Alguns aspectos da informática e suas conseqüências no Direito

Paulo Sá Elias

advogado em São Paulo (SP)

Temos observado intenso e salutar debate na doutrina e na jurisprudência a respeito dos efeitos da informática no direito. É de notório conhecimento a importância da tecnologia em absolutamente todos os ramos da vida humana. As máquinas parecem tender a servir, cada vez mais, como elementos de ligação entre as pessoas.

Congressos e encontros sobre o assunto são realizados a todo instante. Em 1997, *v.g.*, no Rio de Janeiro, no I Congresso Nacional sobre a Internet, juristas de renome já discutiam a revisão de aspectos legais clássicos frente às novas situações jurídicas decorrentes da informática nos diversos campos do direito

brasileiro. Discutiam na ocasião a respeito da necessidade de que fossem repensados antigos dogmas jurídicos no intuito de adaptá-los a uma nova realidade. Como muito bem lembrado, na época, por *José Henrique Barbosa Moreira Lima Neto*, com o brilhantismo que lhe é peculiar: "A Internet é uma verdadeira praça pública, onde todos, independentemente de raça, cor e nacionalidade, tem direito ao uso da palavra. É a versão moderna da Ágora da Grécia Antiga".

Nas diversas áreas do direito brasileiro, estudiosos desenvolvem novos modelos para a legislação frente à tecnologia e suas inevitáveis conseqüências no mundo jurídico: novos tipos penais, novos tipos tributários (envolvendo discussões sobre alguns dos seus princípios fundamentais, como a territorialidade, o estabelecimento comercial e a competência, o *non olet* (cobrança dos rendimentos oriundos de serviços ilícitos), a subsunção tributária – *nullum vectigal sine praevia lege*), disposições sobre o direito autoral, sobre a responsabilidade civil, sobre o direito comercial no que diz respeito a cartularidade, literalidade e autonomia das obrigações cambiais frente às transações eletrônicas e magnéticas, etc. Por outro lado, e com prioridade, estudam os casos concretos para corretamente adequá-los ao sistema legal já existente e capaz de solucionar a grande maioria dos conflitos decorrentes.

Com o advento da Internet, novas condutas ainda atípicas surgem a todo instante. Nos Estados Unidos, o *Computer Fraud and Abuse Act ("CFAA")*, legislação criminal, atualmente, contém dispositivos para o combate ao acesso criminoso em computadores por via interna ou externa (*anti-hacking provisions)*. O *CFAA*, por exemplo, pune o usuário de computador que consegue o acesso não autorizado em sistemas de computadores.

Em 1984 o *CFAA* tipificou o acesso a computadores sem autorização e o uso ilegal das informações obtidas como crime. Foi o primeiro passo na luta contra os crimes cometidos na informática nos Estados Unidos. Em razão das críticas ao seu escopo limitado e incertezas do seu texto legal, o *CFAA* recebeu emendas em

1986, 1994 e 1996, aumentando seu campo de atuação. Foram criados três novos crimes, incluindo a disposição *anti-hacking* [seção – 1030(a)(5)]. Na oportunidade os usuários que acidentalmente, por erro, tivessem o acesso a rede de computadores (sem autorização) não seriam punidos. Segundo interpretação do texto legal em questão, a conduta do agente seria típica e antijurídica se, com dolo, tivesse o agente acesso a algum computador do governo ou de interesse federal e que tal conduta causasse danos.

No famoso caso *United States v. Morris*, um estudante do primeiro ano do programa de Ph.D em computação da *Cornell University, Robert Tappan Morris*, lançou um pequeno programa – "*worm"* – um "vírus" (programa malicioso, de má índole – com potencial de causar danos a terceiros) – que segundo suas alegações nos autos, teria o intuito de testar a capacidade de multiplicação do próprio programa; sendo certo que fora criado sem intenção de causar danos a ninguém. Ao observar que seus cálculos a respeito da taxa de multiplicação e os limites de abrangência do referido *worm* estavam equivocados, lançou na Internet um outro programa a fim de detectar e exterminar o "vírus". A solução foi demorada e causou problemas em diversos computadores dos Estados Unidos. *Morris* foi condenado.

É crime, naquele país, a conduta de transmitir programas direta ou indiretamente com propósito de causar danos. É citado na doutrina penal americana o exemplo da pessoa que envia um *e-mail* (correio eletrônico) a outra pessoa, sabendo que em *attachment* (anexo) a sua mensagem, encontra-se um "vírus" – *harmful program (warm)* e que se este "vírus" multiplicar-se pela rede, tal pessoa será punida por dolo eventual.

Desde 1984, com a entrada em vigor do *CFAA* nos Estados Unidos, o Congresso norte-americano repetidas vezes provocou alterações nos níveis do que eles chamam de *mens rea* necessário à adequação típica. Para os norte-americanos, dois elementos existem em todos os crimes: *actus reus* e o *mens rea*. O primeiro define a ação de um crime, ao passo que o segundo diz respeito ao "estado

mental" do agente. O *Model Penal Code (MPC)* dos Estados Unidos descreve 4 (quatro) níveis de *mens rea*, a saber: 1. *Purposely* (intencionalmente - dolo direto); 2. *Knowingly* (consciência); 3. *Recklessly* (imprudência, descuido – despreocupação no tráfego social) e 4. *Negligently* (negligência).

Tais categorias são divididas em requisitos (altos e baixos) – o nível mais alto inclui os atos criminosos realizados *intentionally* e *knowingly*, arrisco-me a pensar no nosso dolo natural, que é a espécie adotada pela teoria finalista da ação. O nível baixo inclui os atos criminosos realizados *recklessly* e *negligently* e os com *strict liability* (estrita responsabilidade). Os criminosos, segundo eles, possuem o mais alto nível de *mens rea* quando seu intento é mais específico (finalidade), sendo desta forma mais censuráveis. Acredito que tal divisão e subdivisão autorizam o questionamento da finalidade do agente, sendo impossível pensar na conduta como uma simples exteriorização de movimento ou abstenção de comportamento sem qualquer finalidade, como proposto na teoria clássica originada no tratado de *Franz von Liszt*.

Com essas diferentes categorias de *mens rea*, o Congresso dos Estados Unidos em razão do crescimento da Internet preocupa-se com a quantidade inacreditável de situações originadas em razão da comunicação através de computadores e similares. Lembram o pensamento de *Herbert Marshall McLuhan*, de que a "Internet é a coisa mais parecida com a verdadeira anarquia jamais criada". Os legendários *Steve Wozniak*, *Steve Jobs* e *William H. Gates III* (*Bill Gates*), já faziam, há mais de 20 anos, previsões a respeito das inúmeras conseqüências do desenvolvimento da informática na sociedade e no direito.

Alguns crimes cometidos na informática apresentam extrema complexidade em relação a questão probatória. O Procurador de Justiça, *Agamenon Bento do Amaral*, já escreveu um excelente artigo sobre o assunto. Existem, por outro lado, os casos em que se discute a aplicação das provas ilícitas por derivação – *The Fruits of the Poisonous Tree*.

Uma das questões principais atualmente discutida no âmbito jurídico está ligada aos invasores de sistemas de computador sem a devida autorização. O desdobramento natural da questão nos leva ao assunto: privacidade e segurança (que será abordado mais adiante).

Na atividade privada, nos Estados Unidos, estima-se perdas em torno de *USD 550,000,000.00* (quinhentos e cinqüenta milhões de dólares) por ano em razão dos criminosos da informática.

No Brasil, enquanto o Poder Judiciário se depara com ações relacionadas a multiplicação de "CD´s" falsos (cópias não autorizadas de discos de música (sem tocar no assunto do "*software*" ilegal / "pirata") – e as autoridades policiais diligenciam à procura dos referidos "CD´s", a distribuição das referidas músicas é realizada de forma muito mais moderna, barata, ilícita, ilimitada e assustadoramente através de MP3 *[VQF e outros novos formatos de compressão de som*] pela Internet.

Em 1987, o instituto *Fraunhofer-Gesellschaft* (com mais de 50 anos de existência) localizado em Munique na Alemanha, em parceria com o Prof. *Dieter Seitzer*, desenvolvia o projeto EU147 – Eureka (DAB) – *Digital Audio Broadcasting System,* nascendo daí um algoritmo matemático de compressão de dados em som chamado IS 11172-3 e IS 13818-3 - ISO-MPEG (*Moving Pictures Experts Group*) Audio Layer-3 – MP3.

Uma faixa de música de um CD (*compact disc*), com toda sua excelente qualidade sonora, normalmente é gravada em 44,1 kHz. É possível digitalizar a música de um CD (copiá-la para o computador) e transmiti-la pela Internet, por exemplo, como anexo de um *e-mail* ou colocá-la diretamente à disposição de quem quer que seja em servidores na rede. Ocorre que com os divulgados padrões de audio digital existentes até então, uma música com 4 (quatro) minutos de duração, consumia em média 10 (dez) milhões de *bytes* (*10MB*) para o seu armazenamento. É de se concluir portanto, que a transferência de um arquivo tão grande pela Internet, nas velocidades disponíveis nos computadores e nas

conexões à Internet da maioria dos usuários (principalmente no Brasil) tornava essa idéia desanimadora e sem a menor possibilidade de prosperar.

O MPEG *audio coding* – (o algoritmo/codificador MP3) encolhe o som original com qualidade de um CD (44,1 kHz) em até 12 vezes sem causar perdas significativas (audíveis ao ouvido humano) da música (ou som) em questão. O arquivo com mais de 10 milhões de *bytes* pode ser facilmente convertido para um arquivo (.mp3) com pouco mais de 1 a 2 milhões de *bytes*. Tal redução é significativa no que diz respeito ao tempo e a facilidade de transferência deste arquivo pela Internet.

Resultado: Milhares de músicas são colocadas à disposição na rede. O usuário escolhe as músicas de sua preferência, captura o arquivo (*download*) para o seu computador pessoal e a partir daí pode escutar as músicas com a mesma qualidade do CD original em seu computador pessoal, podendo ainda gravá-las em outros formatos, tais como: CD, DVD, DAT, etc.; elaborando um disco personalizado (com as músicas de sua preferência). É possível também, enviá-las a um dispositivo portátil compatível com MP3 (como um *walkman*) já disponível à venda no mercado. Tudo de forma gratuita e ilícita na maioria das vezes.

Algumas empresas já começam a vender licitamente "faixas de músicas" pela Internet em formato MP3. A questão dá origem a discussões de toda a ordem jurídica.

A segurança e a privacidade são temas importantíssimos atualmente. Em 1939, na *Universidade de Cambridge*, *M.G. Kendall* e *B.B. Smith*, tratavam do assunto da combinação aleatória de números. Em 1955, *Paul Armer*, *Bower*, *Bernice Brown*, *Frantz*, *Goodpasture* e outros trabalhavam no projeto "*A million random digits with 100,000 normal deviates – Rand Corporation"* – que também tratava do assunto. Ao longo dos anos a criptografia [*na informática*] (conjunto de princípios e técnicas de matemática, utilizando algoritmos e funções poderosas capazes de codificar uma mensagem, baseadas em grandes números primos com centenas de dígitos e outras técnicas de escrever em cifra) foi se desenvolvendo.

Uma combinação de dados aparentemente ininteligível é o resultado do processo da criptografia, ou seja, uma mensagem cifrada. Teoricamente é possível conseguir descobrir o conteúdo de uma mensagem criptografada, através da criptoanálise (princípios, métodos e meios para se chegar à decriptação de uma mensagem, som, imagem, arquivo, etc. (criptografado), sem prévio conhecimento dos códigos ou cifras empregados na sua produção).

As hipóteses são, por exemplo, a citada criptoanálise da quantidade de variantes, fatoração e complexidade do algoritmo utilizado na mensagem cifrada com a utilização de cálculos de computação matemática de alto nível, através do chamado *brute force attack* - "ataque de força bruta" ao conteúdo secreto.

Sabe-se igualmente das hipóteses de *softwares* com a função de criptografar mensagens que possuem falhas de proteção ocultas – (*back doors)*, propositadamente colocadas por seus programadores e/ou por determinação legal, a fim de permitir o acesso ao conteúdo secreto gerado por aquele programa.

O *IDEA – International Data Encryption Algorithm* (algoritmo de criptografia) desenvolvido em Zurich, Suíça, por *Xuejia Lai* e *James Massey* é teoricamente de segurança absoluta. Não há qualquer avanço na criptoanálise hoje, capaz de descobrir o conteúdo criptografado pelo referido algoritmo. [*Já se discute, em tese, a possibilidade de abordagens computacionais de última geração – capazes de realizar tais cálculos com extrema facilidade – Neste contexto, é interessante conhecer os novos paradigmas de processamento de dados trazidos pela computação óptica – C.f. Donald Frazier, Hossin Abdeldayem, Mark S. Paley e William K. Witherow do Marshall Space Flight Center (NASA) – Estados Unidos (Recent advances in photonic devices for optical computing) – Computação Quântica*].

Sabe-se que a criptoanálise com as teorias matemáticas atualmente conhecidas neste campo, é o método mais demorado para se decifrar o conteúdo de uma mensagem criptografada. Cálculos do ataque de força bruta ao algoritmo já foram estimados e chegou-se a conclusão de que seriam necessários 1 milhão de

computadores, tentando 1 milhão de chaves/"senhas" por segundo, durante a idade conhecida do universo para se conseguir decifrar o conteúdo criptografado. Conclui-se, portanto, que até onde, atualmente, encontra-se a tecnologia e o conhecimento da matemática, a teoria dos números e a capacidade dos supercomputadores, pode-se pensar na impossibilidade de se quebrar a segurança da mensagem ou conteúdo criptografado com tal algoritmo.

O mais conhecido e utilizado *software* de criptografia atualmente é o *PGP – Preety Good Privacy*, desenvolvido originariamente por *Philip R. Zimmermann* em 1991. O algoritmo de criptografia utilizado no *PGP* é o *IDEA* (referido acima) e o *RSA* (*Rivest*, *Shamir and Adleman*). O *software PGP* possui seu código de programação "aberto" – ou seja, é possível verificar a inexistência de *backdoors.*

O *ITAR – International Traffic in Arms Regulations* do Estados Unidos controla a exportação de munições de uso exclusivo das forças armadas norte-americanas, incluindo componentes de aeronaves militares, armas químicas e biológicas e por incrível que pareça, os *softwares* de criptografia. *Zimmermann* passou três anos sendo processado criminalmente a respeito da distribuição do *software PGP* como *freeware* (distribuído gratuitamente) ao resto do mundo.

Atualmente é expressamente proibida (1) pela legislação de exportação dos Estados Unidos (ITAR / *US Export Regulations*) a saída do *PGP* do território daquele país sem prévia licença legal. As penas para os infratores são severas e altíssimas. [*A exportação foi autorizada no final do ano de 1999, com restrições*]

Porém, em razão de uma falha do legislador norte-americano, a restrição imposta a exportação de *softwares* de criptografia abrange apenas o *software* em sua forma eletrônica (*v.g.*, em discos, CD-ROM, via Internet, etc.). Desta maneira, foi possível exportar legalmente o *PGP* para a Europa através da transcrição de todo o seu código fonte (seu código de programação) impresso em livros. Atualmente são 12 livros e mais de 6.000 páginas.

Os livros saíram legalmente dos Estados Unidos de acordo com tais regras de exportação sendo que, posteriormente, tais páginas foram colocadas em um "*scanner*" para reconhecimento óptico dos caracteres (*OCR*) retornando-os, novamente, à forma digital. Divulga-se que mais de 70 pessoas especializadas em toda a Europa trabalharam por mais de 1.000 horas para tornar a versão internacional do *PGP* legal e possível. A atual versão internacional do *PGP* - 6.0.2.i, encontrada e utilizada no Brasil, é absolutamente lícita para ser utilizada fora dos Estados Unidos na medida em que nenhuma linha de código de programação do *software* foi exportada eletronicamente.

A importância da criptografia reside no fato dela permitir a privacidade e a segurança do tráfego de informações na forma eletrônica, principalmente através da Internet. Por outro lado, como citado no início, o governo norte-americano tem demonstrado preocupação com o uso da criptografia por criminosos, determinando que seja possível ao governo, em determinadas hipóteses, ter acesso ao conteúdo critografado de alguma mensagem.

A invasão dos computadores pessoais passa por um dos momentos de sua maior plenitude, principalmente no Brasil. Semelhante a um antigo *software* de administração remota à distância de computadores, chamado *Carbon Copy*, *Hackers* (2) desenvolvem e colocam à disposição de quem se interessar, diversos e pequenos programas com semelhantes características de controle à distância. Os mais conhecidos são: o *Back Orifice* (*Cult of Dead Cow* – [*Phrozen Crew – aux. Divulgação]*) e o *NetBus* (*Carl-Fredrik Neikter*).

Como se fossem um "vírus" *trojan horse* (cavalo de tróia), tais programas são distribuídos pela Internet de forma direta ou indireta (ocultamente); em regra são encontrados junto a outros *softwares*, imagens, *e-mail´s*, etc. Quando o usuário tem o seu computador "infectado" com tal *software*, possibilita ao *hacker* (ou a qualquer pessoa comum que tenha o referido programa) o acesso ao conteúdo das informações disponíveis no computador da vítima.

É possível a captura de documentos produzidos em processadores de texto (tais como: defesas, denúncias, sentenças), planilhas de cálculo, leitura de *e-mail´s* privativos, dados pessoais confidenciais, senhas (descobertas através do que eles chamam de *keystroke recorder*), etc.

Quando se utiliza a Internet, rastros ocultos e expressos são deixados em diversas formas e em diversas partes do sistema. É possível, com a coleta dessas informações em um dado período de tempo, por análise estatística e comparação, traçar os pessoais interesses do usuário (suas preferências de conteúdo acessado na Internet (quais as páginas e que tipo de páginas recebem sua maior atenção), conteúdo de correios eletrônicos, imagens, audio e outras coisas mais).

As opções de proteção à vítima, no campo da tecnologia, estão ligadas à criptografia (*v.g.*: os *softwares PGP, PGP phone*, *PGP disk*), *firewall* (parede de fogo) - proteção da rede interna de um sistema de computadores contra invasões e outras técnicas de segurança. [*Cf. Biometrics – Sistema de Segurança verificador de traços físicos das pessoas – estrutura facial e impressões digitais* -].

O legislador brasileiro deve acelerar seus estudos a respeito da criação de uma legislação específica a respeito da privacidade no mundo da informática, em especial nas comunicações via Internet. Em relação a proteção de dados pessoais, na Grécia, *v.g.*, foi aprovada uma lei a respeito em 19.03.1997, na Itália em 08.05.1997. "Com tal legislação, a Itália habilitou-se a fazer parte plenamente da comunidade dos Estados de *Schengen*, superando as dificuldades que durante anos a afligiram, exatamente pela falta de uma lei sobre a proteção dos dados. A entrada em vigor da lei sobre a proteção dos dados, autorizou a Itália fazer parte da Central Européia de Polícia, a *Europol*, instituída pelo Tratado de *Maastricht* de 1991".

Discussões em torno da viabilidade e da validade de documentos judiciais e extrajudiciais transmitidos via Internet, com a utilização da criptografia (funcionando como assinatura digital) são interessantes e podem retratar um futuro não muito distante.

Na área financeira encontramos referência ao *First Virtual Bank* (trabalhando a partir de conceitos do processo bancário tradicional aplicados ao mundo *online* da Internet). Fala-se das transações seguras via cartão de crédito (*STT – Secure Transaction Technology*). Também do *Cybercash*, do SEPP (*Secure Eletronic Payment Protocol*) e do *e-cash* (dinheiro virtual com lastro no capital disponível na conta corrente real do usuário). [*Ref. SET – Secure Electronic Transaction*]

As empresas com base em dados pessoais dos usuários coletados na rede, dirigem sua publicidade para os que possuem maior propensão a consumir os produtos que tenham a oferecer.

Atualmente [*este artigo foi escrito no início de 1999*], nos Estados Unidos, por exemplo, se discute no Poder Judiciário a questão das *Meta Tags* (são palavras embutidas no código *HTML* (que formam as páginas na Internet) e que são ocultas para os usuários comuns, mas que são encontradas pelos sistemas de procura (*search engines*) e seus classificadores de conteúdo).

Determinados concorrentes utilizam as *Meta Tags* para divulgarem suas páginas comerciais na Internet com palavras-chave que possam orientar os sistemas de procura a encontrá-los com prioridade quando determinado usuário (consumidor) estiver à procura de produtos de sua comercialização (mesmo que sejam, especificamente, o produto dos seus concorrentes). A questão central em debate é saber se o concorrente, na sua página comercial, poderá ou não, usar a marca (*trademark*) do seu concorrente através de *Meta Tags* em páginas na Internet.

Recentemente uma importante decisão do Tribunal da Califórnia, em São Francisco, nos Estados Unidos, pareceu tornar a questão pacífica. O caso é o *Brookfield Communications Inc. v. West Coast Entertainment Corp.* Foi decidido que a utilização da marca do concorrente em *Meta Tags* confunde o interesse e decisão inicial do consumidor. Segundo os advogados da autora, com tal decisão o "seqüestro virtual" de consumidores pela Internet tende a diminuir.

Em relação a reprodução não autorizada de obras pela Internet, discute-se ainda a questão do lucro indireto, "do domínio público das obras publicadas (pela Internet) fisicamente localizadas em países que não participam dos tratados a que tenha aderido o Brasil, e que não confiram aos autores de obras aqui publicadas o mesmo tratamento que dispensem aos autores sob sua jurisdição". Discute-se a questão do *Fair Use* (o propósito educacional e não lucrativo de utilização da obra, com respeito à sua natureza jurídica, quantidade, substancialidade e efeitos).

Em um excelente artigo publicado na revista de administração de empresas da FGV/SP – Fundação Getúlio Vargas de São Paulo em 1990, *A.C. Mattos* traduziu *Tom Forester* (Griffith University, Australia) e *Perry Morrison* (University of New England, Australia) no assunto: "A insegurança do computador e a vulnerabilidade social".

Diziam com absoluta razão, *Forester* e *Morrison*, que a medida que a sociedade se torna mais e mais dependente de computadores, telecomunicações e novas tecnologias, também se torna mais vulnerável às suas falhas e inseguranças.

Exemplos interessantíssimos, na época, foram relatados: "Em 1986, em Chicago, nos Estados Unidos, um funcionário da Enciclopédia Britânica, descontente por ter sido dispensado do emprego, acessou o banco de dados da editora e fez pequenas alterações no texto que estava sendo preparado para ser impresso da nova edição da renomada obra, como por exemplo, trocando o nome de *Jesus Cristo* por *Alah*, colocando o nome dos executivos da editora em situações bizarras e outras condutas danosas".

"O foguete *Atlas-Aegena*, lançado do *Cabo Canaveral* nos Estados Unidos em direção a Vênus, teve que ser explodido, depois de ficar completamente sem controle em razão da ausência de um hífen (-) nas linhas de programação do seu *software* de controle de vôo".

Já em **1978**, segundo *Forester* e *Morrison*, os suecos publicaram um relatório sobre a vulnerabilidade da sociedade informatizada, onde foram listadas 15

(quinze) fontes de vulnerabilidade, incluindo atos criminosos. Diziam ainda que os computadores são inerentemente inconfiáveis devido a duas razões principais: primeiro, são propensos a falhas catastróficas; e, segundo, sua grande complexidade garante que não possam ser exaustivamente testados antes de serem liberados para uso.

Fundamentaram com absoluta razão, da seguinte maneira: "Computadores digitais são dispositivos de estados discretos, isto é, utilizam representações digitais (binárias) dos dados e instruções (*softwares*), de modo que um programa de computador pode efetivamente "existir" em literalmente milhões ou mesmo bilhões de estados diferentes. Assim, cada mudança em uma variável (e alguns programas tem milhares de variáveis com milhares de valores cada uma) efetivamente alteram o estado do sistema. Cada dado introduzido ou emitido, acesso a disco, solicitação para imprimir, conexão a modem, ou cálculo – de fato, qualquer coisa em que o sistema possa estar envolvido, altera o estado no qual o sistema existe. A multiplicação de todos esses estados, e também outros relevantes (hora do dia, sistema em sobrecarga, combinação de tarefas em andamento, *invasão do sistema, vírus,* etc.), um pelo outro, resultará no número de estados possíveis nos quais o sistema poderá existir.

O problema dos computadores digitais é que cada um desses estados representa uma fonte de erro em potencial. Sistemas analógicos, ao contrário, tem um número infinito de estados – são na realidade contínuos, no sentido de que, digamos, um botão de controle de volume de um rádio ou uma tira bimetálica usada em um termostato pode tomar um número infinito de posições dentro de certa faixa, da mesma forma que uma régua possui um número infinito de pontos. A diferença real, entretanto, é que, enquanto que o movimento contínuo do botão do rádio dificilmente terá uma falha de grandes proporções, nossa máquina de estados discretos pode falhar de uma maneira catastrófica, porque a execução de cada estado depende de estar o estado anterior "correto", ou seja, ter atingido o objetivo computacional que o programador esperava conseguir. Se o estado anterior não estiver correto, ou mesmo impedir que a próxima instrução seja

executada, então o programa irá falhar. Programadores honestos admitem ser impossível escrever um programa complexo livre de erros".

As técnicas existentes na engenharia de *software* e *hardware* estão evoluindo muito, é bem verdade, e nem se discute aqui, por impertinente, que a tecnologia digital, apesar das suas peculiaridades de risco é infinitamente superior a tecnologia analógica. O cerne do problema está ligado aos aspectos de desenvolvimento da sociedade, dos meios de comunicação e das inúmeras possibilidades ainda atípicas, desconhecidas e não protegidas pelo sistema legal, oriundas dos avanços da tecnologia.

Os autores em questão discutiam na época que os programadores e engenheiros de *software,* quando solicitados a construir sistemas que continham aplicações com risco de vida, fossem mais honestos sobre os perigos e as limitações no campo da informática. Discutiu-se corretamente a respeito da responsabilidade civil objetiva em razão da atividade potencialmente perigosa.

Deram um exemplo preocupante: "Em março de 1986, um paciente chamado *Ray Cox* visitou uma clínica em Tyler, Texas, Estados Unidos, para receber um tratamento por radiação nas costas, de um onde um tumor maligno havia sido extraído. O tratamento normalmente é indolor, mas naquele dia o paciente recebeu a marca de um duro golpe. Técnicos intrigados, que estavam do lado de fora da sala de terapia, observaram que o computador que operava o equipamento estava fazendo piscar a mensagem "Falha 54", mas não conseguiam saber do que se tratava.

Na realidade, o paciente havia recebido, pela falha do sistema eletrônico, uma dose fatal de radiação e cinco meses após, estava morto. Em menos de 1 mês da morte deste paciente, uma senhora de 66 anos, *Vernon Kidd*, morreu em 30 dias em razão da mesma "Falha 54" no equipamento.

O equipamento em uso no Centro de Tratamento de Câncer em Tyler, Texas, Estados Unidos, na época, era o acelerador linear *Therac-25*, controlado por

computador". Segundo os autores, máquinas iguais ou semelhantes estavam em uso em 1.100 clínicas nos Estados Unidos, administrando terapia por radiação a 450.000 novos pacientes por ano.

É evidente que jamais poderemos nos distanciar na informatização e da alta tecnologia. Teremos que recebê-la de braços abertos. Não se pode negar que o distanciamento das inúmeras facilidades e vantagens da tecnologia, podem levar o indivíduo a um certo desajustamento na atual conjuntura. Em nossa área jurídica, são incontáveis os exemplos de facilidade, como a possibilidade da transmissão de petições, informações, jurisprudência e outros dados pela Internet ao computador, ao (*laptop* / *notebook*) do advogado, do magistrado, do promotor de justiça, enfim, dos operadores do direito em qualquer lugar que estejam, *v.g.*, em viagens, na própria sala de audiências, em palestras ou em congressos.

Citamos, por exemplo, o projeto pioneiro da *EPM – Escola Paulista da Magistratura do Estado de São Paulo*, ao veicular cursos específicos aos magistrados pela Internet (através da tecnologia *real audio* e *real video*) possibilitando aos mesmos, assistirem aulas gravadas anteriormente (som e imagem) ou até mesmo ao vivo. A editora *RT – Revista do Tribunais*, que pioneiramente, lançou na Internet a possibilidade da consulta a todo seu acervo de jurisprudência, tornando também possível, a atualização imediata *online* dos códigos Civil, CPC, Penal, CPP, Comercial, Tributário e Constituição Federal.

É de se notar, portanto, que não faltam argumentos para estarmos atualizados em relação ao desenvolvimento tecnológico da humanidade e que devemos estar prontos a lutar por uma legislação e uma interpretação moderna (se necessárias), que possam proteger nossa sociedade das inúmeras e novas conseqüências jurídicas oriundas da tecnologia que se moderniza diariamente; não sendo demais lembrar, no entanto, que a liberdade do legislador deve encontrar o seu limite na razoabilidade. É imprescindível verificar se existe algum fundamento, alguma razão objetiva para a intervenção do legislador.

Lembro-me de um oportuno comentário de *Ives Gandra da Silva Martins*, em relação a constituição federal e que neste momento, pedindo licença para parafraseá-lo e adaptar seu pensamento ao contexto deste artigo, nos autoriza a dizer que uma legislação não pode ser interpretada como se tivesse sido elaborada para que o país não evoluísse. A interpretação admite que, pelo espectro do texto legal, se retirem as diretrizes exegéticas necessárias para que perenidade da norma permaneça nas gerações futuras. As leis não são feitas para amarrar o país à época de sua edição, mas para orientar o presente e o futuro da nação, dentro de princípios considerados fundamentais para o bem da pátria e da sociedade.

O Poder Judiciário quando se depara com situações inusitadas, oriundas das conseqüências da informática e da atual tecnologia no direito e na sociedade, pode, na maioria das vezes, tranqüilamente, proferir justa decisão sem a preocupação de lacuna ou obscuridade da lei, na medida em que é possível, como sabido de todos, a possibilidade da aplicação de regra válida para hipótese semelhante e da utilização de pareceres técnicos fornecidos por peritos da área de informática no auxílio a formação do convencimento do magistrado.

Como bem lembrado pelo Ministro *Sepúlveda Pertence*, em julgamento realizado em 22.09.1998, *HC-76689/PB - STF*: "não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia, uma vez que se compreenda na decisão típica da conduta criminada; o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal – a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial".

Devemos estar cientes da ampla possibilidade da tutela jurisdicional, quer utilizando de normas legais já existentes há muito tempo em nosso ordenamento

jurídico, que diga-se de passagem, são em diversas hipóteses, absolutamente pertinentes e adaptáveis aos novos casos concretos surgidos em razão da informática, quer através da analogia e do incentivo ao trabalho legislativo específico, quando inevitáveis. Ao mesmo tempo, julgo importante lembrar, que devemos dirigir nossas atenções ao andamento dos "equivalentes jurisdicionais", em especial da arbitragem, que em certos momentos, teoricamente, parece impedir às partes, o acesso a um tratamento jurisdicional adequado.

Encerro lembrando a brilhante anotação de *Platão* (na *República*), citada pelo eminente Prof. *Sidnei Agostinho Beneti*, em seu livro: "*Da Conduta do Juiz*" – "A justiça está em cada um dos componentes da sociedade exercer corretamente sua função. Isso só já é justiça, já é atuação social".

NOTAS

(1) Nota de Atualização: Recentemente o governo dos Estados Unidos autorizou a exportação dos softwares de criptografia com algumas restrições.

(2) *Hackers:* indivíduos com grande habilidade e conhecimento de informática. Podem utilizar seu extraordinário conhecimento na área para atividades lícitas ou para atividades criminosas, em especial a invasão de sistemas de computadores, criação de vírus, etc.

BIBLIOGRAFIA

BENETI, Sidnei Agostinho. *Da Conduta do Juiz*. São Paulo: Saraiva, 1997.

BRANDENBURG, STOLL, et al. In: *The ISO/MPEG-Audio Codec: A generic standard for coding of high quality digital audio*. (Internet). Germany: Fraunhofer-Gesellschaft, 1992.

CASTRO, Clarice Marinho Martins de. In: *Nome de domínio na Internet e a legislação de marcas*. (Internet). Rio de Janeiro: I Congresso Nacional de Internet, Software & Direito, 1997.

COSTA, Marco Aurélio Rodrigues da. In: *Crimes de Informática*. (Internet). Rio Grande do Sul: 1998.

FLINN, Bill., HERMANN, Maurer. In: *Levels of Anonymity*. New Zealand, Auckland. Austria, Graz: Computer Science Department – University of Auckland – Institute for information processing and computer supported new media – Graz University of Technology, 1999.

FORESTER, Tom., MORRISON, Perry. In: *A insegurança do computador e a vulnerabilidade social*. (Australia: University of New England: Futures, 462-474). Tradução de A. C. Mattos, Departamento de Informática – FGV/SP – Fundação Getúlio Vargas, São Paulo: Revista de Administração de Empresas, 1990.

HONG, Haeji. In: *Hacking through the Computer Fraud and Abuse Act*. United States of America, California: The Regents of the University of California, 1998.

KAPLAN, CARL. S. In: *Court Lays Down the Law on Labels (Meta Tags) for Web Sites*. (Internet). United States of America: The New York Times (CLJ), 1999.

LIMA NETO, José Henrique Barbosa Moreira. In: *Aspectos Jurídicos do Documento Eletrônico*. (Internet). Rio de Janeiro. 1998.

LIMA, GEORGE MARMELSTEIN. In: *A reprodução não autorizada de obras literárias na Internet*. (Internet). Universidade Federal do Ceará. 1998.

LOSANO, MARIO G. In: *A lei italiana sobre a proteção dos dados pessoais*. Trad. Marcela Varejão. Italia: Università Degli Studi di Milano, 1997.

MARTINS, Ives Gandra da Silva. In: *A imunidade do livro eletrônico*. São Paulo: Jornal o Estado de São Paulo (14/09), 1998.

PARK, John. In: *Protecting the core values of the First Amendment in an age of new technologies: scientific expression vs. National Security*. United States of America, Virginia: University of Virginia Journal of Law and Technology, 1997.

STUBER, Walter D., FRANCO, Ana Cristina. In: *Internet sob a ótica jurídica*. (Internet). 1998

Fonte:

http://jus2.uol.com.br/DOUTRINA/texto.asp?id=1762

Acesso em 29/05/2009