UNIVERSIDADE FEDERAL DE SANTA CATARINA
Aires José ROVER, professor
http://infojur.ufsc.br/aires

PALESTRA NO CONSELHO DA JUSTIÇA FEDERAL

Direito, sociedade e informática: internet, riscos e acidentes

RIOGRANDINO TABAJARA BARBOSA ALVES BRANCO
Mestre-de-Cerimônias

Senhoras e senhores, boa-noite!

Daremos início à Conferência sobre Direito, Sociedade e Informática, a ser proferida pelo Dr. Aires José Rover, evento promovido pelo Centro de Estudos Judiciários do Conselho da Justiça Federal, com o apoio do Superior Tribunal de Justiça.

O Dr. Aires José Rover é formado pela Universidade Federal de Santa Catarina e Professor Adjunto do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina; atua nas áreas de Informática Jurídica, Tecnologia da Informação e Engenharia do Conhecimento Jurídico, Inteligência Aplicada, Inteligência Artificial e Direito, Comércio Eletrônico, Documentação e Processo Digital: Validade Jurídica; atualmente, leciona Direito, Informática e Sociedade na Universidade Federal de Santa Catarina; possui várias obras e artigos publicados, dentre eles "Organização do Livro", "Direito, Sociedade e Informática: Limites e Perspectivas da Vida Digital" e parte do livro "Introdução aos Sistemas Especialistas Legais: Dificuldades acerca do Sistema Jurídico".

Convidamos o palestrante para dar início ao tema desta noite, que será: "*Internet*, riscos e acidentes, formas de controle e métodos criptográficos de segurança".

Com a palavra o Dr. Aires José Rover.

AIRES JOSÉ ROVER
Professor Adjunto do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina

Agradeço ao Sr. Ministro Ruy Rosado de Aguiar, que me fez o convite quando fizemos uma visita a Brasília. Gostaria também de agradecer ao Conselho da Justiça Federal pela realização deste evento, tornando possível a nossa participação na presença de tão importantes pessoas, tanto ministros como amigos que trabalham na Justiça. É uma honra muito grande estar aqui.

Passarei diretamente ao assunto.

Trabalharemos com o tema "*Internet*, riscos e acidentes, formas de controle e métodos

criptográficos de segurança". Hoje, nos concentraremos um pouco mais na segurança da informação. O tema relativo ao segundo dia de palestra, "Documentos digitais, contratos e comércio eletrônicos", também perpassa pela questão da segurança, na medida em que há uma série de problemas em relação aos documentos digitais e, naturalmente, soluções a partir deles.

A imagem do *slide* mostra um pouco como as coisas funcionam; encontrei-a na *Internet*, onde circula todo tipo de informação: desde imagens que nela não deveriam estar até as mais criativas, como essa, na qual o indivíduo, que não dispõe de dinheiro para comprar um *notebook*, faz do seu *desktop* uma ferramenta. É uma alegoria que nos mostra como a Informática está presente no nosso dia-a-dia de modo estranho e não muito amigável.

Como professor, não posso abordar assuntos técnicos, introduzindo a temática sem uma base teórica e um pouco filosófica. Vivemos uma realidade em que a sociedade está passando por uma transformação gigantesca diante da evolução da tecnologia e da própria sociedade, em todos os ângulos, o que causa, de certa forma, algum desconforto. Uma série de problemas que estão ocorrendo nos marcam profundamente, principalmente porque, como vivemos em uma sociedade globalizada e conectada, no mínimo, pela televisão – apenas 8% ou 9% da população brasileira usam a *Internet*, mas quase a totalidade assiste à televisão, com exceção de uma minoria composta de pessoas mais pobres do interior, talvez até pela falta de energia elétrica –, a maioria dos brasileiros está consciente do que está acontecendo.

Efetivamente, para esses problemas não há solução. É uma questão de evolução, e Tom Peters apresenta dois princípios interessantes, também alegóricos, que demonstram que a eles devemos estar ligados: o SDS (só Deus sabe) o que acontecerá, porque o futuro não nos pertence, a evolução em todos os âmbitos é muito grande, e a ciência, por mais precisa, não consegue prever o que virá, de maneira clara e objetiva, apesar de existirem condições de permear, controlar e eliminar esse risco; e o PSP (pesquisar sem parar) é o antídoto do SDS: se só Deus sabe o que acontecerá no futuro com a nossa atividade do dia-a-dia, com o nosso emprego, com os nossos filhos, convém pesquisarmos sem parar, estudarmos permanentemente – e, por isso, parabenizo esta Casa, porque qualquer órgão, empresa ou setor que não estiver investindo em educação, reeducação e realimentação do processo de pesquisa e estudo, estará perdendo tempo.

Neste *slide,* mais uma brincadeira, mostrando que os perigos vêm de todos os lados.

De maneira genérica, existem alguns riscos gerenciais:

– perdas financeiras resultantes de fraudes, que normalmente não se contabilizam (em alguns países, a contabilidade gira em torno de 25%, 30%);

– roubo de informação confidencial - com o uso da Informática esse é um risco permanente;

– perda de oportunidade de negócio é algo elementar, como obtenção de informação privilegiada de uma empresa qualquer, fazendo-a perder a oportunidade;

– uso desautorizado de recursos - as empresas deixam recursos informáticos disponíveis e seus funcionários os utilizam para usos não autorizados, o que vem ocorrendo em todos os órgãos. Como solucionar esse problema? Simplesmente proibindo com um decreto, uma lei, ou uma regra interna? Evidentemente que não. É claro que há a necessidade de uma norma, mas também de educação, mostrando que, efetivamente, o recurso é caro e deve ser utilizado para o fim para o qual foi pago e montado;

– perda do respeito/confiança do consumidor - hoje, isso é fundamental, porque o consumidor é o centro de tudo. O cidadão - em sentido genérico - é o "consumidor" da Justiça. Se ocorrer qualquer tipo de problema em termos de gerenciamento de informações, é possível a perda da credibilidade por parte do Tribunal, da Justiça. Temos que tomar muito cuidado para que isso não aconteça;

– custos diversos associados às incertezas - vão se agregando em diferentes momentos do processo, sendo difícil contabilizá-los;

Em relação aos documentos, há um fluxo normal em um documento que sai de A para B, mas existem diversos casos de ameaças. Os sistemas de criptografia e de assinatura digital visam, exatamente, eliminar a possibilidade de que esses casos venham a ocorrer:

– a interrupção quando se envia um *e-mail* que não chega;

– a intercepção, quando alguém toma ciência do seu conteúdo;

– a modificação, quando alguém o modifica, encaminhando-o;

– a fabricação, quando alguém "faz de conta" que é outra pessoa que está enviando um *e-mail.* Quando falarmos em criptografia, veremos todas essas ameaças.

Estes são mais alguns exemplos de ameaças de segurança:

– cartão de crédito - 5 bilhões de dólares por ano;

– roubo de informações **on-line** - 10 bilhões;

– comprometimento com a segurança da informação - 50% das organizações têm problemas com essa falta de gerenciamento, de cuidado ou de alguma quebra no processo de gerenciamento da informação. Naturalmente, essa é uma estatística da década de 90. Já se vão três anos, e os sistemas estão evoluindo muito; muitas empresas passaram a utilizar fortes processos de gerenciamento de informação, mas, normalmente, o que acontece, por exemplo, em relação à *Internet,* é o seguinte: a *Web* surgiu em 1984/1985 nos Estados Unidos e, em 1986, no Brasil, quando as empresas a descobriram como um espaço legal para investir. Investiram, então, em um *site*, pois a

preocupação era apenas com a ocupação de espaço, o que durou um ou dois anos. Em um segundo momento, as empresas já estavam na *Internet*, inteiradas, de certa forma, com os consumidores, o que fez com que houvesse uma preocupação estética de melhoria do *site*, que durou um ou dois anos. A preocupação com a segurança - vejam que estamos falando de empresas da *Internet*, ou seja, de comércio eletrônico - surgiu em terceiro e último lugar, depois que os *hackers* começaram a atacar. A questão da segurança não era vista, normalmente, como algo relevante há dois ou três anos.

Falar em segurança parece elementar, mas não é. Não se têm exemplos de grandes tragédias relacionadas a esse tipo de gerenciamento de informação, mas, à medida que o sistema aumenta, as pessoas, pelo menos as que gerenciam, devem ter consciência da importância da segurança; caso contrário, estarão agindo dolosamente.

Quero enfatizar uma contra-ação, exemplo de ameaça de segurança. Se perguntasse aos senhores qual o maior inimigo, o maior problema em termos de ameaça aos sistemas de informação, a maioria responderia que são os *hackers,* porque sempre aparecem na mídia e fazem qualquer coisa, o que já é um estardalhaço - *hackers* brasileiros entraram na Nasa e o tráfego naquele *site* foi cortado por um período. Surge, então, um tipo de aura, de nuvem, de que os *hackers* são os grandes bandidos. Na realidade, assim como os vírus que adquirimos ao longo da vida nos dão imunidade para futuras doenças, os *hackers,* no caso dos sistemas de informática*,* desempenham o papel de mostrar à sociedade, às empresas, aos órgãos, a vulnerabilidade dos sistemas, e que, portanto, há a necessidade de se fazer alguma coisa; afinal de contas, viver em um mundo puro, límpido, livre de vírus é impossível, algo que não existe na natureza, e da natureza é a existência desse tipo de contra-ação; portanto, não sou inimigo deles e, em princípio, penso não representam um grande problema.

A grande ameaça de segurança é o ex-empregado do setor privado, porque, além de descontente, tem a informação privilegiada e pode cometer algum tipo de ação, causando danos à empresa, como perda da credibilidade e, até mesmo, de milhões de reais ou de dólares. Com relação ao ex-empregado dos órgãos do Governo, até que não se trata de uma questão relevante, porque normalmente não são despedidos a qualquer momento.

Também temos como ameaças de segurança:

– representante de vendas - dizer que representa todo o Brasil e não somente São Paulo;

– estudante - alterar/mandar *e-mail* divertido em nome de outros;

– contador - desviar dinheiro de uma empresa;

– corretor - negar uma solicitação feita a um cliente por *e-mail*;

– inimigo - aprender o poderio militar de um inimigo.

Excesso e irrelevância de informação. Trata-se de um processo crucial que os organismos têm de administrar, porque causa fadiga e angústia tecnológica. Quem não se sente angustiado por não ter lido as últimas notícias da sua área ou o último livro divulgado pela *Internet*, do qual se tem conhecimento, mas a ele não se tem acesso? E não se trata apenas de um livro, mas de dezenas, centenas.

Na *Internet*, efetivamente, o que mais existe é informação, em todas as áreas, e sabemos que isso causa uma angústia muito grande. Trabalho com alunos e percebo isso; não penso que seja diferente com uma empresa, no seu dia-a-dia. Não me recordo agora do nome do autor que falou em ignorância controlada ou gerenciada, ou seja, temos que ter consciência de que há um nível de ignorância comum a todos e convivermos com ele. Aliás, essa é uma questão cultural, porque a nossa geração não está preparada para administrar uma quantidade tão grande de informações, mas as novas gerações sim, porque sabem que têm que pegar o que for relevante naquele momento, naquele dia, naquele final de semana ou naquela semana, construindo a vida, no dia-a-dia em termos de busca dessas informações. Infelizmente, como não temos esse anticorpo em relação ao excesso de informação e à irrelevância - o que é pior -, temos que gerenciar, além do excesso, a informação que, em princípio, parece interessante, fazendo-nos gastar uma energia já escassa para, ao final, descobrirmos ser irrelevante, o que é terrível no gerenciamento de informações. Em função desse problema, as pessoas estão tentando construir sistemas mais inteligentes, por isso o uso de inteligência artificial, que foi inclusive minha tese de doutorado: a tentativa de procurarmos fazer com que haja um robô, por assim dizer, que faça essa pesquisa, trazendo apenas as informações relevantes e dentro de um limite determinado.

Existe também o isolamento social, a *infowar* (guerra da informação), o ciberterrorismo, a espionagem digital, a insegurança nacional, a insegurança dos sistemas, a pirataria, o vírus (invasão de sistemas, *spam*), a invasão de privacidade, tudo é digital.

Desses itens, falarei apenas no que diz respeito à insegurança dos sistemas, sobre o qual tenho um vídeo para apresentar. Cito também o exemplo da transmutação da fita cassete para o modelo digital, a fim de demonstrar a transformação da tecnologia, pois a humanidade sempre viveu com ela, desde os primeiros tempos. O que diferencia os tempos da revolução industrial, por exemplo, dos atuais é a adoção maciça da tecnologia digital, mudança da qual não temos muita consciência, pois nos pega de uma hora para outra, dando saltos imensos.

Existem dois modelos de tecnologia: o analógico e o digital. A tecnologia analógica, de alguma maneira, faz analogia à natureza. O dia é dividido em 24 horas, e temos um relógio com 24 pontos, que é uma representação analógica do mundo, e isso pode ser visto em todas as áreas. A indústria dos CDs dominou o mercado, e a última fábrica de "bolachão" está com problemas e, provavelmente, será fechada. O "bolachão" era uma tecnologia analógica: uma agulhinha passava em cima de um filamento que vibrava na mesma batucada da música. Analogicamente, a vibração transportava-se para um alto-falante, que ampliava o barulho. A tecnologia digital é uma onda quadrada (sim, não;

ligado, desligado; um, zero), que elimina as imprecisões do modelo analógico, como os ruídos, que podem ser observados na televisão. A televisão digital está para chegar, e o Governo está decidindo como fazer, já tendo, inclusive, feito um teste: passaram, de automóvel, em um túnel, com uma TV analógica e uma digital. A imagem da TV analógica simplesmente desapareceu, ficando chuviscada, enquanto a da digital permaneceu perfeita, sem nenhum sinal perdido. A informação no modelo digital é precisa.

Outra característica do modelo digital é a possibilidade de representar qualquer coisa digitalmente, tanto que existem jogos simuladores no computador. Os senhores podem dizer que o desenho é feio, mas isso se dá porque o projeto ainda não está bom ou o computador não é potente.

Passarei à exibição de um vídeo.

A fala do responsável, ao final, diz tudo. O problema da quebra de segurança existe, tanto que houve riscos em um sistema relativamente sofisticado. Falar em segurança ou riscos é uma questão totalmente relativa. Beck escreveu um livro sobre a sociedade de risco, e vários autores o estão discutindo. Vivemos, efetivamente, em uma sociedade de risco, onde quem está vivo corre o risco de morrer a qualquer momento; naturalmente, nós os diminuímos, os controlamos, fabricando automóveis mais sofisticados, cintos mais inteligentes e assim por diante. O mesmo ocorre com os sistemas de informação: há a tecnologia, que, bem utilizada, garantirá um bom nível de segurança.

A boa tecnologia nada significa se os empregados estiverem descontentes. É natural um nível de insegurança dos sistemas, mas é preciso controlá-lo e, para isso, dois elementos são importantes: primeiro, utilizar a melhor tecnologia possível, pois, às vezes, se tem a melhor tecnologia, mas não se tem a infra-estrutura necessária nem o pessoal qualificado para com ela trabalhar, tendo que ser feito um processo de adaptação, e, segundo, dar uma atenção especial à questão de pessoal para que uma pessoa não contamine todo o resto. Essa é uma questão importante.

Não adianta, mesmo com os riscos e perigos que nos rodeiam, querermos "matar" o computador ou destruir o sistema. Esse é um exemplo da nossa área, de um colega que, chateado com o sistema da justiça, que não lhe liberava o pedido, deu um tiro no computador e foi processado por destruir um bem público. Há uma frase muito interessante de Renato Borruso: "Se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista." Penso ser a Justiça, hoje, um dos grandes exemplos, no Brasil, de adoção da tecnologia, apesar de estarmos no início do processo.

Esse *slide* apresenta mais uma alegoria, mostrando que o progresso está aí, causando riscos e perigos. Não podemos, ao analisá-los, ter uma preocupação mercantil, pensando apenas nos lucros ou no dinheiro que será gasto para a implantação do sistema, pois, necessariamente, não se estará investindo ou eliminando os problemas que poderão

ocorrer. Não há sentido, por exemplo, em investir-se todo o dinheiro no sistema, deixando de aplicá-lo no treinamento de pessoal, que é muito importante. Em 1991/1992, o diretor do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina comprou os primeiros computadores para aquela instituição e, ao recebê-los, fez um discurso interessante, dizendo que estava investindo em Informática. Os computadores foram instalados, mas ficaram aproximadamente um ano sem utilização, porque o dirigente não investiu no pessoal da casa, que não estava preparado para usar tal tecnologia.

Enfatizando a questão da origem militar, nesse ponto há um paradoxo: a *Internet* nasceu no meio militar e, exatamente por isso, nasceu aberta. Como o meio militar pôde construir uma ferramenta de rede tão aberta e frágil quanto essa? Os senhores já têm a explicação. Os americanos estavam com medo de que uma bomba russa caísse em Washington e destruísse todo o sistema de Informática, que era baseado nos chamados *main frames*, nos grandes computadores IBM, que, destruídos, levariam tudo à destruição, porque a arquitetura era não de cliente-servidor, mas de terminais vinculados a um grande computador. Montaram, então, basicamente, um sistema que não corresse tal risco, no qual cada computador tivesse o seu processamento e o seu protocolo para conversar com os outros.

A grande idéia foi fazer um esquema aberto e distribuído, uma operação descentralizada, pois a *Internet* nada mais é do que uma rede de redes. Na universidade em que trabalho, há uma rede interna com vários computadores, como a que existe aqui. A famosa *Internet*, uma verdadeira maravilha, nada mais é do que a conexão dessas redes com outras. O que hoje parece óbvio não foi previsto por ninguém, nem mesmo pelo dono da IBM, que, em 1990, disse que o mundo não precisaria de mais do que três grandes computadores IBM, ou seja, concluímos que prever o futuro não é tarefa fácil.

A *Internet* é uma rede global e de uso geral. É transitável, podendo ser feito nela qualquer tipo de serviço e qualquer informação pode ser propagada, diferentemente de redes específicas ou particulares para determinada tarefa. Trata-se de uma rede sem dono, ou melhor, os donos são os diversos órgãos que a mantêm. Não há ninguém que a controle centralmente, mas um Comitê Gestor da *Internet* no Brasil, que gerencia os domínios para que não haja desordem nos nomes e nos diversos endereços por ela disponibilizados, ou seja, um órgão administrativo, que, por meio da Fapesp, faz basicamente o controle administrativo dos domínios, nomes e endereços, mas, no restante, nada gerencia.

O correio eletrônico, que, com certeza, todos dele se utilizam, é uma forma assíncrona de comunicação, diferente do telefone, pois, enquanto estamos aqui, os *e-mails* estão entrando em nossa caixa postal. É o recurso mais utilizado na *Internet*, o que dá a ele essa relevância.

Na correspondência eletrônica, é possível trabalhar-se com listas ou grupos de interesses, mas há fragilidade nos protocolos, porque estão montados em cima de um

protocolo também frágil, que é o da *Internet*: o uso do TCP/IP (*Transmission Control Protocol/Internet Protocol*) aberto, sem criptografia, sem nenhum tipo de gerenciamento mais sofisticado. Quando enviamos, por exemplo, um *e-mail*, não ficamos sabendo se a pessoa o recebeu; a *Internet* não nos dá esse controle, e só ficamos sabendo se a pessoa o responder ou se isso for feito automaticamente pelo sistema de correio, ou seja, toda vez que enviarmos um *e-mail*, solicitarmos ao sistema a confirmação do recebimento. O *Notes*, da *Lotus*, tem um sistema de controle de *e-mail*, tanto que certos órgãos o utilizam. Desconheço se existe um protocolo específico, mas, com certeza, pode usar o da *Internet*, e as mensagens são enviadas criptografadas, fechadas, dependendo de como a ferramenta é organizada; se o sistema não estiver preparado para fazer um esquema fechado, as mensagens podem circular de maneira tão frágil quanto na *Internet*, mas, em princípio, é feito para ter mais segurança. A *Internet*, hoje, é uma interface universal, por isso o *Notes* pode rodar dentro dela.

Os tribunais têm utilizado o correio eletrônico internamente, permitindo aos advogados dar entrada em suas petições por meio eletrônico. O Tribunal Regional Federal da 4ª Região foi um dos pioneiros ao aplicar a Lei nº 9.800, a chamada "Lei do Fax", que permite a utilização de sistemas de transmissão de dados tipo fac-símile ou meio similar para iniciar o processo. Os tribunais estenderam essa interpretação e estão utilizando o *e-mail*, mas há uma restrição: devem os originais ser entregues em juízo, necessariamente, até cinco dias da data do término dos prazos. Mas, como fica a questão da segurança?

O advogado, quando envia um *e-mail* para o tribunal de justiça, não o faz pelo *Notes*, mas pelo correio normal. Há, nesse ponto, um nível de insegurança, porque alguém pode fazer uma interrupção do documento, impedindo que chegue ao seu destino. Se o advogado for muito confiante e estiver apressado, fica tranqüilo em relação ao prazo, mas, depois, como se justificar e provar que enviou a petição para pedir mais prazo? A preocupação de garantia, então, é do advogado. Não há uma insegurança total em relação a isso, porque a segurança dos sistemas não envolve apenas a tecnologia, mas diversos objetos, as pessoas, a segurança e os processos, que são feitos mais ou menos seguros, dependendo de como se monte o conjunto de ações para que a informação ande. No caso do uso do *e-mail*, existem diversas maneiras de se sanar esse problema, como, por exemplo, não o enviando de última hora ou recebendo o aviso do tribunal.

Existem, então, diversos momentos no processo do sistema, nos quais é possível verificar se está indo bem ou não, mesmo que um *hacker* o interrompa. No caso de modificação da petição, por exemplo, trata-se de algo mais complicado; de alguma maneira, alguns problemas tornam-se cruéis com o uso do *e-mail* pela *Internet*.

Quando a petição é enviada por *e-mail*, não há como se comprovar quem a enviou e a sua autenticidade, podendo, inclusive, ter sido um *hacker*. Também não há garantia da sua integridade, pois pode ter sido modificada. Algum tipo de prejuízo pode ser causado, nesses momentos, para o advogado ou para o tribunal, que terá de resolver o problema. A verdade é que os tribunais estão utilizando esse sistema há um bom tempo e, em

princípio, podem ter tido problemas, que não foram referidos. Procuro sempre me informar para dar exemplos aos meus alunos, às pessoas com as quais converso, mas não tenho essa informação - devem ter acontecido pequenos problemas, resolvidos pelos tribunais, porque o processo, de certa maneira, ajuda a resolvê-los sem causar danos.

Os Juizados Especiais Federais da 4ª Região fugiram do *e-mail e* estão usando a *Web* como interface principal, que é uma interface universal, onde se pode rodar qualquer coisa. É extremamente fácil e qualquer pessoa a entende. Como um livro, é composta de páginas e, para nela se navegar, vai-se para frente ou para trás, por meio de dois botões. Existem *links* dentro da página e, na hora em que se passa o *mouse* sobre o *link*, surge a imagem de uma mãozinha. É universal, porque, de alguma maneira, faz qualquer coisa. A simulação mais interessante é o *e-mail*. Normalmente, as pessoas utilizam o *Outlook Express*, o *Eudora* etc., mas tenho o *Webmail*. Hoje, existe de tudo na rede e, infelizmente, temos pouco tempo para navegar.

Os Juizados Especiais Federais estão começando a utilizar a *Web* como interface com advogados. Nesse sistema, o advogado se cadastra e, a partir do recebimento de uma conta - que naturalmente por ela se responsabilizará, por ser personalíssima -, troca informações com o juizado diretamente pela *Web*, entrando no *site* da seção judiciária. Algumas cidades que estão com a interface eletrônica, ou seja, com o famoso processo eletrônico são Londrina, Florianópolis e Blumenau. Realmente, a Justiça Federal está na vanguarda.

Creio que os sistemas devam funcionar de forma a que o interessado tome ciência de que o documento foi recebido, até para que haja uma comprovação, e não apenas um recibo, de que tudo esteja certo.

Em face dessa observação, concluiremos pelo uso da assinatura digital, que garante essa finalidade, mas acrescento que a tecnologia em si não é garantia de segurança, porque podemos ter problemas com a criptografia, que é superior, mas se não houver, junto à tecnologia, pessoas alertas aos problemas e bons administradores de Informática para resolvê-los, de nada adiantará.

Diria que o documento no meio papel tem uma certa invulnerabilidade, porque a informação está nele impressa, ou seja, o documento é o papel com a informação impressa.

NELSON JOBIM
Ministro do Supremo Tribunal Federal

A minha preocupação em relação ao dispositivo cogitado é a de que, se começarmos a exigir a segurança absoluta, o sistema jamais será implantado. Hoje, os ministros assinam o documento sem fazer a sua leitura; partem do pressuposto da confiança em seus assessores, ou seja, a assinatura é absolutamente irrelevante no sentido de ser ela

a certificadora da verdade do documento. O que precisamos é assumir a inviabilidade do sistema manual vigente e os riscos da implantação do sistema com as colateralidades deles decorrentes. Se começarmos a dizer que o sistema não permite a segurança, agregaremos um custo inicial que inviabilizará a mudança e não avançaremos.

AIRES JOSÉ ROVER

Fui a uma defesa de banca de mestrado, integrada pelo presidente, que era o orientador na área jurídica, e um técnico da informática professor do curso de Computação. O tema versava sobre a Lei nº 9.800 e o uso do *e-mail*. Foi citado o caso do TRT, um dos primeiros a eliminar a exigência dos cinco dias **a posteriori** para a entrega do original da petição. O técnico de informática, de alguma maneira, fez a defesa do sistema, porque, como tal, analisa os seus problemas e os seus riscos. Não temos a consciência de todos os possíveis percalços que possam ocorrer em relação a uma informação qualquer. Sabemos que existem problemas, mas, tecnicamente, os ignoramos. O presidente, que foi meu mestre, fez um discurso veemente, dizendo o que acaba de ser dito pelo Ministro Nelson Jobim, no sentido de que, se exigirmos a segurança absoluta, o sistema não será implantado.

NELSON JOBIM

Quando os tribunais do Rio Grande do Sul resolveram autorizar a publicação das intimações dos advogados nos diários locais, houve uma reação, porque nós, advogados, controlávamos os prazos. Eu ia ao cartório, onde havia um escaninho com as minhas intimações e me dava por intimado naquilo que me interessava. No momento em que foi deslocado esse controle, a OAB reagiu brutalmente. Eu era presidente de uma subseção à época e recordo-me que a publicação retirou o controle do advogado em relação ao início do prazo. Surgiu, então, um discurso concernente ao problema da acessibilidade, e mais, importou em uma pessoalização local, porque os advogados de outras cidades que advogavam em determinada comarca precisavam, necessariamente, ter um advogado local para dar-lhes informação na intimação, mas não queriam isso. O mercado de trabalho foi, então, atingido. O grande problema que há nesse tipo de mecanismo não é o mecanismo em si, mas a alteração da composição do mercado de trabalho não só da Magistratura como também do meio da Advocacia, alterando, substancialmente, a regra do trânsito, inclusive problemas de honorários profissionais. É isto que precisa ser posto: não estamos mexendo somente em tecnologia, mas no mercado de trabalho, na acessibilidade a esse mercado, no controle sobre ele, que é o mercado dos advogados e também o dos juízes, porque seria muito fácil ocultarmos um mecanismo decisório, o que não é mais possível.

AIRES JOSÉ ROVER

É uma verdadeira revolução. Com certeza, as pessoas que, de alguma forma, combatem esse mecanismo, trazendo, inclusive, elementos interessantes em termos técnicos, sabem que por trás existem questões políticas, mas não podemos olvidar-nos das questões técnicas, até para tentar fazer com que não aconteça nada que ponha em xeque a instalação, por exemplo, do sistema dos juizados especiais, que é uma iniciativa maravilhosa.

Concordo plenamente com a idéia de que a segurança não é só tecnologia, mas um conjunto de elementos e, necessariamente, para se ter uma boa segurança, não é preciso ter a melhor tecnologia. Temos como exemplo os juizados, que estão utilizando a *Web* para fugir do problema do *e-mail*. O indivíduo é citado por meio da *Web*, e o prazo começa a contar a partir do sétimo dia. Essa idéia é muito interessante, pois há a informação de que será citado, o que ocorre no momento em que se acessa o *site*. Não há como fugir dessa informação, pois o indivíduo tem a obrigação de acessar o *site* pelo menos de sete em sete dias. Trata-se, então, de um mecanismo perfeito que supre o problema do *e-mail*, algo que pode dar problemas, dos quais nunca tive notícias. Tecnicamente, o *e-mail* é um cartão postal aberto que qualquer pessoa lê, mexe ou risca. Não há sigilo.

A relatividade da segurança tem que ser posta de forma clara para não serem feitos discursos - infelizmente, alguns os fazem de boa-fé - que põem em xeque iniciativas muito interessantes.

Lipman, quando esteve no Brasil, há algum tempo, proferiu uma palestra muito interessante e disse que a *Web* produz milhões de editores.

Outra noção curiosa é que a *Web* passa a idéia de um ser vivo e, como tal, não há controle total sobre ela, que pode evoluir para algo que não se sabe. A incerteza do futuro é algo sempre presente. Como seres vivos, temos controle relativo sobre a natureza, forma pela qual controlamos as nossas doenças, por exemplo. O importante é ficarmos alertas para utilizarmos a maior tecnologia e o melhor controle para que esse ser vivo não desande.

Na *Internet*, há o protocolo TCP/IP, que é a base de conversação entre os computadores, ou seja, faz com que um computador converse com outro. É uma linguagem e há uma programação. O W*indows*, que é um sistema operacional, por exemplo, já vem com o protocolo de rede TCP/IP, o conjunto de regras que fará com que aquele computador se conecte com outro. Pode também aquele computador ter vários protocolos: o do W*indows* - o *NetBIOS* -, outro conjunto de regras, outras regras de segurança agregadas e, dependendo da rede ou do protocolo utilizado, tem-se mais ou menos segurança.

Imaginem uma pirâmide: a base para a conversa entre os computadores é o TCP/IP. Em cima, outros protocolos, como os do correio eletrônico: o SMTP e o POP3, para envio e recebimento de mensagens. Caso se queira agregar segurança a esse *e-mail*, pode-se colocar sobre essa plataforma vários conjuntos de protocolos, sendo um deles o http - protocolo de texto e hipertexto -, o chamado www, nome dado pelos técnicos para o conjunto de regras que faz com que, dentro da *Internet*, as páginas sejam armazenadas. Com relação aos *links*, o conjunto de regras - protocolo - faz com que as páginas conversem entre si e a mãozinha seja gerenciável. É algo que se agrega dentro da *Internet* e pode ser simulado fora dela, mas hoje o http é um protocolo específico para rodar em cima do IP, protocolo da *Internet.*

ARI PARGENDLER
Ministro do Superior Tribunal de Justiça

A minha idéia é a seguinte: quando coloco http, estou, analogicamente, sintonizando uma estação. Então, a *Web* é o meio pelo qual entro na *Internet.*

AIRES JOSÉ ROVER

Exatamente. Quando se entra em qualquer página da *Internet*, já se está navegando. Não há página sem endereço.

ARI PARGENDLER

O nosso computador está programado para entrar na *Intranet* do Tribunal e, a partir dali, podemos acessar a *Internet*.

AIRES JOSÉ ROVER

Na realidade, quando se entra no computador e abre-se o *netscape*, o computador já está trabalhando autonomamente. Clicando-se em um botão, pode-se entrar em um tribunal de São Paulo ou do Rio de Janeiro. Nesse caso, estará se acessando outro computador em São Paulo, no Rio de Janeiro ou até mesmo no exterior. Um amigo mandou-me um *e-mail* que passou pelos Estados Unidos e pela Noruega. Os *e-mails* fazem todo esse trânsito, motivo de insegurança. Com relação à *Internet,* não há um

protocolo específico que fuja desse trânsito.

Estou dizendo, aparentemente, que o TCP/IP é totalmente inseguro, mas não se trata disso. Todo e qualquer computador que está na *Internet* tem que ter um número IP, do qual as polícias federal e civil poderão recorrer, no caso de prática criminosa.

Outra informação interessante é que na informática não há a possibilidade de se apagar um crime, como na vida real. A *Internet* deixa alguns rastros, mesmo que durem apenas cinco minutos. Se houver, por exemplo, no Tribunal, um sistema e uma equipe permanentemente alerta, no caso da entrada de um *hacker*, será possível tomar conhecimento e procurá-lo.

Kevin Mitnick, o mais famoso *hacker* americano, preso e libertado recentemente, teve um *hacker* japonês no seu rastro durante uns dois ou três anos, juntando dados daqui e de dali, até descobrir o seu modo de agir, para, enfim, encontrá-lo. No mundo real, a polícia, muitas vezes, fica mais de dois anos investigando, sem que encontre o bandido.

Do www, temos que entender que é um protocolo diferente que trabalha com hipertexto. É a interface universal que estamos utilizando, e os juizados especiais estão caminhando nessa direção, eliminando o *e-mail* e usando apenas a interface www. Dei o exemplo do advogado, que já é intimado e também envia a petição por meio da *Internet*, como faz com a sua declaração de rendimentos, para a qual há um pequeno sistema - e é um outro modelo de se trabalhar -, no qual, preenchida a declaração, é feita uma ligação à rede, que se conecta com o servidor aqui em Brasília - ou com vários servidores, se tiver espelho - e conversam, criptografando e protegendo a declaração no computador, enviando diretamente para o sistema. Esse trânsito pode ser interceptado por um *hacker*, porque a *Internet* está sendo utilizada, mas pegará um documento criptografado e, portanto, protegido.

No que diz respeito a problemas gerais e desafios, a desterritorialidade, ou seja, o computador estar nos Estados Unidos ou em Portugal, cria uma série de problemas, principalmente em relação a crimes de informática.

A soberania está, de alguma maneira, se modificando. Nós, profissionais de Direito, temos observado isso. Os Estados não são mais os mesmos, como é, de primeira mão, a globalização em termos econômicos, e a *Internet* vai nesse caminho.

Farei a apresentação de dois vídeos sobre alguns crimes.

O grande problema da pirataria no Brasil não é a *Internet*; baixar música pela *Internet* ainda é algo restrito a 8% dos brasileiros, mas, de qualquer maneira, as gravadoras estão irritadas e procurando se proteger, colocando sistemas criptografados de música e, com isso, prejudicando o consumidor que compra o CD e não consegue rodá-lo, porque o seu aparelho não descriptografa aquele sistema. Há, inclusive, ação judicial no sentido de tirar esses CD's de circulação. Trata-se de um problema que terá que ser discutido.

De qualquer forma, o maior problema é o do modelo de negócio: um CD custar R$24,30. A nossa Constituição diz que o cidadão tem direito à cultura, mas, como pode ter ele esse direito, se não consegue comprar um CD de R$30,00 e nem mesmo se alimentar direito? No entanto, esse mesmo cidadão pode comprar um CD de R$5,00 R$6,00 em um camelô. Em um discurso inverso, diria que o camelô está fazendo um bem para o País, na medida em que está permitindo o acesso desse cidadão à cultura. Naturalmente, trata-se de um discurso antagônico, mas que tem que ser ouvido, até para que as pessoas percebam que o modelo de negócio tem que mudar, pois não é apenas trancafiando camelôs ou destruindo CDs que o problema se resolverá.

Gostaria de fazer duas observações em relação à pedofilia. Uma diz respeito à questão dos provedores, que são de acesso ou de conteúdo. No primeiro caso de pedofilia na *Internet*, ocorrido há mais ou menos três anos, o menino era provedor e, para isso, tinha um computador conectado na *Internet,* precisando apenas instalar um pequeno aplicativo que gerencia páginas na *Internet*, ou seja, agregar o protocolo http ao sistema. instalando-se esse *software*, já se tem condições de ser um provedor e, a partir daí, pode-se colocar páginas na *Internet*. No *Word*, se salva o documento como html, que é transformado em página da *Internet*. É um documento normal, só que com codificações específicas de html vistas pela *Internet*, gerando um arquivo com nome, que passa para a pasta onde está o servidor. É preciso ter um endereço IP, e o servidor tem que ser configurado; por isso, normalmente, não se utiliza o *Windows*, mas o *Unix.* Digamos que essas fases administrativas estejam concluídas e já se tenha um número IP e um domínio: o arquivo é acessado normalmente, de qualquer lugar, como qualquer página da *Internet*. Ser um provedor da *Internet* é algo fácil, necessitando-se apenas de um domínio, que é a parte burocrática, conseguido na Fapesp, que faz esse gerenciamento.

O menino era um provedor de conteúdo e tinha seiscentas páginas na rede. Esse tipo de provedor oferece *o* seu *site*, doando um espaço com um nome. É um provedor no qual se deixam textos, conteúdo.

O provedor de acesso é aquele que provê acesso às pessoas que querem entrar na *Internet*. Para isso, têm que ter uma porta e o acesso a ela é obtido por meio de um provedor de acesso; pode ser um portal - conceito mais sofisticado -, que é um grande *site* que disponibiliza conteúdo e acesso. O grande portal brasileiro é o *Uol*, que tem um grande conteúdo e também é um provedor de acesso. Para ser um provedor de acesso, tem que se ter mais uma condição: máquina para segurar o número possível de usuários.

A relação da responsabilidade é a grande questão. O provedor não se responsabiliza pelo conteúdo - nem isso é possível -, mas alguns gostariam que fosse responsabilizado. Houve projetos de lei nesse sentido, mas foi algo impraticável. O menino tem um *site* pequeno com seiscentos usuários, e a *Uol* tem milhões deles, cada um com direito à página. Na minha opinião, não é possível responsabilizar provedor no sentido de controlar o conteúdo, até porque caracterizaria censura. No entanto, a legislação o responsabiliza no caso de não colaborar quando houver ato criminoso.

A questão paradigmática é central: da mudança da tecnologia analógica para a digital. Na tecnologia analógica, não havia condições para se ter um esquema tão largo de produção. A possibilidade para com ela se trabalhar era limitada. Já no modelo digital, a possibilidade é infinita. O limite da tecnologia digital é o processador, mas já estão falando em computador quântico.

NELSON JOBIM

Estive recentemente nos Estados Unidos, em Princeton, e a pesquisa trabalha na computação quântica.

Nós, profissionais do Direito, trabalharemos com um programa de competência, que é um negócio um pouco complexo. Imaginem a seguinte hipótese: um cidadão de nacionalidade chinesa, em Hong Kong, acessa a *Internet* via *Web* e compra ações de uma empresa inglesa na bolsa de Nova Iorque, via sistema de *Web*, dando ordens à agência do banco de Frankfurt para depositar o valor correspondente no banco de Paris. Surge um jurista e pergunta qual é a autoridade competente para julgar a demanda eventual que possa surgir dessa transação: a do lugar de onde veio o sinal - Hong Kong , a da bolsa de Nova Iorque ou a da sede do provedor de todo esse sistema?

O nosso modelo de competência não se ajusta a isso, mas a nossa tentativa é sempre a de sobreviver. Temos imensa dificuldade em romper com esse tipo de mecanismo.

AIRES JOSÉ ROVER

Penso que já estejam rompendo. Ontem mesmo assisti, na televisão, o "*site* censura", sobre pedofilia, que está fazendo uma pesquisa na *Internet* para encontrar pessoas que a praticam. No começo da entrevista, estavam fazendo um bom trabalho, mas, ao final, queriam uma legislação que, de alguma forma, responsabilizasse os provedores em geral, no caso de aparecerem esses s*ites* que utilizam fotos pedófilas. Trabalham com isso, sabem da dificuldade, mas estão usando o velho modelo, supondo que o provedor tenha tecnologia para controlar o manancial de informações, como também assustando a população, ao dizer que não temos legislação que nos guarde e proteja em relação à pedofilia.

Às vezes, nos utilizamos de um problema que deixa a sociedade consternada para forçar a questão, no sentido de dar uma solução que não seja jurídica, mas de prova. Um dos grandes problemas da *Internet* é a participação, no processo, de diversos provedores, de diversos estados nacionais, o que a torna de difícil solução jurídica, como no caso da busca de provas, pois não há uma polícia bem preparada. Trata-se de algo que se está construindo. A polícia está se preparando, a tecnologia está sendo aperfeiçoada e a sociedade está tomando consciência de que, às vezes, não é possível depender de

juristas, e sim delas mesmas e dos órgãos que, de alguma maneira, são os olhos da sociedade.

O conhecimento tem prazo de validade cada vez menor e é cada vez mais abundante. Essa questão é paradigmática. A indústria fonográfica está brigando por um conhecimento? O direito autoral surgiu há alguns anos para proteger o intelectual que produzia algo que só ele fazia e, por isso, tinha que ser protegido, remunerado; era uma alma viva entre milhões de pessoas. O conhecimento era algo escasso, e o direito autoral surgiu dentro dessas circunstâncias, sendo totalmente legítimo. Hoje, todos estão produzindo conhecimento. Quantos livros de Informática e Direito já existem? Muitos. Todos têm algo a dizer, e não sei como resolver o problema do direito autoral, mas, com certeza, em um futuro próximo, haverá mudanças, até no sentido de flexibilizar a idéia desse direito, porque todos serão intelectuais e produzirão intelectualmente. Se todos produzirem, e se o conhecimento é geral e abundante, como será cobrado, se só pode ser cobrado aquilo que é escasso? E o que é escasso? As obras-primas etc., mas a grande maioria não será obra-prima. Normalmente, esse raciocínio significa uma mudança de paradigma que as pessoas e os próprios juristas não conseguem realizar, por causa do modelo antigo a que estão, de certa forma, vinculados.

Mais controle e mais segurança implicam em mais custos. Não se pode querer montar um sistema que inviabilizará qualquer projeto.

Os processos, em princípio, tornam-se mais complexos, porque temos que preencher alguns espaços, clicar em outros. Posso citar o uso do *e-mail* com criptografia, que o tornará mais complexo, porque pesará na rede e exigirá algumas configurações.

No *slide,* está posto mais ou menos a difusão da informação, a liberdade de informação, o investimento na cultura, os consumidores, os monopólios e a riqueza, porque depende de como for feito o controle da informação, que pode ser para beneficiar, abrir, tornar mais transparente, ou seja, investir realmente em uma sociedade mais libertária, em contato com a cultura, como pode ser para o contrário. O exemplo que eu trouxe, da indústria fonográfica, mostra como estão usando a tecnologia para prejudicar o consumidor.

A sociedade tem muita força no sentido de autocontrolar. O controle não está só na tecnologia, pois a comunidade tem muito controle. Existem, inclusive, organizações que procuram canalizar esses controles, evitando problemas maiores.

Existem diversas formas tecnológicas para controlar, as quais abordarei na palestra de amanhã; falarei sobre criptografia, proteção de documentos e controles biométricos que estão chegando, como também de uma série de instrumentos importantes para a proteção de dados, como cópias de segurança, antivírus e *firewall*, sistemas fundamentais para garantir sistemas confiáveis.

Com relação a sistemas confiáveis, trata-se de mais uma questão para dizer o quanto é

importante definir os níveis de segurança. Pode-se ter um sistema mais aberto, mais tranqüilo para determinadas tarefas ou um mais fechado, o que pode ser definido.

A questão de se investir em cultura e educação também é fundamental, porque hoje temos apenas 8% da população brasileira usando a *Internet* e, naturalmente, para que a grande maioria a ela tenha acesso, além de ser necessário que progrida financeiramente, deverá estar investida de cultura e educação para poder lidar com essa ferramenta, que é mais ou menos amigável, mas não tanto.

O controle jurídico também existe. O Direito está aí e tem condições de dar respostas efetivas para uma série de problemas. Naturalmente, temos que promulgar leis para algumas questões que sejam realistas e tenham longevidade; preparar a polícia e o ministério público; e investir também na questão do Direito Internacional, pois sem ele torna-se difícil. O uso da arbitragem e da mediação, no exterior, é muito freqüente para uma série de problemas da rede, o que ainda não acontece no Brasil.

Todos esses itens dão mais esclarecimento às pessoas, eliminando, na medida do possível, as desordens sistêmicas, as perturbações, que também são necessárias para melhorar os sistemas. Temos que ter cuidado com os velhos paradigmas e deles tentar nos libertar, pensando que os novos meios compensarão as perdas. Os advogados e as pessoas que estão se sentindo prejudicados neste momento, mais à frente ganharão.

Para flexibilizar é necessário leis, sistemas e mentalidades.

O negócio é ficar de olho aberto: "O que distingue a 'modernidade reflexiva' e a torna problemática é o fato de que devemos encontrar respostas radicais aos desafios e aos riscos produzidos pela própria modernidade. Os desafios poderão ser vencidos se conseguirmos produzir mais e melhores tecnologias, mais e melhor desenvolvimento econômico, mais e melhor diferenciação funcional" (Beck).

Einstein falou que "a preocupação pelo homem e por seu destino deve constituir o interesse fundamental subjacente a todo o empenho técnico, a preocupação com os grandes e ainda não resolvidos problemas da organização do trabalho e da distribuição de bens, a fim de que criações da mente humana venham a se constituir em benção e não maldição para toda a humanidade".

Nesse processo, a preocupação tem que ser com o ser humano e não com o dinheiro ou com qualquer outra coisa.

Muito obrigado.

12/08/03