que estabelecem delitos contra a intimidade e contra o segredo das comunicações, nos quais podem subsumir-se ilícitos informáticos relacionados com a vulneração da intimidade do usuário da rede. Vejam-se os artigos 197.1, segundo inciso, e 197.2, que abarcam delitos de intrusão informática.

Outra ordem de atentados informáticos é castigada como delitos contra o patrimônio e a ordem sócio-econômica. São condutas criminais realizadas por meios informáticos e que lesam o patrimônio dos usuários da rede. O art. 248.2, por sua vez, introduz a figura do crime de fraude informática (denominado, pela doutrina anglo-saxônica, de *computer fraud*). Pune-se neste preceito aqueles que, "com ânimo de lucro e valendo-se de alguma manipulação informática ou artifício semelhante, consigam a transferência não consentida de qualquer ativo patrimonial em prejuízo de terceiro. Ao tipificar as defraudações, o novo CP espanhol inclui as que tem por objeto as telecomunicações (art. 255), e também castiga "o uso de qualquer equipamento terminal de telecomunicação, sem consentimento de seu titular, ocasionando a este um prejuízo superior a cinqüenta mil pesetas" (art. 256). Pune, ainda, como meras faltas, as fraudes, apropriações indevidas, ou defraudações em equipamentos terminais de telecomunicação ..."(art. 623.4).

[90] Para um estudo aprofundado dos delitos informáticos no Direito espanhol, *vide*, entre outros, G. QUINTERO OLIVARES (Dir.). *Comentários al nuevo Código Penal*, Pamplona, 1996, p. 1255 e ss., ESTHER MORÓN. *Internet y Derecho Penal ...*, cit., p. 22-62, e A. E. PÉREZ LUÑO. *Manual de informática y derecho*, cit., p. 69-81. Um estudo mais recente sobre os crimes de informática, no âmbito europeu, foi realizado pelo conhecido especialista no tema, o Prof. ULRICH SIEBER. Está disponível em http://www2.echo.lu/legal/em/comcrime/sieber.html. Trata-se do COMCRIME-Study. Consulte-se, ainda, uma interessante coleção de conferências sobre delinqüência informática económica, em http:// www.veraz.com.ar/spanish/noframes/conferen/indic.html.

Considera-se como modalidade de delito de danos, correspondente ao que no âmbito da criminalidade de informática se entende por sabotagem, a destruição, alteração, inutilização ou danos gerais realizados a dados, programas ou documentos eletrônicos alheios contidos em redes, suportes ou sistemas informáticos (art. 264.2).

O art. 278.1 do CP, inserto no genérico Título XIII, dedicado aos delitos contra o patrimônio e contra a ordem sócio-econômica, estabelece a tutela penal da informação empresarial de caráter sensível.

O Código Penal italiano também traz, no seu bojo, alguns crimes informáticos. Estão capitulados nos seguintes artigos: 615-*terza* (acesso abusivo a um sistema informático ou telemático); *615-quater* (detenção e difusão abusiva do código de acesso a sistema informático ou telemático); 615-*quinquies* (difusão de programas que visem a danificar ou interromper um sistema informático); 617- sexties (falsificação, alteração ou supressão do conteúdo de comunicações informáticas ou telemáticas); 635-*bis* (dano de sistemas informáticos e telemáticos).

Na Bélgica, há um projeto de lei que trata de crimes informáticos (*criminalité informatique*). Segundo a exposição de motivos desse projeto, a Bélgica adotou uma posição pragmática propondo, à luz da situação internacional, um certo número de tentativas concretas a fim de fornecer aos agentes da justiça os instrumentos jurídicos adequados para lutar contra a criminalidade nas autopistas da informação[91].

Dito projeto introduz no Código Penal belga os seguintes crimes informáticos[92]: falsificação e uso de falsificação em informática (*faux et usage de faux en informatique*), artigo 210 bis; fraude informática (*fraude informatique*), artigo 504 quater; *hacking*, artigo 550 bis[93]; e sabotagem (*sabotage*)[94], artigo 559 bis.

4.2 Situação no Brasil

4.2.1 Auto-proteção pelos usuários

Preocupado com a segurança do usuário no mundo virtual da *web*, o Comitê

---

[91] BERNARD MAGREZ. *Criminalité informatique: analyse de l'avant-projet de loi belge*, in D&NT – Dossiers, http://www.droit-technologie.org/5_6.asp, 23.01.1999.

[92] Para uma boa compreensão destes novos tipos penais no projeto de lei belga, consulte-se BERNARD MAGREZ, *op. et loc.* citados.

[93] Abrange o *hacking* exterior, sem intenção fraudulenta (pena de prisão de 3 meses a 1 ano e/ou multa) e com intenção fraudulenta (pena de 6 meses a 2 anos); e o *hacking* interno com intenção fraudulenta (pena de 6 meses a 2 anos e/ou multa).

[94] Abarca a sabotagem de dados e a sabotagem de sistemas informáticos.

Gestor da Internet no Brasil editou, recentemente (15.10.2000), o que denominou de Cartilha de Segurança para a Internet, que, em resumo, se destina aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet, com o objetivo de lhes dar uma visão geral dos conceitos mais básicos de segurança, para que possam proteger-se contra a delinqüência desenvolvida no mundo dos *bits*.

Referida cartilha, no subitem 4, trata da *privacidade nas visitas aos sites*. Esclarece que, no momento em que o usuário entra em determinados *sites*, aparecem na página dados de seu computador que às vezes até assustam. Parecem adivinhar até a cor do papel-de-parede que ele está utilizando em seu computador. Isto ocorre porque existe um "bate-papo" entre o seu *browser* e o *site* que está visitando. Entre as informações que seu *browser* entrega de bandeja para o servidor do *site* visitado estão: (a) o endereço na Internet de seu computador (endereço IP); (b) nome e versão do sistema operacional; (c) nome e versão do *browser*; (d) última página visitada; e (e) resolução do monitor.

Com essas informações, os *sites* conseguem fazer as estatísticas de visitação, adequar a página do *site* ao *browser* do usuário, etc. A cartilha em tela faz o seguinte alerta ao usuário: se quer realmente esconder-se (ficar anônimo) e não passar nenhuma informação ao *site* visitado, deverá utilizar-se de serviços que o ajudam a preservar sua privacidade, como o *Anonymizer* (http://www.anonymizer.com).

A mesma cartilha sublinha que os *cookies* são utilizados pelos *sites* de diversas formas. Aponta algumas: (a) para guardar a identificação e senha do usuário quando ele pula de uma página para a outra; (b) para manter uma "lista de compras" em *sites* de comércio eletrônico; (c) personalização de *sites* pessoais ou de notícias, quando o usuário escolhe o que quer que seja mostrado nas páginas destes sites; (d) manter alvos de *marketing*, como quando o internauta entra em um *site* de CDs e pede somente CDs de MPB. Depois de um tempo, ele percebe que as promoções que aparecem são sempre de MPB (as que ele mais gosta); e (e) manter a lista das páginas visitadas em um *site*, para estatística ou para retirar as páginas em cujos links o usuário não tem interesse.

Preocupa-se com os *cookies* ao assinalar que o problema com relação a eles é que "são utilizados por empresas que vasculham suas preferências de compras e espalham estas informações para outros *sites* de comércio eletrônico". Assim, o usuário "sempre terá páginas de promoções ou publicidade, nos sites de comércio eletrônico,

dos produtos de seu interesse. Na verdade, não se trata de um problema de segurança, mas alguns usuários podem considerar este tipo de atitude uma i*nvasão da privacidade*".

4.2.2 NRPOL - Norma de Referência da Privacidade OnLine (espécie de código de ética ou deontológico)

O Brasil conta, hoje, com a denominada Norma de Referência da Privacidade OnLine – NRPOL, de junho de 2000, elaborada pela Fundação Carlos Alberto Vanzolini, ligada à Escola Politécnica da USP, com o objetivo de estabelecer determinados *princípios éticos* que devem ser seguidos por organizações atuantes na Internet, visando a proteger a privacidade das informações pessoais identificáveis de seus usuários. Estabelecidos os princípios éticos, a NRPOL enuncia também um conjunto de atividades complementares e de procedimentos normativos, que deverão ser regularmente cumpridos por todos os componentes da Organização[95]. Ademais, pode ser utilizada não apenas como um guia de referência, para uma organização implantar com eficácia uma cultura interna de preservação da privacidade *on-line*, mas também para propiciar a realização posterior de auditorias e para a obtenção do respectivo Certificado de Conformidade.

Os *princípios éticos de proteção da privacidade individual do usuário na Internet*, em que se assenta a NRPOL, são os seguintes: (a) as informações pessoais identificáveis podem ser obtidas para um ou mais propósitos e devem ser coletadas por meios éticos e legais; (b) o propósito da coleta de informações pessoais identificáveis dever ser especificado antes do instante desta coleta; (c) as informações pessoais identificáveis solicitadas devem ser adequadas, relevantes e não superar os objetivos para os quais são coletadas; (d) as informações pessoais identificáveis coletadas devem ser mantidas íntegras, conforme fornecidas pelo usuário; (e) as informações pessoais identificáveis devem ser atualizadas quando necessário ou quando for solicitado pelo usuário, (f) a Organização deve ter uma política explícita de práticas e procedimentos com relação aos dados pessoais identificáveis de seus usuários; (g) a Organização deve tomar medidas técnicas e organizacionais para

---

[95] Organização, para fins da NRPOL, "é uma unidade de uma empresa responsável por suas atividades na Internet e que, para diversas finalidades, coleta e manipula informações de seus usuários. A Organização é o escopo do Sistema de Privacidade, onde se aplica a NRPOL".

evitar a utilização desautorizada ou em desacordo com a lei e contra a perda acidental, destruição ou dano das informações pessoais identificáveis de seus usuários; (h) devem ser observados rígidos limites éticos na divulgação e utilização de informações pessoais sensíveis dos usuários; (i) o usuário deve ter acesso às informações pessoais identificáveis por ele fornecidas; e (j) o usuário deve ter mecanismos para comunicar-se com a Organização que coletou seus dados pessoais identificáveis.

Segundo esclarece a NRPOL, os citados princípios éticos foram elaborados com base na Legislação Brasileira e Internacional sobre o respeito e proteção à privacidade individual dos cidadãos e em outras matérias e princípios sobre Privacidade OnLine, como, por exemplo, os publicados pelo Conselho Europeu, US Federal Trade Comission, OECD e IRSG.

Para fins da NRPOL, são consideradas *informações pessoais identificáveis* "dados de contato (nome completo, endereços, fones, e-mails etc.), dados de cobrança ou financeiros (n.° de cartão de crédito, nível de renda, patrimônio etc.), documentos de identidade e profissionais (CPF, RG, etc.), informações sócio-demográficas (sexo, idade, estado civil, dados étnicos etc.), dados médicos (históricos ou de condições de saúde, outros), escolaridade (graus e outros), imagens da pessoa e outras informações pessoais identificáveis como *hobbies*, áreas de interesse social, entretenimento, troca de informações (*chat-rooms*), listas de discussão, boletins, etc.". São ainda consideradas informações pessoais as coletadas através de *cookies*[96] e arquivos de log[97], quando tratadas de forma a permitir a identificação do usuário.

Por outro lado, são consideradas *informações pessoais sensíveis* "as informações pessoais identificáveis e cuja divulgação, não autorizada expressamente pelo usuário, a terceiros através de mecanismo afirmativo (opt-in)[98], possa causar algum tipo de

---

[96] *Cookie*, segundo a NRPOL, é o "bloco de texto, recebido pelo usuário que pode ficar armazenado em seu computador e ativado cada vez que o website da Organização é acessado. O principal propósito do cookie é identificar o usuário e personalizar a utilização das páginas da Organização. Os cookies, por identificarem o usuário, são considerados coletores de informações pessoais".

[97] A NRPOL define o arquivo de *log* como o "arquivo que registra as ações que ocorrem no Sistema da Privacidade. Por exemplo, um arquivo de log pode registrar toda solicitação de visita a um website. Com ferramentas de análise é possível saber de onde vêm os usuários, com que freqüência retornam, como navegam no website, além de informações técnicas sobre o computador do usuário".

[98] *Opt-in* é definido, pela NRPOL, como "um mecanismo empregado pela Organização que possibilita ao usuário decidir sobre a inclusão de seus dados pessoais num banco de dados. No preenchimento de formulários, o usuário é informado claramente e opta (opt-in) autorizando que seus dados pessoais sejam incluídos naquele banco de dados, para uso posterior da Organização ou terceiros". Ao reverso, *opt-out* é "um mecanismo empregado pela Organização que possibilita ao usuário meios para excluir seus dados pessoais do banco de dados".

constrangimento moral ou danos ou prejuízos à sua pessoa ou empresa à qual pertence. Estão incluídos neste critério os dados de históricos médicos do usuário ou relacionados à sua saúde (inclusive registros de compras de medicamentos, de pesquisas ou solicitações de serviços e informações ligados à saúde), os dados que revelem origens raciais ou étnicas, dados que revelem opinião política, hábitos sexuais, religião ou credos filosóficos e os dados econômico-financeiros como números de cartão de crédito, de contas correntes em Bancos, de senhas de acesso a serviços financeiros online, dados sobre renda ou patrimônio e outras informações confidenciais que, se divulgadas sem o consentimento do usuário, possam dar origem a fraudes ou outros tipos de problemas".

4.2.3 Âmbito legislativo

A Internet, no Brasil, ainda não conta com nenhum instrumento legislativo regulador. Por decorrência, as práticas ilícitas no ambiente virtual correm soltas, sem mecanismos de adequada e necessária punição dos delinqüentes ou vândalos informáticos, responsáveis por várias das condutas ilícitas abordadas neste trabalho. Por outro lado, também não tem sido possível inibir os fornecedores de serviços no que toca a técnicas informáticas que culminam com a violação da privacidade do usuário, como os *cookies* e os *spams*, sem falar da formação, sub-reptícia, de *mailing lists* e sua conseqüente comercialização, em flagrante vulneração do direito dos usuários ao anonimato (isto é, à proteção de seus dados pessoais).

Urge, portanto, que se regulamentem os negócios realizados no espaço virtual da Internet (comércio eletrônico), com o estabelecimento de respostas jurídicas suscetíveis de proteger a privacidade e os dados pessoais dos cidadãos-usuários e outros direitos e interesses, como, por exemplo, os patrimoniais.

Vários projetos de lei tramitam no Congresso Nacional. Todos estão relacionados com aspectos do mundo virtual. O mais expressivo é o Substitutivo[99] ao Projeto de Lei n. 4.906, de 2001 (ao qual foram apensados os Projetos de Lei n.ºs 1.483, de 1999, e 1.589, de 1999), o qual *dispõe sobre o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital, institui normas para as transações de comércio eletrônico e dá outras providências*.

---

[99] Substitutivo do relator, deputado Júlio Semeghini (PSDB-SP), aprovado pela Comissão Especial da Câmara dos Deputados. Seguiu para votação no Plenário da Câmara. Se resultar aprovado, irá para o Senado e, depois, à sanção presidencial.

O art. 33 do aludido Substitutivo diz com a proteção da privacidade do usuário[100]. Está assim redigido:

> *Art. 33 - O ofertante somente poderá solicitar do destinatário informações de caráter privado necessárias à efetivação do negócio oferecido, devendo mantê-las em sigilo, salvo se prévia e expressamente autorizado pelo respectivo titular a divulgá-las ou cedê-las.*
>
> *§ 1.° A autorização de que trata o caput deste artigo constará em destaque, não podendo estar vinculada à aceitação do negócio.*
>
> *§ 2.° Sem prejuízo de sanção penal, responde por perdas e danos o ofertante que solicitar, divulgar ou ceder informações em violação ao disposto neste artigo.*

Esse dispositivo objetiva evitar que os fornecedores de produtos ou serviços na Internet exijam do consumidor mais dados pessoais do que *os efetivamente necessários para a realização do negócio jurídico*[101], prática esta muito freqüente no mercado de consumo virtual. Visa, ainda, a indevida divulgação (contra a vontade do consumidor) desses dados ou informações de caráter privado e, conseqüentemente, a sua comercialização e a formação das famigeradas *mailing lists*, a revelia dos titulares dos dados pessoais que transmitiram ao fornecedor quando da realização do negócio, situações estas que vulneram a privacidade dos usuários. Não alcança, todavia, a recepção de *cookies* e envios de *e-mails* com *spams* ou outras mensagens que importunam o usuário.

De se notar que, nos termos do artigo 40 do mesmo Substitutivo, a quebra do sigilo de informações de que trata o precitado artigo 33 caracteriza crime punido com reclusão, de um a quatro anos. A nosso ver, andou bem o legislador ao tipificar criminalmente a conduta de violação do sigilo das informações privadas fornecidas pelo consumidor, uma vez que a privacidade insere-se, induvidosamente, no campo dos bens jurídicos dignos de tutela penal. Como tem revelado a experiência, as sanções civis e administrativas não são suficientes para proteger certos bens ou interesses jurídicos, como, por exemplo, a privacidade do consumidor nos negócios realizados na Internet, de modo a justificar-se o concurso do Direito Penal, como *ultima ratio.*

---

[100] Integra o Capítulo III, que trata "da solicitação e uso das informações privadas".

[101] Em caso de litígio, o juiz definirá, de acordo com as circunstâncias do caso concreto, "as informações de caráter privado necessárias a efetivação do negócio oferecido".

O sujeito ativo desse crime é o fornecedor (o Substitutivo usa o termo ofertante) de produtos e serviços na grande rede. O crime se consuma quando ele divulga ou cede informações privadas (dados pessoais) recebidas do comprador quando da realização do negócio. Só estará isento de responsabilidade criminal se este último o autorizou a divulgar ou ceder seus dados pessoais e fez constar tal autorização em destaque no contrato. Do contrário, não terá como provar que houve a autorização do comprador.

A norma do artigo 34 do Substitutivo também é dirigida à proteção da privacidade do usuário da rede. Está vazada nos seguintes termos:

> *Art. 34 – Os provedores de acesso que assegurem a troca de documentos eletrônicos não podem tomar conhecimento de seu conteúdo, nem duplicá-los por qualquer meio ou ceder a terceiros qualquer informação, ainda que resumida por extrato, sobre a existência ou sobre o conteúdo desses documentos, salvo por indicação expressa do seu remetente.*
>
> *§ 1.° Igual sigilo recai sobre as informações que não se destinem ao conhecimento público armazenadas no provedor de serviços de armazenamento de dados.*
>
> *§ 2.° Somente mediante ordem do Poder Judiciário poderá o provedor dar acesso às informações acima referidas, sendo que as mesmas deverão ser mantidas, pelo respectivo juízo, em segredo de justiça.*

A quebra do sigilo das informações privadas exigido por essas disposições também é tipificada como crime (punido com reclusão, de um a quatro anos) pelo artigo 40 do Substitutivo em análise. Na hipótese do *caput* do artigo 34, o sujeito ativo é o *provedor de acesso*, enquanto no caso do § 1.° do mesmo artigo o sujeito-agente é o *provedor de serviços de armazenamento de dados*, como se deduz claramente de seus textos.

Não se pode olvidar, por fim, da importante norma do artigo 18, inciso VIII, do Substitutivo em exame. Tal norma obriga as autoridades certificadoras a *manter confidencialidade sobre todas as informações obtidas do titular que não constem do certificado.* É um desdobramento da norma do artigo 16, inciso II, do mesmo Substitutivo, que estabelece que, entre outros princípios, a atividade de certificação digital será regida pelo *princípio da preservação da privacidade do usuário.*

A não-observância dessa confidencialidade também tipifica crime de quebra de sigilo de informações privadas fornecidas por usuários da rede, a teor da norma

do artigo 40 do mesmo Substitutivo. O sujeito ativo, aqui, é a autoridade certificadora[102]. O Substitutivo, dentro do Título V, que trata do comércio eletrônico, traz um capítulo dedicado à proteção e defesa do consumidor no âmbito do comércio eletrônico. É o Capítulo II, no qual se destaca a norma do artigo 30, *in verbis*: *"Aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor vigentes no País".* Tais normas estão consubstanciadas, basicamente, na Lei n. 8.078/90 (Código de Defesa do Consumidor). Esse preceito deverá ser interpretado no sentido de que, na lacuna da lei sobre o comércio eletrônico ou no conflito de qualquer de seus dispositivos com os do Código de Defesa do Consumidor, deverão ser aplicados estes últimos, uma vez que a aplicação das normas do CDC jamais poderão ser vistas como subsidiárias daquelas - da lei do comércio eletrônico, caso esta venha à luz, por meio da aprovação do Substitutivo em comento ou de outro Projeto de Lei que se faça elaborar, no cipoal de PLs que tramitam no Congresso Nacional.

O Substitutivo, nos artigos 41 a 46, equipara comportamentos do mundo digital - relacionados com certificação digital e documentos eletrônicos - a condutas do mundo real tipificadas no Código Penal.

Com efeito, o artigo 41, *caput*, equipara ao crime de falsificação de papeis públicos (CP, art. 293), *a falsificação, com fabricação ou alteração, de certificado digital de ente público*; o parágrafo único desse artigo pune pela prática do mesmo crime quem *utilizar certificado digital público falsificado*; o artigo 42 equipara ao crime de falsificação de documento público (CP, art. 297), *a falsificação, no todo ou em parte, de documento eletrônico público, ou a alteração de documento público verdadeiro*; o artigo 43 equipara ao crime de falsidade de documento particular (CP, art. 298), *a falsificação, no todo ou em parte, de certificado ou documento eletrônico particular, ou alteração de certificado ou documento eletrônico particular verdadeiro*; o artigo 44 equipara ao crime de falsidade ideológica (CP, art. 299), *a omissão em documento ou certificado eletrônico público ou particular, de declaração que dele devia constar, ou a inserção ou fazer com que se efetue inserção, de declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante;* o artigo 45 equipara ao crime de supressão de documento (CP, art. 305), *a destruição, supressão ou ocultação, em benefício próprio ou de outrem, de documento eletrônico público ou particular verdadeiro, de que não se poderia dispor*; o artigo 46 equipara ao crime de extravio, sonegação ou inutilização de documento (CP, art. 314), *o extravio de qualquer*

documento eletrônico, de que se tem a guarda em razão do cargo, ou sua sonegação ou inutilização, total ou parcial.

Digno de menção é, também, o Projeto de Lei n.° 6.541, de 2002, do Deputado Paulo Rocha (PT-PA), cujo artigo 1.° acrescenta o artigo 153-A ao Código Penal, assim redigido:

> *Art. 153-A Divulgar ou comercializar endereços e dados pessoais, sem a devida autorização*
>
> *Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.*
>
> *Parágrafo único. Somente se procede mediante queixa.*

Nesse crime – de ação penal exclusivamente privada – pode ser enquadrada a conduta, hoje muito freqüente no mundo *on-line*, de formação e comercialização de *mailing lists*, sem autorização das pessoas cujos nomes e endereços, além de outros dados, figuram nessas listas. A nosso ver, como essa conduta viola a privacidade das pessoas, protegida constitucionalmente, entendemos que não se justifica considerá-la crime de ação penal privada, mas, sim, crime de ação penal pública, uma vez que nítido é o interesse público na persecução penal dessa intrusão na vida privada das pessoas.

Outro Projeto de Lei importante sobre a matéria é o n.º 3.356, de 2000, apresentado pelo Deputado Osmânio Pereira (PSDB-MG), que dispõe sobre o acesso a redes de informação, o tratamento e a disseminação de dados através de redes de informação[103].

Importa destacar o artigo 4.º desse PL, por dispor que "a oferta de acesso à rede de informação mediante remuneração de qualquer natureza, seja ao público em geral ou a uma comunidade restrita, caracteriza um serviço sujeito às disposições da Lei n.º 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor e dá outras providências".

O mesmo PL prevê várias infrações penais cometidas através de rede de informação, a saber:

---

[102] Nos termos do artigo 17, *caput*, do Substitutivo, já aprovado pela Comissão Especial da Câmara dos Deputado, *"poderão ser autoridades certificadoras as pessoas jurídicas de direito público ou privado, constituídas sob as leis brasileiras e com sede e foro no País".*

Art. 11 - Coletar dados por meios fraudulentos, desleais ou lícitos, inclusive através do exame, sem prévio consentimento, da configuração do equipamento do usuário ou de dados disponíveis no mesmo.

Pena - detenção de três meses a um ano e multa de dois mil reais, acrescida de um terço na reincidência.

Art. 12 - Divulgar informações, na forma de textos, sons ou imagens que apresentem, descrevam ou aludam a atos, atitudes ou posturas de natureza sexual, envolvendo a participação direta ou indireta de crianças ou adolescentes, ou que caracterizem, de outra forma, a prática de pornografia infantil.

Pena - reclusão de um a quatro anos e multa de dois mil a dez mil reais.

Art. 13 - Divulgar informações, na forma de textos, sons ou imagens que estimulem ou façam apologia do uso de drogas ilegais.

Pena - detenção de seis meses a dois anos e multa de dois mil a quarto mil reais, acrescida de um terço na reincidência.

Art. 14 - Divulgar informações, na forma de textos, sons ou imagens, que estimulem ou façam apologia do uso da violência, ou ensinem métodos de fabricação de armas e explosivos.

Pena - detenção de seis meses a dois anos e multa de dois mil a quatro mil reais, acrescida de um terço na reincidência.

Art. 15 - Inserir, em equipamento do usuário ou da própria rede, programa ou rotina destinada a provocar danos em dados, informações ou outros programas ali existentes, ou afetar, de qualquer modo, o desempenho, a velocidade ou a eficácia do processamento de dados e instruções.

Pena - detenção de seis meses a dois anos e multa de dois mil a quatro mil reais, acrescida de um terço na reincidência.

O artigo 16, estatui, por fim, que “as infrações às demais disposições desta lei sujeitarão o infrator à pena de multa, de trezentos a mil reais, acrescida de um terço na reincidência”. Tal disposição refere-se, obviamente, às infrações de natureza civil.

Afigura-se oportuno fazer alusão ainda, nestes tempos em que a legislação disciplinadora da Internet encontra-se em constituição, ao Projeto de Lei do Senado n.º 76, de 2000, apresentado pelo senador Renan Calheiros, que também tipifica vários crimes de informática, a saber:

Art. 1.º Constitui crime de uso indevido da informática:

§ 1.º contra a inviolabilidade de dados e sua comunicação:

I - a destruição de dados ou sistemas de computação, inclusive sua inutilização;

II - a apropriação de dados alheios ou de um sistema de computação devidamente patenteado;

III - o uso indevido de dados ou registros sem consentimento de seus titulares;

IV - a modificação, a supressão de dados ou adulteração de seu conteúdo;

V - a programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade.

Pena: detenção, de um a seis meses e multa.

§ 2.º contra a propriedade e o patrimônio:

I - a retirada de informação privada contida em base de dados;

II - a alteração ou transferência de contas representativas de valores;

Pena: detenção, de um a dois anos e multa.

§ 3.º contra a honra e a vida privada:

I - difusão de material injurioso por meio de mecanismos virtuais;

II - divulgação de informações sobre a intimidade das pessoas sem prévio consentimento;

Pena: detenção, de um a seis meses e multa.

§ 4.º contra a vida e integridade física das pessoas:

I - o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou homicídios;

II - a elaboração de sistema de computador vinculado a equipamento mecânico, constituindo-se em artefato explosivo;

Pena: reclusão, de um a seis anos e multa.

§ 5.º contra o patrimônio fiscal :

I - alteração de base de dados habilitadas para registro de operações tributárias;

II - evasão de tributos ou taxas derivadas de transações "virtuais";

Pena: detenção, de um a dois anos e multa.

§ 6.º contra a moral pública e opção sexual:

I - a corrupção de menores de idade;

II - divulgação de material pornográfico;

III - divulgação pública de sons, imagens ou informação contrária aos bons costumes.

Pena: reclusão, de um a seis anos e multa.

§ 7.º contra a segurança nacional:

I - a adulteração ou revelação de dados declarados como reservados por questões de segurança nacional;

II - a intervenção nos sistemas de computadores que controlam o uso ou ativação de armamentos;

III - a indução a atos de subversão;

IV - a difusão de informação atentatória a soberania nacional.

Pena: detenção, de um a dois anos e multa.

O artigo 5.º prescreve "que todos os crimes por uso indevido de computador estão sujeitos a multa igual ao valor do proveito pretendido ou do risco de prejuízo da vítima".

A nosso ver, esse PL, além de exagerar na tipificação, apresenta várias imperfeições, de modo a merecer a devida correção e aprimoramento. Em virtude do estreito limite deste ensaio, deixamos de apontar, aqui, o que entendemos incorreto nesse PL. Certamente, emendas a esse projeto serão apresentadas, de forma a escoimar-lhe os vícios que ostenta.

A tipificação penal da delinqüência desenvolvida no mundo digital deve restringir-se, a nosso ver, às condutas ilícitas praticadas no ambiente virtual dirigidas contra bens jurídicos dignos de proteção penal, em respeito ao princípio de que o Direito Penal somente deve atuar como *ultima ratio*, ou seja, quando as sanções civis e administrativas são insuficientes para inibir o ilícito. Seguindo rigorosamente tal princípio e os passos da legislação estrangeira, merecem ser definidas como crimes condutas tipicamente digitais, que escapam do âmbito da legislação penal e não se consegue evitar com o recurso a mecanismos de controle civis ou administrativos, como o *hacking*, a introdução de vírus nos sistemas informáticos, a sabotagem de dados ou de sistemas

informáticos, fraudes informáticas, talvez o envio maciço de publicidade pelo correio eletrônico (*spamming*), à revelia dos destinatários etc.

Hoje, há uma verdadeira febre do legislador em tipificar criminalmente os ilícitos cibernéticos, como demonstram os vários projetos de lei que prescrevem crimes de informática, parte deles abordada neste estudo. Há necessidade de reunir esses projetos com vista à sua harmonização, para se evitar o risco de repetição de tipificações ou tipificações assemelhadas, que dificultam sobremaneira o trabalho do intérprete e do aplicador do Direito, como sói acontecer neste País. Demais, devem ser extirpados desses projetos os ilícitos típicos que se referem a bens jurídicos que não são dignos de uma tutela penal, à medida que podem ser prevenidos com a simples aplicação de sanções no âmbito administrativo e/ou civil, reservando-se, pois, a tipificação criminal para as condutas digitais mais graves, como já vem ocorrendo na Europa e nos Estados Unidos.

Várias condutas ilícitas praticadas através da Internet já encontram subsunção no próprio Código Penal, como o estelionato praticado por meio informático, mas há necessidade de se alterar ou acrescentar dispositivos a esse *Codex* para permitir a perfeita subsunção no seu corpo de certos ilícitos informáticos, sob pena de se violar o basilar princípio da legalidade (*nullum crimem, nulla poena, sine lege*). Ou então, como já se fez nos artigos 41 a 46 do Substitutivo ao Projeto de Lei n. 4.906, de 2001 – anteriormente comentado -, equiparar mais condutas ilícitas do mundo digital a comportamentos já tipificados no Código Penal

VICENTE GRECO, a propósito da necessidade, ou não, de se tipificar condutas ilícitas na Internet, manifesta-se no sentido de que "se houver alguma modificação a fazer, deve ser feita dentro de uma perspectiva de proteção genérica de um bem jurídico"[104]. Exemplifica afirmando que "se quer discutir a proteção à intimidade, não se deve fazê-lo especificamente para a Internet, porque a proteção, se for o caso, deve ser genérica, porque tanto a intimidade pode ser invadida na utilização da rede quanto por uma gravação ambiental ou pelos *paparazzi*"[105]. Na mesma direção é o escólio de RAÚL CERVINI, para quem, sem prejuízo de propugnar soluções de *lege ferenda*, sustenta que "es imperioso ensayar ante todo uma lectura imaginativa de

---

[103] Rede de informação é conceituada, no aludido PL, como "qualquer sistema destinado à interligação de computadores ou demais equipamentos de tratamento de dados, por meio eletrônico, ótico ou similar, com o objetivo de oferecer, em caráter público ou privado, informações e serviços a usuários que conectem seus equipamentos ao sistema" (art. 2.º).

[104] VICENTE GRECO FILHO. "Algumas Observações sobre o Direito Penal e a Internet", in *Boletim IBCCRIM*, edição especial, ano 8, n.° 95, outubro – 2000, p. 3.

[105] *Ibidem*

los textos vigentes, procurando abarcar en ellos, caso a caso, algumas de las manipulaciones por computadora de mayor dañosidade"[106].

A posição de VICENTE GRECO afina-se com a adotada pelo Código Penal espanhol (de 1995). Concordamos com ela; porém, urge que se crie um título no Código Penal relacionado com a proteção da privacidade ou da intimidade e nele se incluam condutas violadoras desses bens jurídicos, independentemente do meio em que forem realizadas. O legislador, todavia, por ora, está preferindo tipificar a quebra do sigilo de informações de caráter privado, em lei extravagante, conforme se dessume da norma do artigo 40 do Substitutivo anteriormente comentado. Mas há outras condutas que merecem repressão penal, como a subtração de informações e danos a programas praticados por *hackers*, as quais não se subsumem adequadamente nos tipos de furto e de dano previstos no Código Penal.

De fato, problemas existem no tocante ao enquadramento de comportamentos informáticos ilícitos nos tipos do Código Penal que definem os crimes contra o patrimônio, como, por exemplo, o furto, que requer que a subtração seja de *coisa alheia móvel*. Se uma pessoa subtrai informações gravadas no disco rígido de um computador que não lhe pertence e não está autorizado a usar, cometeria ela o crime de furto? Os dados subtraídos podem ser considerados *coisa móvel*?

MONTANO GÓMEZ entende que os dados podem ser enquadrados no conceito de coisa imaterial e, portanto, podem ser objeto do crime de furto[107]. Mas a questão não é pacífica. Pode-se entender o contrário, ou seja, que os dados, as informações em *bytes*, não se traduzem em coisa alheia móvel, na acepção da doutrina e jurisprudência fincadas no Código Penal, precedente à eclosão do fenômeno Internet, que conta pouco mais de dez anos de existência.

Como se vê, a questão da punição de condutas ilícitas praticadas por meios informáticos é demasiado complexa, máxime no campo criminal. Exige um estudo

---

[106] RAÚL CERVINI. Reflexiones sobre los fraudes informáticos por manipulaciones, in *Cursillo sobre derecho penal económico*, Montevideo, FDSC, 1990, p. 167, *apud* MONTANO GÓMEZ, Delitos informáticos y los tipos que exigen la "cosa ajena mueble", in *Justiça penal*, São Paulo: Ed. RT., n. 7, 2000, p. 341, nota 36.

[107] PEDRO J. MONTANO GÓMEZ, *op. cit.*, p. 340-342. Em sentido contrário, afirmando a impossibilidade do furto de dados, ver: JEAN PRADEL, C. FEUILLARD. Les infractions commises au moyen de l'ordinateur, in *RD pénal, crim.*, 1985, p. 317; G. CHAMPY. *La fraude informatique*, PU, Aix-Provence, 1992. *Lamy* Informatique,1998, p. 1693. Apud MONTANO GÓMEZ, *op. cit.*, p. 340. Segundo este último autor, aqueles remetem a tutela al âmbito de la propriedade intelectual, uma vez que os dados são criação intelectual. Sem embargo, admite-se a "apreensão" de dados em pirataria, coisa que seria contraditória, *Lamy...*, cit., p. 1694.

aprofundado, o que não é possível nos estritos limites do presente artigo, um simples ensaio sobre práticas ilícitas na Internet, com vistas à sua prevenção e repressão, de *lege lata* e, principalmente, de *lege ferenda.*

Marco Antonio Zanellato,

procurador de Justiça,
coordenador do CENACON

BIBLIOGRAFIA

BELLAZZI, G. *Lo 'spamming' nel diritto italiano*. In: http://www.iusseek.com/civile/spamming.htm.

CERVINI, R. Reflexiones sobre los fraudes informáticos por manipulaciones. *Cursillo sobre Derecho Penal Econômico.* Montevideo: FDSC, 1990.

CHAMPY, G. La fraude informatique. Aix-Provence: PU, 1992.

DE LUCCA, N. Títulos e Contratos Eletrônicos: o advento da informática e seu impacto no mundo jurídico. In: *Direito & Internet – Aspectos jurídicos relevantes.* Bauru-SP: EDIPRO, 2000, p. 21-100.

FERNÁNDEZ ESTEBAN, M. L. *Nuevas tecnologias, Internet y derechos fundamentales.* Madrid, 1998.

FERREIRA, I. S. A criminalidade informática. In: *Direito & Internet – Aspectos jurídicos relevantes.* Bauru-SP: EDIPRO, 2000, p. 207-233.

GAUTHRONET, S. e DROUARD, E. *Comunicações comerciais não solicitadas e proteção dos dados – síntese das conclusões do estudo,* janeiro de 2001. In: http://europa.eu.int/index_pt.htm, 16.07.2002.

GRECO FILHO, V. Algumas observações sobre o direito penal e a internet. In: *Boletim IBCCRIM,* edição especial, ano 8, n.º 95, outubro-2000.

GRECO, M. A. Transações eletrônicas. Aspectos jurídicos. In: *Revista de Direito Bancário, do Mercado de Capitais e da Arbitragem*. São Paulo: Editora Revista dos Tribunais, v. 8, abr.-jun. de 2000, p. 65-69.

GUTIÉRREZ FRANCÉS, M. L. Delincuencia económica e informática en el nuevo Código Penal. In: *Ambito jurídico de las tecnologías de la información,* Cuadernos de Derecho Judicial, Madrid: CGPJ, 1996.

¾¾. Notas sobre a delincuencia informática: atentados contra a información como valor económico de empresa, Arroyo Zapatero e Klaus Tiedemann (orgs.). *Estudios de Derecho Penal Económico.* Cuenca, 1994, p. 205 e ss.

LEVY, P. Sobre a cibercultura. In: *Revista de Occidente,* n.º 206, Madrid, 1998.

LORENZETTI, R. L. Informática Cyberlaw, E-Commerce. In: *Direito & Internet – Aspectos jurídicos relevantes*. Bauru-SP: EDIPRO, 2000, p. 419-460.

MAGREZ, B. *Criminalité informatique: analyse de l'avant-projet de loi belge*. In: D&NT – Dossiers, http://www.droit-technologie.org/5_3.asp, 23.01.1999.

MAUDONNET, M. C. Invasão da privacidade. In: *Revista Consultor Jurídico*, www.conjur.com.br, 24.04.2002.

MONTANO GÓMEZ, P. J. Delitos informáticos y los tipos que exigen la “cosa ajena mueble”. In: *Justiça penal.* São Paulo: Ed. Revista dos Tribunais, n.º 7, 2000, p. 335-348.

MORALES PRATS, F. Prólogo à obra de Esther Morón, *Internet y Derecho Penal: “hacking” y otras conductas ilícitas na red, Revista de Derecho y Proceso Penal.* Pamplona: Aranzadi Ed., n.º 1, 1999.

MORÓN LERMA, E. Internet y Derecho Penal: “hacking” y otras conductas ilicitas em la red. In: *Revista de Derecho y Proceso Penal,* Pamplona: Aranzadi Ed., n.º 1, 1999.

NEGROPONTE, N. *Vida digital.* 2ª ed. – Trad. de Sérgio Tellaroli. São Paulo: Companhia das Letras, 1999.

PÉREZ LUÑO, A. E. *Nuevas tecnologías, sociedad y derecho.* Madrid, 1987.

PRADEL, J., FEUILLARD, C. Les infractions commises au moyen de l’ordinateur. In: *RD pénal, crim.,* 1985.

QUEIRÓZ, R. M. S. de. Assinatura digital e o tabelião virtual. In: *Direito & Internet – Aspectos jurídicos relevantes,* Bauru-SP: EDIPRO, 2000, p. 371-418.

QUINTERO OLIVARES, G. (Dir.). *Comentários ao nuevo Código Penal*. Pamplona, 1996.

RIEFA, C. *Le consommateur et l’Internet.* Tese apresentada à Universidade de Montpellier I e Perpignan, sob orientação do Prof. Jean Calais-Auloy, 1997.

SILVA NETO, A. M. e. *Privacidade na internet: um enfoque jurídico*. Bauru, SP: EDIPRO, 2001.

TERCEIRO, J. B. *Sociedad digital,* Madrid*,*1996.

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO

Procurador-geral de Justiça
Luiz Antonio Guimarães Marrey

Corregedor-geral do Ministério Público
Agenor Nakazone

Conselho Superior do Ministério Público

Luiz Antonio Guimarães Marrey (presidente)
Agenor Nakazone
Antonio Hermen de Vasconcellos e Benjamin
Eduardo Francisco Crespo
Fernando Grella Vieira
Francisco Stella Júnior
José Benedito Tarifa
José Oswaldo Molineiro
Newton Alves de Oliveira
Paulo Hideo Shimizu
Walter Paulo Sabella

Órgão Especial do Colégio de Procuradores de Justiça

Membros Natos

Gomides Vaz de Lima Júnior
José Roberto Garcia Durand
Clóvis Almir Vital de Uzeda
Jobst Dieter Horst Niemayer
Guido Roque Jacob
Luiz Cesar Gama Pellegrini
Herberto Magalhães da Silveira Júnior
René Pereira de Carvalho
Francisco Morais Ribeiro Sampaio
Newton Alves de Oliveira
José Ricardo Peirão Rodrigues
Luiz Antonio Forlin
José Roberto Dealis Tucunduva
Eduardo Francisco Crespo
Oswaldo Hamilton Tavares
Fernando José Marques
Irineu Roberto da Costa Lopes
Regina Helena da Silva Simões
Antonio Paulo Costa de Oliveira e Silva
Roberto João Elias
Claus Paione
José de Arruda Silveira Filho

Membros Eleitos

Cyrdêmia da Gama Botto
Antonio Augusto Mello de Camargo Ferraz
Adelina Bitelli Dias Campos
Jethro Pires
Carlos Roberto Barreto
Paulo Álvaro Chaves Martins Fontes
Carlos Henrique Mund
Renato Nascimento Fabbrini
Geraldo Félix de Lima
Ruy Alberto Gatto
Maurício Augusto Gomes
Nelson Gonzaga de Oliveira
Luiz Claudio Pastina
Heloísa Antonia Barreiros de Souza
Antonio Ferreira Pinto
Rubens Rodrigues
Paulo Marcos Eduardo Reali Fernandes Nunes
Antonio Visconti
José Correira de Arruda Neto
Lúcia Maria Casali de Oliveira

Conselho do Centro de Estudos e Aperfeiçoamento Funcional

Luiz Antonio Guimarães Marrey
Agenor Nakazone
Renato Narcimento Fabbrini
Walter Paulo Sabella
Arthur de Oliveira Costa Filho
Silvana Buogo
Jocimar Guimarães
Luís Daniel Pereira Cintra