CÂMARA DOS DEPUTADOS

DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

COMISSÃO DE DIREITOS HUMANOS E MINORIAS		
EVENTO: Seminário	Nº: 1195/06	DATA: 14/11/2006
INÍCIO: 14h30min	TÉRMINO: 18h40min	DURAÇÃO: 04h10min
TEMPO DE GRAVAÇÃO: 4h10min	PÁGINAS: 82	QUARTOS: 50

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

EDUARDO AZEREDO – Senador;
CRISTINA ALBUQUERQUE – Representante da Secretaria Especial de Direitos Humanos da Presidência da República e Coordenadora do Grupo de Trabalho para Enfrentamento à Pedofilia e à Pornografia Infantil na Internet;
MARCELO BECHARA – Consultor Jurídico e especialista em Inclusão Digital do Ministério das Comunicações;
JAMES GÖRGEN - Secretário-Executivo do Fórum Nacional pela Democratização da Comunicação — FNDC;
ANTÔNIO ALBERTO VALENTE TAVARES - Presidente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet — ABRANET;
PEDRO ANTÔNIO DOURADO DE REZENDE - Professor da Universidade de Brasília;
DEMI GETSCHKO - Conselheiro e representante do Notório Saber em Assuntos de Internet do Comitê Gestor da Internet no Brasil;
THIAGO TAVARES NUNES DE OLIVEIRA - Presidente da SaferNet do Brasil;
ELA WIECKO VOLKMER CASTILHO - Procuradora Federal dos Direitos do Cidadão, representante do Ministério Público Federal;
SÉRGIO LUÍS FAVA - Perito Criminal, representante da Divisão de Direitos Humanos da Polícia Federal;
RENATO OPICE BLUM - Advogado especialista em Direito Eletrônico, representante da Federação Brasileira de Bancos.

SUMÁRIO: Seminário "*Liberdade de Acesso à Internet e Combate ao Crime Cibernético.*"

OBSERVAÇÕES

Houve exibição de imagens.
Há orador não identificado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Declaro abertos os trabalhos do presente seminário, que debaterá o tema *Combate ao Crime Cibernético e Liberdade de Acesso à Internet*.

Agradeço ao Deputado Luiz Carlos Sigmaringa Seixas, Presidente da Comissão de Constituição e Justiça e de Cidadania, o oferecimento deste auditório, a fim de que a Comissão de Direitos Humanos e Minorias da Câmara dos Deputados possa realizar este Seminário.

Antes de usar a palavra, convido para compor a Mesa o Deputado Julio Semeghini, que vem se destacando na Câmara dos Deputados no tratamento da legislação da Internet.

Tenho a honra de chamar também o Deputado Luiz Piauhylino, autor de um projeto discutido com a sociedade, o primeiro aprovado na Câmara dos Deputados e que agora está no Senado Federal, sobre o qual a imprensa noticiou em virtude do relatório do Senador Eduardo Azeredo.

Agradeço aos Deputados Julio Semeghini e Luiz Piauhylino, em especial a este último, que desmanchou toda sua agenda para estar aqui conosco. Deputado Luiz Piauhylino, sinceramente, agradeço a V.Exa.

Convido o Senador Eduardo Azeredo, Relator desta matéria na Comissão de Constituição, Justiça e Cidadania do Senado Federal, a tomar assento à Mesa.

Agradeço aos Parlamentares por estarem aqui numa terça-feira à tarde, véspera de feriado. Ontem e hoje não houve *quorum* sequer para abrir a sessão, muito menos hoje para se votar qualquer coisa. Os Deputados já estão em debandada para aproveitar o feriado. Para nós, contar com a presença de um Senador da República e de 2 Deputados Federais interessados no tema é muito importante.

Convidei também o Ministro Paulo de Tarso Vannuchi, da Secretaria Especial de Direitos Humanos, que tem justificativa absolutamente plausível para sua ausência: S.Exa., o Presidente da República, acaba de convocá-lo para reunião às 15h no Palácio do Planalto. Em seu lugar, convido a Dra. Cristina Albuquerque, representante da Secretaria Especial de Direitos Humanos da Presidência da República, a tomar assento à mesa. S.Sa. coordena, no âmbito desta Secretaria, o

Programa Nacional de Combate à Pedofilia, que está relacionado ao nosso assunto. Agradeço a ela o comparecimento a esta audiência.

Convido também a compor a Mesa o Dr. Marcelo Bechara, consultor jurídico e especialista em inclusão digital do Ministério das Comunicações.

Está composta a Mesa inaugural deste seminário.

Peço licença aos presentes para fazer pequena digressão sobre os fundamentos deste seminário, cuja realização deve-se à preocupação da Comissão de Direitos Humanos com as violações de direitos humanos na Internet e também com os projetos de lei em tramitação no Congresso Nacional sobre crimes na Internet.

Essa questão envolve 2 valores fundamentais para os direitos humanos: o primeiro é a necessidade de normas que fortaleçam o combate aos crimes cometidos por meio da Internet, o segundo, é assegurar a plena liberdade de expressão, a maior acessibilidade física, legal e econômica à rede mundial de computadores.

Na era do conhecimento, a inclusão digital é condição para igualdade de oportunidades e para a inclusão social.

O paulatino crescimento das violações dos direitos humanos na Internet, nos últimos tempos, chamou a atenção dos Deputados que integram a Comissão de Direitos Humanos da Câmara dos Deputados. Essa criminalidade virtual contra os direitos fundamentais implica os mais diversos tipos de delitos: crimes contra a honra — injúria, calúnia, difamação —, ameaças veladas e explícitas nos mais diversos tipos de agressão e também ameaças de morte; veiculação de pornografia infantil, inclusive com fotos da prática de pedofilia; comércio ilegal de armas e de drogas; incitação ao suicídio; incitação à prática de condutas delituosas, especialmente contra grupos vulneráveis, afro-descendentes, homossexuais, migrantes, indígenas; prática de racismo; divulgação de ideologia nazista, racista e nazi-fascista e as mais diferentes formas de discriminação de gênero, de classe, de origem, de etnia, de raça, de orientação sexual, de cor, de idade, de crença religiosa, entre outras.

Essa realidade motivou-nos, na Comissão de Direitos Humanos, desde o início da gestão de que estamos à frente, a buscar diálogo com outras entidades e instituições, governamentais e não governamentais.

Por isso, realizamos audiência pública no dia 26 de abril deste ano sobre este assunto. Muitos dos debatedores e expositores deste seminário que se inaugura agora participaram daquela audiência pública.

Em razão do grande interesse suscitado por esta audiência, tomamos, em seguida, outras iniciativas, com a finalidade de debater mais amplamente a questão. Fizemos 2 ou 3 reuniões de trabalho sobre esse tema com representantes da empresa Google e de outras empresas provedoras da Internet; com a Polícia Federal; com o Ministério Público Federal; com entidades representativas da sociedade civil, em especial a SaferNet.

Todas essas iniciativas trouxeram à superfície a demanda premente da sociedade civil da necessidade de normatização, de regulamentação da questão, ao mesmo tempo em que se reconheceu a necessidade de haver colaboração das empresas provedoras, que detêm as informações que permitem chegar àqueles que utilizam a Internet com finalidade de práticas de crimes e violação dos direitos humanos.

Também, nessas audiências públicas e reuniões de trabalho, ficou clara nossa preocupação com a manutenção da liberdade de expressão e o reconhecimento da Internet como inovação tecnológica que veio para ficar e que não pode sofrer censura ou outras restrições que venham a colocar em risco as liberdades públicas, arduamente conquistadas ao longo da História do nosso País e da humanidade, e o objetivo da inclusão digital de toda sociedade brasileira.

Estamos diante da seguinte situação: no Congresso Nacional tramitam diversos projetos de lei, alguns já aprovados aqui na Câmara dos Deputados, como é o caso do projeto de lei do Deputado Luiz Piauhylino, que está na Comissão de Justiça do Senado Federal e que tem o ilustre Senador Eduardo Azeredo como Relator, e é nesse espectro que queremos iniciar o nosso seminário, ouvindo essas pessoas, a quem agradecemos antecipadamente a presença.

Temos de garantir a liberdade de informação e de expressão do pensamento, mas temos também de nos precaver, em termos de sociedade brasileira, contra os abusos, a prática de crimes, o uso ilegal da rede mundial de computadores.

Essa é a disjuntiva sobre a qual estamos debruçados neste seminário.

Proponho, primeiro, ouvirmos o Deputado Luiz Piauhylino, autor do projeto original; depois, o Deputado Julio Semeghini, especialista do tema em nossa Casa e, sobre os comentários de S.Exas., o Senador Eduardo Azeredo. A partir da exposição dessas 3 ilustres pessoas, ouviremos o Dr. Bechara, do Ministério das Comunicações, e a Dra. Cristina, da Secretaria Especial de Direitos Humanos.

Feita essa exposição e apresentado o tema, vou desfazer esta Mesa e convidar os outros ilustres expositores que nos dão a honra de sua presença.

Se possível — idéia minha —, ao final deste seminário, vamos procurar o consenso em algumas propostas, objetivos e idéias para torná-lo prático. Em geral, os seminários na Câmara são extremamente retóricos e pouco práticos em suas conclusões. Não espero que este seja prático, mas creio que deveríamos afunilar nossas propostas para estabelecermos o consenso.

De qualquer forma, o tema é da maior importância, atualidade e da maior gravidade.

Passo a palavra ao meu ilustre colega, amigo e advogado, Deputado Luiz Piauhylino, que fará falta a esta Casa porque sequer concorreu à reeleição. Eu deveria ter seguido seu conselho.

O SR. DEPUTADO LUIZ PIAUHYLINO - Caro Presidente, Deputado Greenhalgh, o que V.Exa. disse sobre minha pessoa deve-se ao fato de seu coração ser muito bondoso e por ser um Deputado que marcou esta Casa, que sempre se lembrará de V.Exa. pela sua atuação, pela democracia e pela defesa dos direitos humanos e da justiça, pois é um brilhante advogado.

Agradeço a V.Exa. o convite para participar deste seminário. Quando fui convocado, vim com a maior alegria, mesmo porque estou ao lado do meu dileto amigo Deputado Julio Semeghini, um dos mais brilhantes e talentosos Deputados que dominam essa área de tecnologia e que tem ministrado verdadeiras aulas na Câmara e no Congresso, assim como ao lado do Senador Eduardo Azeredo, a quem aprendi a admirar, desde a época em que foi Governador do Estado de Minas Gerais e pela sua conduta no Senado, e ao lado da Dra. Cristina e do Dr. Bechara, respectivamente do Ministério de Direitos Humanos e do Ministério das Comunicações.

Cumprimento os demais presentes a este seminário, de extrema importância não apenas pela matéria tratada, mas também pelo que cada um representa em suas atividades específicas. Cumprimento também a imprensa, que tem sido fundamental neste debate.

Sr. Presidente, tenho certeza de que sairemos daqui com idéias e diretrizes para que o Brasil possa também ter uma legislação sobre matéria tão palpitante. Indago a V.Exa. o que sugere com relação ao horário. Dez minutos está ótimo. Solicito a V.Exa. que me dê um sinal, caso eu extrapole o tempo.

Este assunto surgiu na Casa em 1996, quando o então Deputado, hoje Governador reeleito pela Paraíba, Cássio Cunha Lima apresentou projeto que não era específico, mas que tratava, entre outras matérias, da tipificação de crimes na rede da informática.

O Presidente da Comissão de Comunicação à época, Deputado Ney Lopes, indicou-me para Relator e, como tal, recordo-me da primeira vez em que abordei o tema e como este permeou todo o projeto.

O Plenário da Comissão de Ciência e Tecnologia foi refratário a que se abordasse esse assunto, por entender que discutir regulamentação na comunicação da informática seria censura, seria limitação à livre comunicação.

E o que fizemos? Trouxemos o assunto para debate. Solicitei ao Presidente um debate na Comissão, e S.Exa. o aprovou, e depois criamos uma Comissão virtual, que, acredito, foi a primeira desta Casa. E o advogado, Dr. Renato Opice Blum, brilhante conhecedor do assunto, lembrou que o coordenador foi o nosso colega Dr. José Henrique Barbosa Lima Neto, advogado do Estado do Rio de Janeiro, e que os integrantes da Comissão que abriram a discussão com a sociedade foram o Dr. Damásio de Jesus, advogado de São Paulo, o Dr. Ivan Lira, Juiz Federal do Rio Grande do Norte, auditores militares, professores universitários, desembargadores, peritos criminais da Polícia Federal, enfim, todos participaram. E dessa ampla discussão, que iniciamos em 1997, conseguimos elaborar um substitutivo em 1999.

Ocorre que ali terminava a legislatura, e o substitutivo não pôde ser apreciado. Mas, diante da nossa vinculação ao projeto e do estímulo que recebemos da sociedade e de todos os segmentos envolvidos com a informática e a Internet, no

início da Legislatura de 1999 apresentamos o PL nº 84, de 1999, que era exatamente o aproveitamento daquele substitutivo que havíamos discutido amplamente com a sociedade.

Abrimos a discussão na Câmara, o projeto percorreu diversos estágios, não só internamente, caro Senador Eduardo Azeredo, como também externamente. Tivemos oportunidade de percorrer o País para participar de discussões sobre esse tema, até que houve a apresentação do substitutivo do ilustre Deputado Nelson Pellegrino, da Bahia, que, inclusive, enriqueceu o PL ao acrescentar itens referentes aos cartões de crédito e à clonagem de telefonia celular, e, com isso, o projeto foi aprovado por unanimidade.

Quero aqui, mais uma vez, dar o crédito do estímulo tanto à coordenação como ao lado técnico para o projeto fornecido pelo Deputado Julio Semeghini, que trouxe na bagagem profissional todo esse aprendizado e, assim, o projeto foi aprovado na Câmara Federal, em 2003, por unanimidade, o que ficou expresso na posição de todos os Líderes dos partidos com assento nesta Casa.

Menciono que se discutiu esse aspecto que aflora novamente, no sentido de haver risco de limitação da comunicação e da informação. Na época, em 1997, quando aprovada a lei americana que tratava de crime na rede, recordo que um artigo foi considerado restritivo à comunicação, o que gerou luto mundial na rede de Internet. Então, o Brasil e a Câmara discutiram esse projeto com o sentimento mundial de que o mesmo não poderia significar nenhuma restrição à livre comunicação.

Ao chegar ao Senado, o Senador Eduardo Azeredo, não só pela sua condição política de Senador, mas também pela sua condição de especialista na matéria, foi indicado Relator do projeto e, no primeiro momento, encaminhou no sentido de que o projeto da Câmara fosse aprovado.

Como já havia outros projetos no Senado e a matéria é dinâmica, todo dia há novidade, a idéia inicial era aprovar o projeto que havia saído da Câmara, fruto de discussão da sociedade, para que, depois, constasse da legislação do Brasil e o País pudesse subscrever diversos tratados, convenções, do que estava impedido por falta de legislação. Em seguida, seria aberta discussão sobre outros assuntos que permeiam o tema.

Mas o Plenário do Senado achou melhor discutir logo os projetos que estavam em andamento, e o Senador buscou, então, fazer um substitutivo que pudesse contemplar esse processo.

Temos debatido, conversado informalmente e trocado idéias. E todo meu sentimento de Parlamentar, de cidadão e de advogado, militante que fui e que agora volto a ser por opção pessoal — a partir de fevereiro voltarei a ingressar na minha casa, que é a OAB, no setor de advocacia, uma profissão liberal —, demonstra que o espírito, ao trazer essa discussão para a Câmara, foi exatamente o de suprir uma lacuna, inspirado no princípio do Direito segundo o qual não há crime sem lei que o defina.

Na verdade, temos legislação que contempla diversas hipóteses, mas para a dos crimes cometidos com requisito tecnológico dentro da rede não poderia haver legislação porque o sistema de informática não existia anteriormente. A partir do momento em que passou a existir, precisamos da legislação para disciplinar a hipótese de crime para que os crimes na rede possam ser punidos, como são punidos os crimes cometidos no trânsito, na sociedade. Agora, sempre levando em conta a liberdade da comunicação, sem nenhuma restrição.

Sr. Presidente, fiquei muito feliz ao receber a mensagem da Comissão sobre liberdade de acesso à Internet e combate ao crime cibernético, que é o intróito deste seminário, em que V.Exa. diz que é preciso compatibilizar essa necessidade com 2 valores fundamentais para os direitos humanos.

Esta é uma Comissão de mérito sobre direitos humanos, mas que também precisa penetrar nesse setor quando debate e defende a liberdade de expressão, o direito à comunicação e à informação e, de outro lado, a preservação das condições econômicas que permitam a inclusão digital para todos.

É muito bom que este seminário seja realizado com esse norte, para que possamos, nesta Casa Legislativa, saber que trabalhamos para preservar esses direitos fundamentais.

Foi importante eu iniciar afirmando a influência do Deputado Julio Semeghini, cujo projeto enriqueceu a discussão, no sentido de que tenha exeqüibilidade. Temos também o substitutivo do Deputado Pellegrino, que trouxe novos temas que surgiram durante a discussão. Em seguida, enquanto o projeto inicial, concebido em

1999, modifica o Decreto-Lei nº 2.848 e a Lei de Interceptações Telefônicas, o substitutivo do Senador avança em outros setores, como o Código Penal, o Código Penal Militar, o Código de Processo Penal, a Lei de Repressão Uniforme, o Código do Consumidor.

Tudo isso são contribuições, mas é evidente que vamos ferir o assunto em pauta, que é o problema da identificação do usuário. Entendo, Sr. Presidente, que a respeito deste tema não devemos deixar nada debaixo do tapete. Temos de discuti-lo. Apesar de não existir consenso; existe ampla discussão, temos de debatê-lo, ouvir nossos tribunais a respeito e ver se é conveniente que entre na discussão desse projeto legislativo ou vá para outro setor.

Minha sugestão, com a devida vênia dos 2 especialistas e dos nossos representantes do Poder Executivo, a Dra. Cristina e o Dr. Bechara, é no sentido de mergulharmos na parte em que já há consenso, em que há manifestação legislativa expressiva, para agregar temas consensuais enriquecidos pelo Senado, porque a cada ano, a cada mês, a cada hora há modificações no setor de informática.

Espero que possamos sempre levar em conta a regra que aprendi nesta Casa: lutamos pelo ideal, mas atingimos o que é possível. Esse é o meu sentimento. Na minha passagem pelo Legislativo, especificamente nesta Casa, durante 20 anos, esse foi o tema que mais me deu satisfação pessoal na condição de cidadão, discutir e contribuir para o aperfeiçoamento da matéria.

Coloco-me à disposição de todos, hoje ainda na condição de Deputado Federal e de representante do povo de Pernambuco, a partir de fevereiro na condição de cidadão e de advogado, para também continuar nessa discussão e poder verificar o que é melhor para o País.

Sr. Presidente, agradeço a V.Exa. a oportunidade e, mais uma vez, cumprimento os membros da Mesa, especialmente a os que, apesar de não residirem em Brasília, na véspera de um feriado, vieram aqui com o espírito de contribuir para buscar o que é melhor para o País e para a nossa sociedade.

Muito obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Deputado Luiz Piauhylino, pelas suas considerações.

Concedo a palavra ao Deputado Julio Semeghini para suas considerações iniciais.

O SR. DEPUTADO JULIO SEMEGHINI - Sr. Presidente, é um prazer estar com V.Exas., com várias pessoas do nosso setor, com os jornalistas, com os especialistas e com aqueles que têm tentado ajudar na elaboração de leis para que possamos utilizar a Internet como realmente precisa ser feito.

Na Comissão de Ciência e Tecnologia dividimos o nosso tempo e tratamos da Internet com especialistas e consultores do setor na Câmara dos Deputados, na tentativa de elaborar leis que nos permitam utilizar o máximo possível a Internet e assegurar, cada vez mais, o compromisso do Governo com a inclusão digital, para que seja um projeto rápido que avance tanto na regulamentação da Banda Larga como no conceito da sua universalização, como foi feito com a voz, e que possamos agregar a essa rede de computadores aquilo que temos de mais prático e de mais moderno no resto do mundo.

A Comissão de Ciência e Tecnologia discutiu vários projetos de lei, a exemplo daquele que trata da validade jurídica para o documento digital, da criação da estrutura da certificação digital no País e outros projetos de lei que nos têm permitido avançar no uso da Internet de maneira profissional.

Agradeço a todos que têm ajudado na elaboração desses projetos.

Parte das leis, de cuja elaboração o Deputado Luiz Piauhylino participou, foi debatida com especialistas do setor, com advogados, com a Polícia e com aqueles que, na verdade, delas se beneficiarão ou com elas conviverão.

Fiz o mesmo com algumas pessoas, que, inclusive, estão aqui presentes, a quem agradeço por sempre participarem dos debates na Câmara dos Deputados.

Sr. Presidente, parabenizo V.Exa. pela iniciativa, uma vez que é uma das maiores autoridades em direitos humanos, questão essa que sempre tem de estar acima de tudo. Às vezes, nós, técnicos, como eu, que sou engenheiro, ficamos afoitos e com vontade de disponibilizar o acesso à tecnologia para facilitar nossa vida.

Nos Estados Unidos, quando discutíamos tema referente ao combate à pirataria, vi o Congresso inteiro impedir a aprovação de lei que introduzia a validade jurídica da assinatura digital por entender que a sociedade americana não possuía

uma boa lei da privacidade e que aquilo poderia comprometer uma série de coisas do dia-a-dia do cidadão. Assim, parou-se, por um ano, ferramenta de tal importância para se elaborar essa lei.

A preocupação de V.Exa. é muito oportuna, importante, e mostra sua sensibilidade para com o setor. É uma pena que, pelo menos por 4 anos, talvez não esteja na Câmara, mas espero que esteja no Governo e continue a ajudar nosso País e rapidamente retorne a esta Casa.

Agradeço ao Senador Eduardo Azeredo, um dos homens que mais conhece tecnologia de informação no Congresso, não só do lado das leis, mas também na condição de usuário, de técnico, de especialista e de Presidente de companhia de processamento de dados, da mesma forma que eu, e, acima de tudo, de Governador, que utilizou fortemente essa ferramenta para o bem de sua gestão e do povo de Minas Gerais.

Agradeço à Dra. Cristina e ao Dr. Bechara a participação.

Sr. Presidente, o Congresso tem de fazer autocrítica. Precisamos encontrar uma forma de ser mais objetivos nos debates de temas importantes para o Brasil. O projeto de lei do Deputado Luiz Piauhylino, se não me engano, vem sendo debatido há 6 anos nesta Casa e com a sociedade. Aquelas pessoas que iniciaram o debate hoje são as maiores especialistas do assunto na sociedade, que tem crescido muito, mas ainda discutimos o mesmo projeto de lei, isto é, não saímos do lugar. Essa é a autocrítica que o Congresso tem de fazer.

O projeto inicial do Deputado Luiz Piauhylino visava algo claro. Naquela época houve bastante resistência. Queríamos discutir se o Brasil precisava ou não do projeto de lei que chamávamos de “crimes de Internet”. Não era nada disso, e devagar amadureceu-se a idéia, houve debate e se chegou à redação correta, que era a tipificação desses crimes no mundo digital.

Como transportar os crimes previstos e esperados na sociedade e no mundo real para o mundo digital? Como seria possível detectar um crime numa tentativa de roubo de um arquivo eletrônico sem que houvesse sido invadida a propriedade fisicamente?

Ora, é o mesmo crime que se comete ao tentar pular um muro e invadir uma casa. Discutíamos como tipificar esses crimes também para poder combatê-los, ou

preveni-los. Como poderíamos prevenir a ocorrência desses crimes? Não era possível que só fosse considerado crime quando realmente tivesse sido causado um dano ou um mal a alguém ou a alguma empresa, senão jamais se poderia evitar que esses crimes fossem cometidos.

Esse projeto foi debatido e aprimorado. Foi incluída a parte do debate sobre vírus e foram discutidos vários outros aspectos. A cada ano inserimos uma novidade. Foi muito bem lembrado pelo Senador Eduardo Azeredo a tipificação do *fishing*. Além dessa, houve várias outras melhoras propostas por S.Exa. ao projeto. A tipificação do *fishing* é hoje técnica muito comum de lançar uma isca, é uma ferramenta para que se possa cometer um crime.

Em resumo, esse projeto de tipificação foi muito bem elaborado na Câmara dos Deputados e melhorado de forma muito competente pelo Senador Eduardo Azeredo. Não há nenhuma restrição nessa parte da tipificação, o que quer que seja previsto. Vou deixar que o Senador Eduardo Azeredo faça os comentários.

Percebemos, naquela época, que a tecnologia nos permitia chegar a um mundo novo, à sociedade, à casa de uma pessoa, à empresa, ao dia-a-dia das pessoas. Era importante que usássemos essa mesma tecnologia, a infra-estrutura da rede de computadores, para esclarecer a tentativa de um crime e não só transformar isso em crime. Era preciso identificar quem era o criminoso ou qual o ambiente mais próximo que esse criminoso usava, um terminal ou alguns terminais da rede de computadores, para tentar cometer ou para realmente cometer o crime.

Discutimos com os provedores de acesso à Internet, com os advogados, com os escritórios de advocacia especializados, com a Polícia Federal, com o promotor, com o juiz. O resultado foi um projeto de lei muito simples, que acabei por assinar com muito orgulho, mas que não é de minha autoria. Houve um debate muito grande com a Polícia Federal e com as Polícias Estaduais especializadas sobre esse assunto.

Esse projeto de lei, ao mesmo tempo que complementava o projeto que tipificava os crimes, permitia a rastreabilidade e a identificação da rede ou de alguns computadores e obrigava os provedores a guardarem informação por um período entre 1 e 3 anos.

A cada reunião que fazíamos, o debate era sobre a duração do período em que se deveria armazenar informação no *lobby* dos bancos de dados dos provedores, no seu *login* e *logout*, sobre a hora em que as pessoas se conectavam e se desconectavam da rede, e quem estava se conectando.

Depois foi dito que era preciso se cadastrar, até porque o provedor tem um cadastro. Se o provedor tem um contrato que lhe permite cobrar de alguém pelo uso do serviço, tem de ter algum cadastro, o endereço, o nome da pessoa, para que possa fechar o contrato e enviar a conta.

Também era preciso avaliar se as informações constantes dos cadastros eram ou não suficientes; porque, por essas informações, com certeza, as pessoas seriam identificadas, senão como pagariam a conta? Não estou falando de um relacionamento rápido, relâmpago, na verdade é um relacionamento comercial que existe entre os provedores. Portanto, eles conseguem identificar fisicamente onde estão o terminal e a pessoa que paga pela conta de acesso.

Na verdade já havia o cadastramento dos provedores, o que queríamos é que eles guardassem essas informações nos seus bancos de dados por 1 ou 3 anos. Chegou-se ao acordo de que guardariam as informações por até 3 anos. E mesmo que os provedores questionassem isso, ao mesmo tempo era importante darmos privacidade a essas informações. Se vou começar a acompanhar a vida de um cidadão, é preciso termos um projeto de lei que discuta a privacidade e o que está acontecendo nesse grande mundo digital com um monte de informações.

O Congresso deve um projeto de lei de privacidade ao povo brasileiro. Enquanto isso, em cada lei aprovada é importante responsabilizarmos alguém para tomar conta dessas informações. Na verdade será quebrado qualquer sigilo dessas pessoas, portanto devemos responsabilizar os provedores pela guarda das informações e garantir que somente eles cedam essas informações.

Houve muito debate sobre isso, e fomos muito firmes porque recebemos muitos pedidos das polícias especializadas para que as autoridades tivessem o direito de pedir informações aos provedores.

Entendemos, na Câmara dos Deputados, naquela época, que isso não era possível porque não temos ainda um grande projeto que trate da privacidade. Naquele momento era melhor assegurar a privacidade do cidadão ou da empresa,

seja pessoa física ou jurídica, em relação ao interlocutor com quem ele conversa por meio da rede de computador. E essa informação teria de ser passada pelo provedor mediante mandado judicial, ou requisição judicial, não estou certo — não sou engenheiro e há advogados presentes na platéia. Mas seria necessário pedido judicial para que essas informações fossem cedidas. E, a partir da solicitação das informações, o provedor teria de guardá-las até que houvesse autorização para destruí-las.

Eu entendia que esse era um passo significativo para a sociedade. Já teríamos tipificado os crimes e não teria sido criada uma lei específica apenas para o computador. A estratégia foi sendo completamente melhorada e atualizada. No próprio texto há alterações no Código Penal, no Código Penal Militar, na Lei de Repressão. Mudam-se as leis, às quais são acrescentadas essa tipificação, sem a necessidade da criação de uma nova lei para o mundo digital, que não é nada mais que o nosso dia-a-dia envolvido pela tecnologia.

Foi esse o consenso a que chegamos na Comissão de Ciência e Tecnologia, e os 2 projetos foram aprovados por unanimidade, o do Deputado Luiz Piauhylino e esse que assinei, de autoria da sociedade, que saiu com o substitutivo e que iria para o Senado.

Dou o testemunho de que o Senador Eduardo Azeredo tentou aprovar o projeto do Luiz Piauhylino, no substitutivo, mas houve um pedido no Senado para que fosse apensado a outros. Sei que não foi pessoal a decisão de apensar, foi decisão da Mesa do Senado, e o Senador Eduardo Azeredo tinha de cumpri-la. Parabenizo S.Exa. pelo avanço, uma vez que aproveitou a experiência dos técnicos para aprimorar o projeto e o fez de forma muito bem-feita.

Há 2 problemas polêmicos que estão causando esse debate. Na minha opinião, devemos ouvir o Senador para podermos avançar. O Brasil tem de ter esse projeto de lei. À época muitos juízes foram contra. Segundo eles, o Brasil não precisa disso. Mas isso acabou. O que tenho percebido é um grande consenso em torno da idéia de ter esses 2 projetos de lei. Falta essa lei para que o Brasil possa assinar uma série de tratados e acordos internacionais. Precisamos aprovar esse projeto de lei rapidamente, assim como alguns outros de que esta Casa precisa tratar, como o da assinatura digital.

É uma pena ainda não incluirmos a certificação digital. Seria possível obrigar o brasileiro a cadastrar-se pela certificação eletrônica, uma vez que se vai cadastrar pela rede de computador. Aliás, essa medida melhora significativamente a confiabilidade dos dados inseridos na rede pela pessoa, facilita sua vida e a protege no seu dia-a-dia. Infelizmente, Senador, ainda não é o momento para isso no Brasil. O País tem avançado muito pouco.

Este Congresso deve ao nosso povo uma lei que garanta a massificação dessa ferramenta, que é muito importante para introduzir segurança na rede de computador de forma mais profissional.

Esse é o nosso ponto de vista. Ouviremos os especialistas depois de ouvirmos o Senador Eduardo Azeredo. Estou à disposição para qualquer esclarecimento.

Muito obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Agradeço ao Deputado Julio Semeghini a exposição. A linha de raciocínio de S.Exa. é a mesma do Deputado Luiz Piauhylino.

Tenho a honra de passar a palavra ao Senador Eduardo Azeredo, Relator desta matéria no Senado, cujo relatório, semana passada, foi considerado conflituoso em relação às liberdades individuais, ao direito de expressão da informação, à idéia do anonimato e do sigilo etc.

Quando convidei S.Exa. para vir a este seminário, conversamos um pouco, disse-lhe que era a oportunidade também, com os especialistas, no seminário que estamos fazendo, de colocar os pingos nos is. S.Exa. mesmo reclamou de interpretações distorcidas do seu pensamento no relatório.

Este seminário está sendo transmitido ao vivo pela *TV Câmara*, pela *TV Justiça* e pela *TV Senado.* Este programa será retransmitido na programação dessas televisões neste final de semana.

E esse é o assunto. Trata-se de suscitar o tema, estabelecer a polêmica e tentar chegar a algum consenso.

Agradeço a V.Exa. por estar aqui conosco.

Muito obrigado.

O SR. SENADOR EDUARDO AZEREDO - Boa-tarde a todos.

Saúdo o Deputado Luiz Eduardo Greenhalgh, a quem agradeço pelo convite para falar sobre projeto de suma importância para o País; o Deputado Luiz Piauhylino, autor do primeiro projeto, aprovado pela Câmara; o Deputado Julio Semeghini, nosso colega não só de partido, mas também da área de informática; a Dra. Cristina Albuquerque e o Dr. Marcelo Bechara, que também participam da Mesa; bem como a todos que vão hoje também expor e discutir essa questão.

Já estou satisfeito porque, até a semana passada, eu não tinha recebido nenhuma emenda ao projeto; mas agora o projeto está em discussão. Quem sabe aparecem sugestões pertinentes.

Toda esse polêmica suscitada, na verdade, está localizada em alguns pontos do projeto, que é muito mais amplo do que um mero cadastramento de usuários. É um projeto que combate os crimes cibernéticos no Brasil e que guarda sintonia com o que está sendo discutido no mundo todo. Não há nada, como alguns aí me mandaram nos *e-mails*. Eu estou respondendo a cada um dos *e-mails* que chegam. Estou tendo a paciência, com a minha assessoria, de responder.

Alguns disseram: *"Olha, esse Senador maluco está inventado isso"*. Eu não estou inventando nada. Isso está sendo discutido. Disponho dessa convenção sobre crimes cibernéticos. Trata-se da Convenção de Budapeste, assinada em 23 de novembro de 2001. O senado americano ratificou essa matéria agora, no dia 7 de agosto de 2006.

É bem verdade que está dito aqui que o senado ratifica tratado controverso sobre o crime cibernético. Está bom. Mesmo os americanos consideram que é controverso. Eu não nego isso. E está assinada não é por Cuba, China ou Coréia do Norte, como alguns também criticaram. Está assinado pelo Canadá, pelos Estados Unidos, pela Dinamarca, pela Noruega. São esses países que assinaram a Convenção de Budapeste, que trata da identificação. Agora, como em toda convenção, depois o país tem de ter uma lei que detalhe a adesão à mesma.

O processo ainda está nesse pé. Quer dizer, não há neste momento a identificação, a forma como está no projeto não está implementada. A informação da Embaixadora do Brasil na Comunidade Européia, com quem eu entrei em contato, revela que a Dinamarca já teria internalizado essa convenção e já estaria com ela em funcionamento.

O histórico feito pelo Deputado Luiz Piauhylino é exatamente o que eu tenho também apresentado sobre esse projeto. Ou seja, é um projeto muito mais amplo, discutido há muito tempo. Não se trata de nada que esteja sendo discutido na correria. Pelo contrário, acho que devemos uma legislação como essa ao País, porque há uma década que se discute o tema.

Quero ainda dizer que, quando o projeto chegou à Comissão de Educação — e eu fui Relator —, a minha primeira defesa foi no sentido de aprová-lo como ele tinha vindo da Câmara. Por quê? Por uma visão bem objetiva. Pensei: *"Vamos aprovar o projeto como está, porque ele já é bom, atende basicamente a 80% do que queríamos atender"*. É verdade que, com a velocidade da tecnologia, de lá para cá, algumas coisas mudaram. Mas vamos aprová-lo como está.

O Senador Hélio Costa, na época, ponderou que não, que já havia algumas coisas novas. Foi S.Exa., inclusive, que levantou essa questão do *fishing.* Mas, mesmo assim, foi aprovado num acordo. Aprovaríamos daquele jeito e faríamos um projeto complementar, uma PEC Paralela, aquela famosa PEC Paralela que nunca mais vingou. O problema é esse: a PEC Paralela não foi mais votada.

A idéia era essa, que aprovássemos como estava. E faríamos um projeto paralelo, para complementar o primeiro projeto.

Quando já corria o prazo no Senado, foi apresentado requerimento no sentido apensar os projetos. Aí ele voltou para a Comissão de Educação. Como estava vencida aquela etapa que eu tinha defendido, pensei: *"Então, vamos agora fazer um projeto mais atualizado. E vamos complementá-lo com o que aconteceu da época da aprovação na Câmara até hoje"*.

Daí, então, é que o substitutivo foi feito. Foram fundidos, na verdade, vários projetos, o do Senador Renan Calheiros, do PMDB; o do Senador Leomar Quintanilha, do PC do B. Aproveitou-se a idéia do cadastramento, do Senador Delcídio Amaral, do PT de Mato Grosso do Sul.

Aí é que fizemos, então, este substitutivo que está em discussão, aprovado por unanimidade na Comissão de Educação e enviado para a Comissão de Constituição, Justiça e Cidadania, onde houve todo esse qüiproquó, digamos assim.

Aqui está escrito assim:

> *"Com o controle da comunicação eletrônica pelo Estado, as autoridades teriam acesso desde a uma simples troca de mensagens entre adolescentes apaixonados até à correspondência sigilosa entre empresas e seus fornecedores e clientes."*

Onde é que está isso no projeto? É a minha pergunta.

Outros dizem assim: *"Não, o projeto atenta contra a privacidade."* Não sei onde. Eu disponho aqui de decisões da Justiça, em que se afirma:

> *"Assim, pode-se concluir que o fornecimento de dados cadastrais em poder do provedor de acesso à Internet, que permita a identificação de prováveis autores de infrações penais, não fere o direito à privacidade e o sigilo das comunicações, uma vez que dizem respeito à qualificação de pessoas e não ao teor da mensagem enviada".*

Não sei onde estaria algum atentado à privacidade das pessoas.

Com relação à liberdade de expressão, da mesma forma, não sei onde pode haver alguma coisa contra a liberdade de expressão. Quer dizer, a Internet está livre da mesma maneira. É realmente um avanço enorme que aconteceu no mundo. Essa coisa toda aqui do *cybercrime*, eu consegui tudo pela Internet. Se não fosse a Internet, não conseguiria. Então, não estão em dúvida as vantagens que existem em poder utilizar a rede como um todo.

Quanto à inclusão digital, eu não sei também como se poderia prejudicá-la: *"Ah, mas é porque os alunos teriam de se cadastrar".* Não é nada disso. Em todo lugar em que há um computador existe algum responsável, senão vira anarquia.

Aliás, lá na cidade de São Paulo, existe uma lei municipal, porque o assunto é municipal, segundo a qual as *lan houses* são obrigadas a identificar os usuários. Por quê? Porque chegou-se à conclusão de que a maior parte dos crimes surgia nas l*an houses.* Eram pessoas que pagavam 10 reais, usavam o computador, mandavam vírus, mandavam agressões, atentados e tudo o que pode acontecer.

O Brasil, felizmente, é um País mais pacífico. Não temos nada do ponto de vista do terrorismo, mas podemos ter um dia. Então, temos de estar também

prevenidos contra atentados à segurança nacional no que tange aos nossos sistemas vitais. Ou seja, com relação à de transmissão de energia elétrica, todos devem se lembrar de que, numa época, houve a queda de linha de transmissão, que ficou meio no ar. Não se sabia se tinha sido um fato normal, um mero acidente, ou se tinha havido algum agente provocador.

Então, temos de buscar essa proteção também no caso da segurança nacional, eu diria, nas questões gerais que tratam da computação.

A certificação digital também não existe. Não há nenhum ponto do projeto que mande usar certificação digital. O Deputado Julio Semeghini emitiu sua opinião, que é um outro ponto. A Receita Federal já usa. Mas não existe, no projeto, nada que obrigue a certificação digital.

Em resumo, não existe atentado à privacidade, nem restrição à liberdade de expressão, nem certificação digital, nem nada que impeça a inclusão digital. O que está prejudicando a inclusão digital, vamos ser claros aqui, na verdade, é que existe o Fundo de Universalização dos Serviços de Telecomunicações — FUST, que tem como um dos objetivos colocar computador nas escolas públicas. Esse fundo já arrecadou mais de 4 bilhões de reais, e nada disso foi utilizado para essa finalidade até hoje. Esse, sim, é um ponto forte que ataca e prejudica a inclusão digital.

Eu já fiz vários pronunciamentos a respeito, já apresentei requerimentos de informação, e ainda estão estudando a melhor forma de sair. Ainda no Governo passado, o Ministro Pimenta da Veiga chegou a colocar em andamento uma licitação para os computadores. Houve uma queixa da Oposição da época, foram feitas algumas críticas, e o processo foi suspenso. Depois de 4 anos, ainda não se colocou nada para usar os 4 bilhões de reais arrecadados. Essa, sim, é uma questão que ataca e prejudica a inclusão digital.

Sobre o projeto em si, volto a dizer, toda a sua primeira parte trata da tipificação dos chamados crimes cibernéticos, como clonagem de cartão de celular, de cartão de crédito, difusão de vírus, falsificação em si. São crimes que foram surgindo. Os juízes podem resolver hoje? Podem. Há muito juiz que tem resolvido. Trouxe aqui o exemplo de uma decisão do Tribunal de Justiça de Minas, porque sou de lá. Agora, também existem muitos casos em que ocorre o inverso: as pessoas

deixam de decidir pela falta de tipificação. Dizem que não podemos ter regra nenhuma, que a Internet tem de ser totalmente livre. Pode até ser que sim.

Enfim, eu não tenho nenhuma restrição a discutir esse projeto. Ele não é um projeto acabado. Eu disse mais de uma vez e repito aqui: de minha parte, se nós tivermos que chegar a um ponto em que o ótimo é o inimigo do bom, se tivermos que fazer uma divisão do projeto, como propôs o ex-Ministro Miro Teixeira ou, ainda hoje, o Senador José Jorge, podemos também.

Vamos supor que tirássemos os arts. 20 e 21, que falam especificamente da identificação do usuário. O que vai acontecer é que nós, seguramente, vamos ter um prejuízo no processo investigativo, porque se chegará até o IP, mas não até o usuário. Muita gente afirma que hoje já tem como se identificar, mas o que se identifica é o IP. O IP identifica o computador, mas não o usuário. Um computador pode ter vários usuários, e um IP também pode ser subdividido em outros IPs.

Aliás, é sempre bom nos informarmos melhor. Eu comecei a conhecer a realidade dos pequenos provedores, dos provedores de cidades pequenas do interior. Precisamos também olhar para esse lado, porque os pequenos provedores dependem da liberação dos IPs pelas companhias telefônicas, e não é algo que acontece com a facilidade que imaginamos. Então, eles acabam tendo um IP e subdividem em IP virtuais. Esse é mais um complicador. Essa é outra questão que afeta a inclusão digital, porque as cidades pequenas acabam tendo mais dificuldade para ter provedores, para ter um acesso.

Por outro lado, não são só os provedores que dão acesso à Internet. As próprias telefônicas dão acesso diretamente; as empresas, em geral, acabam sendo provedoras também. O Senado é o seu próprio provedor. Então, não é sempre que se precisa acessar um provedor de Internet. Tanto é assim que vamos modificar a proposição anterior. Em vez de usar a palavra “provedor”, poderia ser “a quem liberar o acesso”. Podemos fazer essa modificação, porque é mais amplo. É uma hipótese. Não fica só “o provedor”.

Então, sobre os arts. 20 e 21, podemos avançar, sim. Aprovamos agora o projeto inicial do Deputado Luiz Piauhylino acrescido de vários pontos, como esse do *phishing* e outros que foram trazidos aqui, e deixamos o cadastramento para um segundo momento, acompanhando a Convenção de Budapeste. A minha convicção

pessoal é a de que esse assunto não morre. Ele vai continuar sendo discutido no mundo.

Temos, num primeiro momento, uma explosão. Vamos usar como exemplo os serviços bancários no Brasil. Todos sabem que a alta inflação fez com que o nosso sistema bancário fosse o mais informatizado no mundo. Num primeiro momento, você poderia fazer qualquer transação bancária. O que acontece hoje? Os bancos impuseram uma série de regras por conta da falsificação e dos danos que estavam acontecendo.

Sou cliente do Banco do Brasil e, agora, eu tenho que cadastrar cada computador que uso para poder fazer uma transação bancária; tenho um limite para poder fazer uma transferência financeira ou pagar alguma conta; tenho uma senha que tem outra senha. Para acessar meu outro banco, tenho de consultar uns cartõezinhos que ficam na minha carteira para fazer uma senha diferente.

Essas restrições vão aparecendo porque, infelizmente, o mau uso da tecnologia acontece, e nós temos de proteger o bom usuário. O bom usuário deve ser o objetivo maior de toda a legislação. Temos de procurar evitar a deturpação do uso da tecnologia, que leva o temor às pessoas. Hoje, muita gente já não está mais fazendo operações bancárias via computador, e isso não é do interesse do banco, é interesse nosso, do cliente. Dizem que é interesse do banco, mas o interesse na operação segura é nosso! É do correntista, do brasileiro que não quer correr o risco de um processo demorado para provar quem é que tirou o dinheiro da sua conta corrente.

Então, Sr. Presidente, era isso o que eu queria dizer. Minha posição é de total abertura às sugestões pertinentes, a uma discussão que seja baseada no texto, e não na desinformação, em questões quixotescas que foram mencionadas, como a de que eu estaria propondo que se rastreasse os *sites* visitados pelos internautas. Isso não existe em nenhuma parte do projeto. As pessoas ficam com aquela paranóia: *"Ai, vão ver que eu olhei o site da* Playboy*, então, não pode"*. Não existe isso no projeto; não existe rastreamento em lugar algum no projeto de lei por mim relatado.

Minha disposição é, portanto, a de chegar a um objetivo que dote o Brasil, rapidamente, de um projeto que combata, isso, sim, o crime cibernético.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Senador Eduardo Azeredo, pelas explicações sobre seu relatório.

Passo a palavra à Dra. Cristina Albuquerque,

A Dra. Cristina Albuquerque, que representa o Secretário Especial de Direitos Humanos, Ministro Paulo de Tarso Vannuchi, como disse no início, é responsável por um grupo de trabalho que desenvolve um programa nacional de combate à pedofilia, que tem a ver com o nosso tema. Eu, desde já, lhe agradeço a presença e lhe concedo a palavra.

A SRA. CRISTINA ALBUQUERQUE - Boa-tarde a todos. Agradeço, em nome do Ministro Paulo Vannuchi, a oportunidade de participar deste debate.

Sr. Presidente desta Comissão, Deputados que compõem a Mesa, Senador, meu colega do Ministério da Comunicação, colegas que compõem o Grupo de Trabalho para Enfrentamento à Pedofilia e à Pornografia Infantil na Internet — há, pelo menos, 4 membros presentes —, inicialmente, quero me alinhar com a satisfação do Senador ao ver que a polêmica gerada criou esta oportunidade e, certamente, criará outras. Um projeto com propósito tão meritório, evidentemente, só vai ser construído, não tenho a menor dúvida, por meio do amadurecimento e da polêmica. Por isso também acho extremamente importante que ele seja exaustivamente debatido, compartilhado e que possamos trabalhar em cima de consensos.

É sabido que temos acompanhado — e agora não me refiro só à pedofilia e pornografia infantil na Internet — o avanço dos crimes cibernéticos contra os direitos humanos. Racismo, neonazismo, homofobia se espraia por toda a Internet, violando de forma degradante os direitos de todas as pessoas, de todos os seres humanos. Infelizmente, o Brasil é hoje um dos países que integram o *ranking* do mal na produção desses crime por meio da rede mundial de computadores.

Portanto, mais uma vez, certamente, não poderíamos nos furtar a responder à sociedade — e falo particularmente para as crianças e adolescentes — com um mecanismo que ajude a coibir esses crimes abomináveis. Porém, temos de ser bastante cautelosos com a abrangência dessa legislação.

Todos que estão aqui, especialmente os que compõem a Mesa, que tiveram a coragem de colocar esse tema na agenda, têm o mesmo propósito. Temos de ter

cautela, repito, com a abrangência dessa lei, determinar exatamente o que ela preconiza e os seus efeitos. Não podemos agir movidos pelo afã de resolver esse problema e deixar alguma brecha, por menor que seja, que possa restringir os direitos de todas as pessoas. Essa restrição poderia ser de forma expressa, ou talvez até de um efeito colateral. Como médica, como cirurgiã, conheço efeitos colaterais indesejáveis. Eles têm que ser exaustivamente debatidos, e podem acontecer. A legislação a ser mudada deve ter um caráter cirúrgico, ou seja, é preciso examinar atentamente os vazios da nossa legislação, no que estamos defasados em função da tecnologia — aqui foi citada a propagação de vírus — e verificar em que medida, na prática, isso vai ter o seu efeito maximizado.

Resguardo-me para um segundo momento da discussão sobre o trabalho que o Governo Federal vem realizando em parceria com outras instituições, inclusive com o Parlamento, e que culminou na proposta do Plano de Ação Nacional de Enfrentamento à Pedofilia e Pornografia Infantil na Internet e, finalizando, repito as palavras do Deputado Julio Semeghini: os direitos humanos têm que estar acima de tudo; acima, inclusive, de interesses de setores econômicos.

Obrigada.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Dra. Cristina.

Passo a palavra ao Dr. Marcelo Bechara, Consultor Jurídico do Ministério das Comunicações sobre a matéria, que neste instante representa o Ministro Hélio Costa, ausente do País cumprindo missão oficial.

O SR. MARCELO BECHARA - Exmo. Deputado Luiz Eduardo Greenhalgh, Senador Eduardo Azeredo, Deputado Julio Semeghini, Deputado Luiz Piauhylino, Dra. Cristina, minha colega de Governo, agradeço a esta Comissão a oportunidade de debater, com uma platéia seleta e realmente interessada, assunto que levantou alguma polêmica nas última semanas, o que nos dá a oportunidade de discutir um projeto realmente importante para o País. É preciso que se diga que poucos são os que têm a coragem do Senador Eduardo Azeredo de enfrentar um tema tão difícil, e S.Exa. é, efetivamente, o maior especialista no assunto no Congresso Nacional.

Sinto-me muito honrado de estar sentado à mesma mesa que o Deputado Luiz Piauhylino, porque acompanho esse projeto desde 1999.

Desde então pude participar, a convite do Senador Hélio Costa, na Comissão de Educação, de um substitutivo que tratou da questão do *phishing*, da pornografia infantil. Enfim, é um projeto que venho acompanhando há muito tempo.

Antes de mais nada, é preciso desmistificar algumas questões. Como um todo, é um bom projeto. Como vem da Câmara dos Deputados, o PLC 99, de 2003, traz efetivamente algumas inovações importantes para a atualização de algumas condutas ilícitas que estão sendo praticadas em um novo ambiente cibernético. Realmente existem muitos avanços, em razão disso entendo ser esse um projeto importante, e acho que a discussão já está até demorada em razão da urgência e dos prejuízos que vêm sendo causados para o País.

A única questão específica a que vou me ater é a referente à identificação positiva. Como estamos aqui, na Comissão de Direitos Humanos, eu não poderia deixar de citar mais uma vez — já fiz isso em outra oportunidade aqui na Câmara dos Deputados — o art. 19 da Declaração Universal dos Direitos do Homem, de 1948:

> *"Art. 19. Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e idéias por quaisquer meios e independentemente de fronteiras."*

Isso, para mim, é Internet.

O art. 27 da mesma Declaração diz o seguinte:

> *"Art. 27. Toda a pessoa tem o direito de tomar parte livremente na vida cultural da comunidade, de fruir as artes e de participar no progresso científico e nos benefícios que deste resultam."*

O que entendo com isso? Quem estuda a Internet, quem a conhece, como o Senador Eduardo Azeredo e o Deputado Julio Semeghini, que estão aqui presentes, sabe que esse instrumento de comunicação e de conhecimento foi construído com bases sólidas de liberdade, de colaboração da comunidade científica, da comunidade acadêmica. Com isso, construímos um ambiente em que é possível

reproduzir tudo ou quase tudo daquilo que praticamos no que chamam de mundo real.

Não faço distinção entre mundo real e mundo virtual, até porque muitos danos causados na Internet são reais, razão da importância do projeto. Contudo, o que tem de ficar claro é que qualquer forma de restrição ou limitação ao acesso prejudica o próprio desenvolvimento, vai na contramão da Internet. É exatamente esse o ponto específico que venho debatendo e questionando.

Foi dito que não há no projeto, mas já houve em um determinado momento, a questão da certificação digital. Quero ler então dispositivo que diz o seguinte:

> *"Art. 21. Todo provedor de acesso a uma rede de computadores sob sua responsabilidade somente admitirá como usuário pessoa natural (...)."*

A pessoa natural antecede a pessoa física e jurídica, é a pessoa mais original dentro do Direito.

> *"(...) dispositivo de comunicação ou sistema informatizado que for autenticado por meio hábil e legal à verificação positiva da identificação de usuário, ficando facultado o uso de tecnologia que garanta a autenticidade e integridade dos dados e informações (...)"*

A Medida Provisória nº 2.200, que efetivamente instituiu a infra-estrutura de chaves públicas brasileiras, diz em seu art. 1º:

> *"Art. 1.º Fica instituída 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."*

Então, estamos falando efetivamente de certificação digital dentro desse projeto.

Outra coisa que ficou clara é que, realmente, vários crimes estão sendo praticados, sejam crimes de racismo, de pornografia infantil, sejam ameaças. Já

temos cerca de 5 mil decisões dos tribunais brasileiros, na área penal ou não, que tratam da Internet.

Existem pelo menos 2 tipos de crimes informáticos: os crimes impuros e os crimes puros. Os impuros são aqueles em que se utiliza o sistema informático como meio. Por exemplo, o racismo acontece na Internet, mas pode acontecer por outros meios; ameaças podem acontecer na Internet, mas também por outros meios. Esses crimes, em regra, já são tipificados e, portanto, puníveis. A Internet é um meio.

O Direito Penal trabalha com os bens jurídicos que devemos tutelar: o direito à vida, o direito à honra, o direito ao patrimônio. A discussão é: o bem informático é efetivamente um bem a ser tutelado juridicamente do ponto de vista tal? Eu acredito que sim, e aí nós criamos aqueles chamados crimes informáticos puros, em que o alvo da ação é o próprio sistema informático. Esse é o caso do dano por vírus, que é um tipo penal que está aqui previsto.

A identificação positiva é uma forma de atingir um meio, de ir em busca do meio, ou seja, não necessariamente todos aqueles que são identificados são agentes delituosos. O que se tem que focar é a tutela do bem jurídico a ser protegido pelo ordenamento jurídico, que é o próprio sistema de informação. Esses são os crimes que estamos querendo tipificar, porque nós estamos falando de informação, de patrimônio. Agora, para isso, criar um mecanismo em que todos nós seremos obrigados a nos identificar para acessar a Internet e, pior, estabelecer responsabilidade criminal àquele que der esse acesso de forma indevida, não autorizada, isso, sim, não pode acontecer e vai na contramão do que pretendemos, até porque nós sabemos que, efetivamente, aquele que tiver má-fé — se o provedor nacional for obrigado a fazer essa identificação — vai procurar provedores internacionais e, com isso, a norma torna-se inócua.

Fiquei muito satisfeito quando o Senador Eduardo Azeredo falou sobre os pequenos provedores, porque são eles que, desde o começo da Internet, têm sido os mais prejudicados. Eles foram os responsáveis pela disseminação da Internet no começo, na antiga BBS Internet, ou naquele pequeno provedor que se acionava com *fax modem* de 36600, conexão *dial-up*, discada. O que aconteceu de lá para cá? Com o surgimento da Internet grátis — que de grátis não tinha absolutamente nada, porque havia uma repartição da empresa de telecomunicações com o provedor

grátis — esses provedores começaram a ser achacados. A partir daí, com a prestação de serviços de acesso à Internet pelas prestadoras de serviço de telecomunicação, mais provedores quebraram. A expectativa era de que houvesse 3 mil no País; hoje talvez não cheguem a 300. Com uma medida dessa natureza, efetivamente, os 300 que ainda existem vão fechar, porque é uma responsabilidade criminal que está sendo atribuída efetivamente, como estava no projeto original, ao provedor de acesso.

O provedor de acesso é pessoa jurídica e não pode ter responsabilidade penal. A responsabilidade penal da pessoa jurídica só existe no Direito brasileiro, e de forma discutível, no Direito ambiental. Isso foi alterado, é verdade; foi transformado em *"responsável pelo provedor de acesso"*, mas quem é o responsável? É o dono? É o representante legal? É o advogado? É o contador? É o técnico responsável? E, agora, passou para *"aquele que der o acesso"*.

Bom, são questões que tratam, de forma um pouco lacônica, da imputação do crime, no caso do provedor de acesso. E dentro do Direito Penal nós sabemos que isso não pode acontecer, porque os tipos penais têm que ser bem definidos.

Infelizmente, não vai dar para falar tudo o que eu gostaria. Mas proponho efetivamente que o projeto de lei que veio da Câmara dos Deputados e sofreu várias melhorias do Senado seja aprovado naquilo em que efetivamente haja consenso,. Essa identificação positiva, essas normas, essas disposições gerais que não têm natureza criminal, mas natureza cível dentro de um projeto de lei criminal, precisam ser discutidas em apartado.

Nós não podemos atrasar avanços importantes em razão de outros avanços que, efetivamente, são polêmicos. Eu acho efetivamente, Senador, que a inclusão digital fica comprometida, na medida em que estabelecermos qualquer tipo de burocracia, de restrição a acesso. Isso vai na contramão, sim, da inclusão; torna-se exclusão digital, principalmente quando há essa possibilidade da certificação digital. Sabemos o custo do certificado digital, com o qual a nossa população não tem condição de arcar.

Não poderia encerrar minha participação sem falar do Fundo de Universalização dos Serviços de Telecomunicações, o FUST. Quando esse fundo foi criado, em 1997, por meio do art. 81 da Lei Geral das Telecomunicações, no

processo de privatização das empresas do setor e de criação da Agência Nacional de Telecomunicações, qual era a intenção do legislador, acertadamente? A universalização da telefonia fixa. Acontece que, em 2000, quando a Lei do FUST foi criada, já havia a necessidade de universalização de acesso à Internet de banda larga.

A tentativa de utilização desses recursos, no ano de 2000, foi travada pelo Tribunal de Contas da União, que, em recente decisão, estabeleceu metas para que o Ministério das Comunicações criasse um cronograma e um programa para utilização desses recursos. Isso foi feito. Os primeiros 7 milhões de recursos do FUST já estão sendo utilizados para atender aos portadores de necessidades especiais. Foi encaminhada ao próprio Tribunal de Contas, bem como à Casa Civil, proposta de decreto para que seja regulamentada a utilização dos recursos do FUST, porque o decreto atual não se propõe a isso; trata apenas de repetir a Lei do FUST.

O FUST, como disse anteriormente, virou uma questão quase que filosófica, tese de pós-doutorado, quando, na verdade, deveria ser uma questão de bom senso. A trava de 1997 estabelecia a utilização desses recursos para obrigações de universalização, só que a LGT não traz o conceito de universalização. Então, o conceito de universalização difere de obrigações. Obrigações e universalização, essas, sim, são atribuídas a serviços de telecomunicações prestadas em regime público, mas a universalização da banda larga é dever do Poder Público.

Está na própria LGT, no seu art. 2º, que o Poder Público tem o dever de garantir, a toda a população, o acesso a serviços de telecomunicações, não apenas ao Serviço Telefônico Fixo Comutado — STFC. A nossa intenção é a de utilizar esses recursos não apenas onde seja necessário o STFC, mas estendê-los, sobretudo, à universalização da banda larga.

Agradeço a V.Exas. a oportunidade, em nome do Ministro das Comunicações, Hélio Costa, que se encontra em missão oficial na Turquia. Desde já, peço desculpas por não poder permanecer mais neste evento. Gostaria muito, mas fui convocado pela Casa Civil para tratar da televisão digital, e, portanto, terei que me retirar.

Muito obrigado a todos.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Dr. Marcelo Bechara, Consultor Jurídico do Ministério das Comunicações e especialista em inclusão digital.

Desfaz-se a Mesa.

Temos 7 ou 8 convidados para o seminário, especialistas no tema. Peço encarecidamente aos que já fizeram apresentações que nos dêem a honra de suas presenças, apesar do conteúdo de suas agendas. O Deputado Luiz Piauhylino, por exemplo, mudou a sua agenda, adiou o seu vôo. Se pudéssemos ouvir as demais pessoas e, a partir disso, estabelecermos um sadio debate, seria bom.

Chamo imediatamente para compor a Mesa deste seminário os seguintes expositores: Dr. Antônio Alberto Valente Tavares, Presidente Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet — ABRANET, nosso convidado e sócio de carteirinha; Dra. Ela Wiecko Volkmer de Castilho, Procuradora Federal dos Direitos do Cidadão do Ministério Público Federal, também sócia honorária da Comissão de Direitos Humanos da Câmara dos Deputados; Dr. Thiago Tavares Nunes de Oliveira, Presidente da SaferNet Brasil, nosso sócio benemérito — agora, já não sei mais que adjetivos usar *(risos)* ; Dr. Renato Opice Blum, advogado e consultor da Federação Brasileira de Bancos, a FEBRABAN; Dr. Sérgio Luiz Fava, Perito Criminal da Polícia Federal, representante da Dra. Dinamar Cristina Pereira, Delegada da Divisão de Direitos Humanos da Polícia Federal; Dr. James Görgen, Secretário-Executivo do Fórum Nacional pela Democratização da Comunicação.

Tenho a honra e a satisfação de anunciar a presença do Dr. Demi Getschko, conselheiro e representante de notório saber em assuntos da Internet no Conselho Mundial da Internet. Convido S.Sa. para compor a Mesa. Foi ele quem trouxe a Internet ao País, é o pai da Internet no Brasil, cujo nome é mais complicado do que Greenhalgh. Desculpe-me por tê-lo pronunciado errado.

Quantos somos na Mesa? Está faltando alguém? Pode vir todo mundo.

Esta reunião está sendo transmitida ao vivo pela *TV Justiça*, pela *TV Câmara* e pela *TV Senado*. Este seminário será matéria obrigatória nos próximos dias. *(Pausa.)*

Passo a palavra ao Dr. James Görgen, Secretário-Executivo do Fórum Nacional pela Democratização da Comunicação, por pedido dele próprio, em função do horário do seu vôo de retorno. S.Sa. dispõe de 10 minutos.

Desculpem-me, cometi um erro. Esqueci-me de chamar o Dr. Pedro Antônio Dourado de Rezende, professor do Departamento de Ciências da Computação da Universidade de Brasília, também nosso parceiro assíduo, a quem peço desculpas de público.

Com a palavra o Sr. James Görgen, por favor.

O SR. JAMES GÖRGEN - Agradeço à Comissão e ao Deputado Greenhalgh por receberem o Fórum Nacional para Democratização da Comunicação, da qual sou Secretário-Executivo. Trata-se de instituição que reúne 124 entidades da sociedade civil, entre as quais o Conselho Federal de Psicologia, a Federação Nacional dos Jornalistas, a CUT, a ABCCOM (Associação Brasileira de Canais Comunitários) e a ABTU (Associação Brasileira de Televisão Universitária), enfim, toda uma gama de entidades que não só estão cada vez mais ligadas ao setor de Internet, como passam a ser, inclusive, operadores do serviço, com a convergência de mídias e com a digitalização das comunicações.

Minha apresentação vai destoar um pouco do início da discussão, porque, na visão do Fórum, o direito à comunicação, desde a cúpula da sociedade de informação até a TV digital brasileira, perpassa todos esses novos serviços digitais entre os quais a Internet é apenas mais uma plataforma. Ela não é exclusiva nem perfeita; é mais uma. Dela derivam várias linguagens, várias culturas e várias formas de se lidar com o meio de comunicação, libertárias ou não.

Vou tentar mostrar isso muito rapidamente. Tinha-me preparado para usar um tempo maior, mas vou tentar resumir.

O ciclo histórico da Internet — o Dr. Demi pode me corrigir; sempre ficamos nervosos ao seu lado, pois é uma referência no assunto —, em todo o mundo, na nossa visão, realmente fecha uma lacuna importante. Tal ciclo começa com o interesse militar dos Estados Unidos em descentralizar seus servidores. É importante perceber que houve interesse militar do Departamento de Defesa em criar, no final dos anos 60, a ARPANET, a primeira rede mundial.

Depois, a comunidade científica e acadêmica se incorpora a esse esforço, porque, na Internet, nas redes — na verdade, na comutação e nos pacotes de dados — percebe uma grande floresta a ser descoberta, uma grande oportunidade de troca de informações, no sentido mais elevado do termo, que diz respeito ao descobrimento, à ciência e ao desenvolvimento da cultura. Essa comunidade começa então a se apropriar dessa rede, desenvolvida, inicialmente, pelo Departamento de Defesa americano.

Nos anos 80 e 90, dá-se a explosão tecnológica, principalmente a popularização de serviços comerciais de Internet no mundo. Vamos experimentar isso só no final dos anos 90, mas é importante perceber que, lá fora, todas essas questões que vimos tendo nos últimos 10 anos se dão há 20 ou 30 anos, e, mesmo assim, não se conseguiu chegar a um consenso sobre elas.

Agora, começamos a experimentar uma exacerbação da presença dos conglomerados de mídia nessa área. No momento em que a AOL, a America Online, se funde com o conglomerado Time Warner, a Internet deixa de ser um serviço como a comunidade acadêmica considerava até então, com um sentido libertário próprio, e passa a ser, cada vez mais, controlada e dominada por grupos econômicos, cujos objetivos específicos muitas vezes passam longe dos direitos humanos. Ainda se pressupõe que a busca incessante pelo lucro, por parte dessas empresas, esteja acima dos direitos humanos. Portanto, é fundamental este seminário da Comissão de Direitos Humanos para explicitar essa visão da Internet. O predomínio desses conglomerados está estourando agora e, na nossa visão, está começando a atingir todas as áreas digitais, não só a Internet.

A todo momento, vou defender a regulação da Internet, a regulação e regulamentação dos serviços de comunicação, a fim de não cairmos na “lei da selva”, onde lei melhor é lei nenhuma. Acreditamos, como o Senador e várias outras pessoas, que a lei possível, que será respeitada pela maioria da sociedade — sempre haverá rupturas e desrespeitos — é a que tenha o consenso de todos os setores da sociedade, inclusive dos cidadãos, do consumidor, e não apenas de empresas e do Estado.

Uma das contradições dessa realidade, e que se deu no mundo todo, foi justamente colocar em campos opostos coisas que, na verdade, muitas vezes são

complementares, ou seja, direitos sociais *versus* liberdades individuais; diversidade cultural *versus* padronização de conteúdo; identidade nacional *versus* globalização de mercado; liberdade de expressão *versus* direito à privacidade; inclusão digital *versus* exclusão social; sociedade de informação *versus* sociedade de saberes e conhecimento; auto regulação *versus* controle estatal.

O Fórum Nacional pela Democratização da Comunicação não acredita nessas visões extremas, mas sim no caminho do meio. Quando falamos em lei possível, falamos em um caminho do meio que poderia ser simplesmente uma metáfora da nossa vida. Precisamos deixar de encarar a Internet como um mito ou, como o Bechara disse, como um gueto, onde tudo acontece de modo diferente. A Internet é um alongamento da nossa vida, em todos os sentidos. Essa realidade, como ele disse e eu concordo, não é virtual; passa a ser real quando a comunicação em tempo real e o convívio entre as pessoas se estabelece.

Então, na nossa visão, os princípios básicos são os meios que norteiam os princípios da vida social, como se depreende dos arts. 4º, 5º e 220 da Constituição Federal. Nós agregamos o art. 220 porque comunicação social e comunicação interpessoal têm muito a ver com a manifestação do pensamento. Existe essa diferença na Constituição Federal, que inclui na comunicação social, no art. 220, direito à liberdade de expressão, direito à informação e comunicação, e não nos arts. 4.º e 5.º, como direitos fundamentais, apesar de acreditarmos que eles são fundamentais.

Depois, é preciso garantir a autonomia dos Estados. Temos que deixar de lado esse mito de que a Internet é mundial. Ela é mundial no sentido do alcance, mas não no sentido da regulação e dos limites. Enquanto houver Estado-Nação, vai haver regulamentações, leis e códigos estabelecidos, e não definidos em uma convenção coletiva em Genebra, da qual a sociedade mal participa, onde há definições para o mundo todo, em um processo de discussão e de diálogo que quase inexiste.

Pessoas como o Demi e outros componentes do Comitê Gestor conseguem estar lá, as empresas em massa conseguem estar lá, os órgãos reguladores em massa conseguem estar lá, mas a sociedade está de fora. Foi uma briga para, em todo o processo da Cúpula da Sociedade da Informação, a sociedade, os indivíduos,

os cidadãos e entidades da sociedade civil de trabalhadores serem ouvidos. Desde então, trabalhou-se com documentos da Cúpula da Sociedade da Informação paralelos aos documentos oficiais da OIT, porque quase nunca se deu brecha para a opinião da sociedade civil nesses processos, e eles continuam dessa forma.

Defendemos também o acesso ao conhecimento de informações públicas, basicamente as informações do Estado, mas também informações empresariais de interesse público. Outro mito que a Internet pode ajudar a desfazer é que, se vamos defender uma lei como a FOIA, que é uma lei pela liberdade de acesso à informação, ela tem que servir ao Estado e a empresas privadas que atuam em áreas estratégicas para a Nação, em áreas de segurança nacional, em áreas de interesse de infra-estrutura, de concessões púbicas. É importante não termos 2 pesos e 2 medidas para tratar várias áreas no caso da regulamentação. Precisamos tentar entender que tanto o Estado quanto os conglomerados econômicos, cada vez mais, exercem papéis fundamentais para a vida em sociedade. A responsabilidade de um conglomerado é tão importante quanto a do Estado em várias questões, mesmo em um conglomerado que não é de mídia, de qualquer área fundamental para a sociedade.

Atualização dos conceitos de comunicação social e comunicação interpessoal.

Estamos vivendo isso na comunicação no Brasil há quase 10 anos. Quando a convergência começa a se estabelecer, não se sabe o que é comunicação social e o que é comunicação interpessoal.

Quando estou falando ao telefone, trata-se de comunicação interpessoal, mas se passo a usar meu telefone para gerar um *blog*, que é transmitido via Internet para milhões de pessoas no mundo todo, isso ainda é comunicação interpessoal? O programa telejornalístico que passa pela manhã na tevê aberta, quando passa mais tarde, 2 horas depois, na tevê por assinatura, é comunicação social? Não, hoje em dia ele é enquadrado como telecomunicações.

É inacreditável a discrepância que toda essa floresta regulatória criou no Brasil, no sentido de que, quando se separou telecomunicações de radiodifusão no Código Brasileiro de Telecomunicações e quando se estabeleceu a Lei Geral, criou-

se uma anomalia, que é essa que estamos evidenciando agora não só na questão dos crimes de Internet, mas também na comunicação social como um todo.

É fundamental, portanto, rever códigos que levem à atualização desses 2 conceitos. Muitas vezes eu os vi aqui, de forma equivocada, em um substitutivo, e podemos dar várias sugestões para melhorar isso.

Conceito de rede pública e de rede única de acesso livre e gratuito.

Cada vez mais, no mundo todo, está-se revendo o conceito de que as redes privadas são a melhor saída para a comunicação e para as telecomunicações.

John Dvorak escreveu na *InfoExame*, uma revista que vocês podem acessar facilmente, que a melhor forma de garantir preço baixo, neutralidade da rede e acesso a condições isonômicas são as redes estatais de governo, controladas por governos, por Estados, com mecanismos de controle público.

O FNDC ajudou a construir a Lei do Cabo, em 1994, e desde então defende como princípio o conceito de rede pública e de rede única, que não foi respeitado no cabo, gerando endividamento das empresas de comunicação, com a expansão do *overbuild*, com várias redes construídas ao mesmo tempo, em paralelo. Defendemos que a rede é única e, por isso mesmo, precisa ter velocidade única garantida para todos; não pode ter etapas e preços diferenciados.

Aí há crime, também, na nossa visão. Os crimes não são só os do Código Penal, são crimes na dificuldade de acesso da população ao serviço. Hoje mesmo, em casa, por exemplo, pelo excesso de informação que eu baixo, estou sem Internet. A minha empresa de telefonia resolveu desligar minha Internet porque uso muita banda.

Isso tem que acabar no País. É o principal obstáculo ao avanço da inclusão digital, na minha visão, ou seja, tratar indivíduos que pagam valores interessantes, importantes, como pessoas distintas, que podem ser desligadas com um botão a qualquer momento. É invasão de privacidade, é desrespeito aos direitos econômicos fundamentais do indivíduo quando as operadoras de telefonia, e mesmo as operadoras de tevê por assinatura, começam a controlar a vida das pessoas, quem pode e quem não pode baixar arquivos, quem pode e quem não pode ver IPTV, porque a banda delas está sobrecarregada. Estamos pagando por ela. Então, é um direito básico do consumidor, que também está sendo desperdiçado. Tanto esse

código substitutivo quanto várias outras leis não estão dispostas a enxergar esse lado do cidadão.

Incentivo à adoção de serviços e conteúdos digitais com licença pública geral.

Acho que o Pedro vai falar muito melhor que eu sobre isso, porque é um militante do *software* livre e dessa área de GPL, de todas essas licenças de compartilhamento. Não vou, portanto, me estender, mas defendemos também que tudo isso seja permitido.

O substitutivo, como está aqui, mantém algumas restrições, que consideramos preocupantes, aos desenvolvedores de código fonte, de *software* livre e também de outros tipos de aplicativo para a Internet ou mesmo para celular e para TV digital, que vai haver muito agora. Acreditamos que pode haver enquadramento, e ilegal, ao considerarmos que uma pessoa que esteja desenvolvendo seu próprio código, às vezes baseado em idéias fundamentais, que são de domínio público, mas que foram registradas como de propriedade intelectual, acabe sendo presa simplesmente por querer fazer um *software* sem fins comerciais, sem ganhar nada com isso, porque são licenças distribuídas gratuitamente. Então, preservado o direito do autor, todo gerenciamento dessa área precisa ser relativizado. Isso traz desafios regulatórios, na nossa visão.

Vou concluir com os desafios regulatórios que se apresentam, na nossa visão, a partir daquele cenário sobre o qual conversei até agora com vocês.

Preservação da diversidade cultural e identidade nacional.

Cada vez mais, com a entrada desses conglomerados no mundo da Internet e pela telefonia, em todas as áreas de comunicação, vemos no mundo todo uma perda, tanto da diversidade cultural quanto da identidade nacional. Essa foi uma preocupação das entidades da sociedade civil na Cúpula Mundial da Sociedade da Informação. Preservar a diversidade das populações, as diferenças entre elas, é fundamental para fugirmos da padronização a que alguns tipos de código podem levar dentro da Internet.

Autonomia das Nações. Manutenção dos preceitos constitucionais, respeito a tratados e protocolos internacionais, delimitação de territórios digitais.

Veio à tona na Mesa essa discussão de, quando houver um código muito pesado sobre uma pessoa, ela acabar derivando e indo para outro país para praticar

esse ato ilícito. Na verdade, se esse outro país também regular de forma importante, rigorosa, a Internet, essa pessoa vai acabar sendo desestimulada ou vai ter que procurar guetos para praticar o ilícito que pretende. Então, cabe a cada país se preocupar com o seu território. Para isso, definir até onde vai o território digital de um país e onde começa o do outro é fundamental, na nossa visão.

Preservação do Conselho de Comunicação Social.

Eu já vinha falando sobre isso antes, essa idéia de que, quando se gera conteúdo de um para muitos, numa situação anônima, isso é comunicação social, independentemente do dispositivo que se use. Temos que deixar de regulamentar comunicação e sociedade da informação no Brasil por qualquer uma dessas tecnologias pelas plataformas; começar a focar na produção de conteúdo e não nas plataformas; começar a regular por camadas a cadeia produtiva desse setor e não simplesmente quem opera a infra-estrutura.

Entendendo a infra-estrutura dessa rede como supervias, infovias de informação, temos que entender que as pessoas podem colocar pedágios, mas não podem barrar a livre circulação das pessoas. As empresas não podem impedir que uma pessoa tenha acesso àquela avenida e nela circule com o seu carro, se ela pagar os impostos e tirar carteira de motorista. Então, temos que ter limite para esse tipo de cobrança e de impedimento de acesso a essas redes, que também são autorizações públicas. Falo tanto de radiodifusão quanto de telecomunicações.

Limites da concentração da propriedade. Já me referi a isso.

Mecanismos de controle público dos meios de comunicação de massa.

Isso, para nós, inclui também a Internet. Quando falo em controle público, não é essa falsa polêmica do controle estatal ou da censura. Na verdade, os Deputados e o Senador Azeredo sentiram na pele agora o que nós, do movimento social, sentimos na pele há alguns anos quando algumas entidades associadas ao Fórum Nacional pela Democratização da Comunicação propuseram idéias, como o Conselho Federal de Jornalismo, e mesmo o Governo quando propôs a ANCINAVE, ou seja, projetos que, por conta de um dispositivo que poderia dar margem a questionamentos, foram execrados publicamente.

Entendemos que nenhuma discussão no Brasil vai longe nessa área se não derrubarmos esse mito e guardar o esqueleto no armário. A ditadura trouxe-nos

muitas celeumas. Não vivi essa época, mas acredito que essa vigilância democrática não pode impedir outros avanços democráticos, que são as garantias dos direitos tanto dos indivíduos quanto das empresas. Temos de fugir desse mito e dessa polêmica. Sempre que a liberdade de expressão estiver sendo atacada, as empresas de comunicação correm a dizer que há censura; que qualquer Parlamentar de qualquer partido é censório, e começa a recuperar aqueles anseios do regime estatal.

Na verdade, temos de medir tudo isso. É quase infantil esse argumento, uma vez que todas as sociedades capitalistas do mundo têm regulações fortes nessa área. A liberdade do direito comercial não está acima das liberdades individuais. Fundamental só as regras para o conhecimento de gerenciamento de direitos digitais.

Muito obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - A Mesa agradece ao Dr. James Görgen, Secretário-Executivo do Fórum Nacional pela Democratização da Comunicação.

Concedo a palavra ao Dr. Antônio Tavares, Presidente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet — ABRANET. Esta é a segunda vez que S.Sa. está conosco, sempre trazendo suas preocupações e sua contribuição.

O SR. ANTÓNIO ALBERTO VALENTE TAVARES - Sr. Presidente, inicialmente agradeço o convite feito à ABRANET, o que muito nos honra.

Cumprimento todos os companheiros da Mesa, em especial o Senador Eduardo Azeredo, que comigo tem polarizado essa situação nos dias mais recentes, mas reafirmo publicamente o respeito que tenho pelas intenções de S.Exa., embora a discordância em muitos casos nos traga para o caminho da solução, para o consenso que buscamos também.

Talvez possa ser um erro meu, mas creio que, por um lapso, a versão distribuída hoje não corresponde à última que a assessoria do Senador nos enviou. Portanto, gostaria que fosse depois enviada a última versão, pois há alguns pontos que diferem. Há avanços que não estão reproduzidos nessa versão que foi distribuída, e gostaria que isso fosse corrigido, porque é fundamental.

A nossa apresentação é muito específica. Vamos começar pela preocupação que temos, porque a vontade é de acertar. Deve ficar clara que essa atitude é muito louvável por parte do Congresso Nacional. Mas precisamos ter cuidado. A vontade de acertar eventualmente pode levar-nos a cometer ou permitir a legitimação de outros crimes, de tão amplo que é esse projeto. Esse é um cuidado para o qual queremos chamar a atenção, e resulta de um exemplo que, ao desenvolvermos uma lei *anti-spam*, vários de nós estávamos presentes e percebemos que, ao dizer o que era e o que não era *spam*, praticamente estávamos legitimando *spam* de uma forma indesejável. Às vezes, ao se legislar, comete-se esse tipo de erro.

Ainda que se pretenda tratar este assunto como se estivéssemos resolvendo os problemas todos da Internet numa legislação brasileira, há pontos que precisamos cuidar no que ela interage com todas as outras redes globais. Temos uma proposta, e não é a primeira; por vezes temos ouvido dizer que a ABRANET não faz propostas.

Está aqui claramente uma proposta, além de outras que já fizemos, que se constitui no sentido de, primeiro, separar — aliás, o Sr. Senador já disse aqui que está disposto a fazê-lo — os arts. 20 e 21, que tratam especificamente dos provedores. É um grande avanço. Não precisamos polemizar mais.

Devemos reconhecer que, como já foi dito aqui, boa parte — mais de 90% — da tipificação dos crimes já está feita. Também é louvável que cuidemos, estudemos e analisemos o aspecto daquilo que não está cuidado. Por exemplo, a difusão dos vírus, dos códigos maliciosos, do *phishing* e do *scam*, que são efetivamente bastante perigosos.

É preciso fazer um esclarecimento público também sobre a quem cabe a responsabilidade por isso. Vamos entrar adiante nesse ponto, quando nos referirmos ao que os provedores fazem, como fazem e até onde pode ir a responsabilidade deles. Também é preciso definir o correto entendimento dos processos de autenticação do usuário, se é sempre resultante da existência de um cadastro do usuário, como nós também vamos ver adiante.

Como referencial daquilo que já disse, algumas das atitudes que têm sido tomadas por nós provam que temos um espírito propositivo e colaborativo. Na apresentação do Sr. Senador Delcídio Amaral, com a presença do Sr. Senador

Eduardo Azeredo, nós nos congratulamos que esse fosse um projeto que tivesse passado pela Câmara dos Deputados, pela Comissão de Educação e Cultura, porque é exatamente nisso que acreditamos. As leis não vão resolver o problema, embora eventualmente possam ser necessárias. Mas a educação é necessária, e nós precisamos estimular as boas práticas. Portanto, já nessa apresentação, da qual existem registros em vídeos que podem ser checados, nós dizíamos, com coerência, a mesma coisa.

Fizemos contribuições e propostas na apresentação do projeto de lei feito pelo Excelentíssimo Senador, num almoço da SUCESU em São Paulo. Fizemos também em um evento do *Valor Econômico*. Através de conversas telefônicas com o Sr. Senador, trocamos idéias, trocamos sugestões, manifestamos o espírito de respeito e da busca de consenso, do que acho que hoje estamos mais perto. Fizemos publicações estratégicas, quer na ABRANET, quer no Comitê Gestor, como quando patrocinamos a publicação de um livro que se chama *Crimes Cibernéticos.* Trata-se de um manual de investigação — não é um livro para todos —, um livro feito em conjunto com o Ministério Público Federal, em São Paulo, com apoio do Comitê Gestor e da ABRANET, no sentido de uniformizar os padrões de entendimento de investigação para os crimes praticados na Internet. A isso nós decidimos juntar aquilo que há muito tempo já existe, a *Cartilha de Segurança para Internet*, resultado do trabalho de um dos órgãos do Comitê Gestor e do NIC.br — Núcleo de Informação e Coordenação do Ponto Br, por meio do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o CERT.br.

Então, tudo isso se faz de forma propositiva e ajuda todos a entender que nós poderemos melhorar a Internet, às vezes, sem impor a regra de uma lei, que nem sempre poderá ser entendida, nem atingir a todos que precisamos.

Temos feito debates e entrevistas na mídia que eu acredito — pela forma como têm sido feitos — serem esclarecedores.

Vamos falar um pouco das formas de autenticação para que fique claro para todos. Há 2 tipos básicos de autenticação que o provedor faz. Isso serve para confirmar que já existe, sim, um cadastro de provedor, e que esse cadastro serve para validar a autenticação do usuário, quando ele se conecta ao seu provedor para navegar na Internet. É a autenticação feita por Hayes. Trata-se de um s*oftware* que,

ao conectar a base de dados através do ID *e* do *password,* permite que a pessoa se habilite a navegar na Internet. Esta não é única autenticação, porque quando se quer utilizar serviços de *webmail* e outros dentro da *web*, há necessidade eventualmente de outros tipos de autenticações.

Nada disso seria possível acontecer se não houvesse um cadastro. E como já foi dito aqui também, é evidente que a era dos provedores gratuitos passou. Por volta do ano 2001, surgiram vários provedores gratuitos. Contra eles a ABRANET se debateu e temeu que isso fosse uma ameaça ao crescimento da indústria de Internet. Ao se falar dos provedores, não se pode esquecer de que há muitos pequenos provedores, como se referiu o Senador, que fizeram a Internet no interior deste País. De outra forma, não se justificaria, economicamente, se estabelecer. Pegaram os fundos de economia e fizeram isso no interior deste País. Apesar de ainda haver muita exclusão digital, temos pulverização bastante significativa da Internet no Brasil. Temos de tratar o grande e o pequeno provedor no mesmo nível.

Vou voltar ao aspecto do provedor gratuito. Como disse o Dr. Marcelo Bechara, esses provedores surgiram na esteira de uma oportunidade de negócios, que não era exatamente provimento de acesso, e foi aproveitada uma falha da regulamentação de telecomunicações. Daí aproveitarem recursos que eram chamados distribuidores de tráfego, que, por meio de interconexão, lhes davam a sobrevida. Isso acabou rapidamente. Hoje esses provedores são talvez os que cobram mais caro. Eles também têm os seus cadastros bem atualizados.

Já entrei um pouco na página seguinte.

É, de fato, prática corrente e obrigatória dos provedores a existência do cadastramento — e aí se destaca o grande problema da responsabilização do provedor. Ele não tem acesso a nenhum tipo de base de dados oficial como, por exemplo, um setor da Receita Federal, que permita verificar se efetivamente aquela informação que está sendo dada pelo usuário é verdadeira. Como ele pode checar e assumir essa responsabilidade?

Embora tenha sido dito que não é espírito do projeto impor a certificação digital, sobre a qual vou fazer meu comentário daqui a pouco, em agosto, quando tratávamos desse projeto, induzia-se, sim — não intencionalmente, é verdade —, que a certificação digital fosse o caminho.

Quero deixar bem claro para todo mundo: nós, da ABRANET, acreditamos na certificação digital, respeitamos e entendemos que, quando for massificada, será certamente o elemento mais seguro de acesso à Internet. Mas, pelo preço que se pratica, ela fará certamente com que existam 2 Internets: a do certificado e a do não-certificado. E, com isso, não podemos, de forma nenhuma, concordar. Essa é uma preocupação nossa, e temos usado esse argumento. Sei que é um argumento veemente e, às vezes, pode fazer parecer que somos contra a certificação digital. Absolutamente não. No Comitê Gestor, temos tido oportunidade de discutir isso com o Renato Martini, da Casa Civil. E ele já sabe a nossa opinião. Precisamos evoluir um pouco mais nisso, continuar conversando.

Queremos que a inclusão digital se faça com acesso à certificação digital para todos. Costumo dizer que os grandes certificadores digitais, as agências de certificação digital são empresas do sistema financeiro, são os bancos, que hoje são também os principais prejudicados com os crimes de fraudes na Internet. Temos, juntamente com os nossos associados da ABRANET — o SERASA, por exemplo, tem participado ativamente da elaboração desse projeto, com suas opiniões —, discutido a forma de conseguir trazer esses preços para uma realidade de acesso a todos. No momento em que isso se popularizar, vamos dar todo o apoio a esse projeto, também com certificação digital, porque não somos nós que vamos dizer, nem para o mercado brasileiro nem para ninguém, que não apoiamos a segurança na Internet. Ao contrário, é isso que queremos.

Portanto, fica a provocação no sentido de que o Governo faça com que, talvez *on-line* ou de outra forma, os provedores tenham acesso a bases de dados públicas. Isso está previsto, inclusive, no projeto de lei. Quem sabe nesse caminho dividiremos responsabilidades. Não estamos fugindo da responsabilidade, só não queremos arcar com toda ela nem ser os vilões da história.

Quanto ao tempo de guarda *login/logout*, fomos convencidos pelo Dr. Demi Getschko, há algum tempo, que talvez um CD ou um DVD resolva o problema dos 3 anos do registro. Não nos opomos a isso. Só é preciso lembrar que vamos registrar *login/logout* e distribuir naquela altura.

Vou fazer mais um parêntese. Quando fazemos o *login/logout*, se eventualmente tivermos clientes do estrangeiro para validar, precisaremos saber a

hora que está sendo acessado. Para isso, o Comitê Gestor está trabalhando o projeto Observatório Nacional da Hora — o Dr. Demi Getschko vai falar certamente sobre isso. É importante termos todos os elementos válidos, caso contrário a hora poderá ser um elemento inválido de informação.

Não sei como está meu tempo.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Terminou.

O SR. ANTÓNIO ALBERTO VALENTE TAVARES - A SaferNet tem tido um papel fantástico nesse trabalho de melhorar a segurança e tratar os crimes cometidos na Internet. Certamente eles vão falar sobre isso.

A cadeia de valor tem-se relacionado muito bem — a ABRANET com o Ministério Público Federal, com o Comitê Gestor, com a SaferNet. Chamo a atenção para o fato de que há um trabalho muito importante feito no Comitê Gestor de Internet, nem sempre conhecido, que é o trabalho nessas áreas dos centros de tratamento de acidente, do *anti-spam*, do trabalho dos PTTs e dos trabalhos de indicadores de Internet. Esses trabalhos nos ajudariam também a ver que, às vezes, os números referidos no Brasil, de um jeito ou de outro, sobre patrocinadores de crimes, nem sempre são assim. Vamos nos ater às informações produzidas por encomenda do Comitê Gestor em pesquisas específicas.

Faço novamente um parêntese para saudar o trabalho dos PTTs, na presença do Dr. Nelson Simões, Presidente da Rede Nacional de Pesquisa, que tem integrado academias, comunidades e provedores, e faz um trabalho fantástico para nós.

Trouxemos mais do que uma proposta, trouxemos um compromisso público para que possamos continuar os esforços na prevenção e no combate à pornografia infantil, enfim, a todos os crimes cometidos na Internet. Sugerimos a manutenção permanente em *sites* de provedores, de forma destacada, selos representativos e campanhas também no âmbito das áreas referidas acima. Alertados os riscos de incriminação, portanto, já tipificados os códigos, devidamente separados, vamos continuar alertando e trabalhar de forma educativa no sentido de orientar nossos usuários para que se reduza a incidência desses crimes. E também nos propomos junto com o Comitê Gestor, com o Congresso Nacional, a promover eventos que ajudem sempre no esclarecimento desses pontos.

Nos contratos de adesão aos serviços, que são efetivamente a origem do cadastro de usuários, nós nos propomos fazer o que for necessário para que eventualmente algum dado que ainda hoje falte e que seja substantivo possa ser incluído. Estamos absolutamente abertos para que isso seja feito.

Quero referir-me de novo à nossa relação com o Ministério Público. Quando fizemos aquele convênio, os grandes provedores, a ABRANET e o Comitê Gestor com o Ministério Público, propusemo-nos, independentemente de mandado judicial, a aceitar em fase investigativa que a polícia nos solicite informação de dados cadastrais básicos, e estamos prontos para oferecer esses dados cadastrais para que a polícia possa fazer a sua investigação e não haja nenhum tipo de obstrução por parte dos provedores.

Isso está lá explícito na página da ABRANET, está lá o contrato, o convênio e pode ser esclarecido. E poderemos de novo criar o *link* para denúncias anônimas.

Uma reflexão: o projeto de lei que trata da limitação de acesso à Internet certamente expõe a privacidade e cerceia o direito à informação. Novamente, a maioria dos juristas sabe que 90% dos delitos cometidos já estão tipificados. Se pensarmos que, para cada nova tecnologia que está chegando — já falamos do Aimex, do iMESH, de várias tecnologias — teremos que fazer leis específicas, porque cada uma delas vai gerar circunstâncias diferentes, vamos ter o problema de nos entendermos aqui no meio.

Pergunto: em países onde o direito consuetudinário ainda impera, onde a própria Constituição tem uma vintena de artigos, como vamos mudar os hábitos, os costumes das pessoas? Quer dizer, talvez não sejam as regras, as leis escritas, que resolverão o problema.

Um posicionamento público. Uma carta que foi enviada ao Sr. Senador e assinada por essas associações e apoiadas por outras mais e a conclusão.

A ABRANET e o Comitê Gestor recomendam que caminhemos para um consenso. Se há que legislar, o mínimo é que se faça a legislação especifica, mas tentemos buscar, a exemplo do que já existe — provavelmente o Dr. Demi Getschko aborde esse tema —, o processo de auto-regulamentação, porque reparem: quando se fala de nomes de domínio, de atribuições, de números IP, não há nenhuma lei no Congresso Nacional que os estabeleçam ou que os definam. São resoluções

simples do Comitê Gestor que todos respeitam. Isso é auto-regulamentação, e este é um bom exemplo. Poderíamos pelo menos em parte seguir por aí para facilitar as coisas.

Era o que tinha a dizer.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Agradeço ao Dr. Antônio Tavares as considerações e, mais uma vez, a presença na qualidade de representante da ABRANET.

Vamos passar a palavra ao Sr. Pedro Antônio Dourado de Rezende, professor do Departamento de Ciências da Computação, na Universidade de Brasília.

O SR. PEDRO ANTÔNIO DOURADO DE REZENDE - Boa-tarde, senhoras e senhores. Agradeço ao Deputado Luiz Eduardo Greenhalgh o convite para participar desse evento.

Pergunta o Senador onde estão essas coisas que falam por aí os críticos a respeito do projeto de lei, mais especificamente do substituto do qual ele é Relator.

Especificamente em relação à privacidade, gostaria de propor que V.Exas. me acompanhassem para que pudessem tirar suas próprias conclusões. Vou começar relatando um episódio, que deve ser da lembrança recente de todos, ocorrido com a indústria bancária. Preocupado com as fraudes no sistema de auto-atendimento, em algum momento do passado os bancos começaram a instalar leitores de cartão nas portas das salas ou dos quiosques que davam acesso aos terminais de auto-atendimento. Provavelmente o computador leria a mesma informação que a máquina de auto-atendimento.

Lembro-me muito que aqui em Brasília o banco do qual sou cliente utilizou isso em todos os seus terminais, pelo menos em todos aqueles que eu precisava utilizar. Ocorreu que todos os clientes percebiam que aquilo era uma medida de segurança adicional, havia a tentativa de se identificar o usuário que adentrava no espaço onde estava a máquina de auto-atendimento. O espaço onde o correntista teria acesso ao auto-atendimento estava agora identificando o usuário.

Lá dentro tinha um balcão com alguns formulários. Antes, para se ter acesso aos formulários não era necessário se identificar, bastava a pessoa entrar na sala para acessar a conta corrente. Nesse ponto, sim, era necessário uso do cartão. Mas

a partir dessa medida de segurança, passou a ser necessário o uso do cartão para entrar naquele espaço também. Entretanto, em menos de um ano, percebi que esse banco retirou os leitores de cartão dessas salas.

Como a minha atividade principal é ser professor de Segurança Computacional e de Criptografia na universidade, não pude furtar-me ao exercício mental de entender o porquê daquele retrocesso. E não é preciso ter nenhum conhecimento específico de informática ou de criptografia para perceber o que havia ocorrido. A medida era de certa forma exagerada, e o benefício dela era desproporcional e menor do que o prejuízo que ela poderia acrescentar. É claro que uma pessoa que abrisse aquela porta com seu cartão magnético poderia, se não tivesse o devido cuidado ou a devida atenção, ou se não se preocupasse, permitir que alguém entrasse atrás dele antes que a porta se fechasse.

Se adotarmos uma medida parecida na Internet, vamos estar diante de uma situação mais delicada ainda, metaforicamente, porque vamos abrir uma porta no escuro. Além disso, esse local onde era instalado o leitor de cartão não era controlado específica e necessariamente pelo dono da máquina de auto-atendimento. A porta onde era instalado o leitor de cartão poderia ser controlada pelo proprietário do imóvel a quem o banco alugava aquele espaço.

E os bancos, em vez de tentar aprovar uma lei que responsabilizasse o dono do imóvel pela guarda, pela responsabilidade e pelo correto uso daquele mecanismo de identificação instalado na porta, resolveu tirar a leitora de cartão.

Muito bem. Isso diz respeito à eficácia quando se tem o ímpeto de implementar um sistema de controle de acesso universal para um espaço onde várias atividades estarão sendo executadas ao mesmo tempo. Alguém, ao conectar seu computador no seu servidor de correio eletrônico ou numa sala de bate-papo, por exemplo, vai rodar um sistema operacional com mais de 3 mil *softwares* intermediando essa comunicação. Ele não tem a menor idéia do que se faz enquanto ele está acessando a sala de bate-papo. Pode haver vírus, pode haver programa espião, que entrou ali sem o seu conhecimento ou sem o seu consentimento, apesar da cautela que ele possa ter na máquina dele.

Então, penso que é muito perigoso apostar na identificação via provedor e na responsabilização do provedor pela correta atribuição dessa informação à

autoridade judicial ou policial como uma bola mágica para resolver o problema da eficácia no combate ao crime digital.

Especialista em segurança na informática que sou, sei que isso é apenas um passo a mais, além de identificar o endereço IP do Usuário que está fazendo uma conexão. Mas, devido à complexidade da arquitetura da rede hoje, principalmente da plataforma que as pessoas vão usar para se conectar, essa não será uma solução final nem definitiva e, se contribuir, contribuirá apenas marginalmente para o problema da identificação de atos ilícitos, da autoria de atos ilícitos.

Mas estamos diante da afirmativa de que esse projeto de lei, como está, não vai violar a privacidade de ninguém. Não temos como saber, porque o projeto de lei não está em vigor. Temos opiniões, conjecturas, especulações, mas não há como saber, não há um paralelo a ser feito com situações anteriores.

Há cerca de 1 ano, o Secretário de Logística do Ministério de Planejamento, Sr. Rogério Santana, foi consultado pelo repórter do jornal *Estadão*, no dia 30 de novembro de 2005, sobre o que pensava do projeto de lei. Ele concordou com a necessidade da tipificação de novos crimes, mas fez o seguinte comentário: *"O problema do projeto são os acréscimos do Senador Eduardo Azeredo e de seu assessor, especialmente no inciso IV do art. 22".* Na ocasião, foi o que citou o Secretário Rogério Santana.

Então, para evitar que sejamos acusados de criticar o projeto ou o substitutivo ao projeto sem o devido conhecimento, sem estarmos devidamente informados, convido os senhores a fazer como fez o Secretário Rogério Santana, que leiam o inciso IV do art. 22 e perguntem a si mesmos que palavras usariam para descrever o que ali está sendo imposto ao provedor. Sugiro que tomem conhecimento de indícios e de ilícitos.

Estamos diante do mesmo problema que o Marcelo Bechara levantou. Trata-se do provedor pessoa jurídica? Do provedor máquina roteadora, que está recebendo e empurrando *bites* de um lado para outro da rede? O que significa tomar conhecimento? Sem saber o que quer dizer *"tomar conhecimento"* uma pessoa jurídica ou um roteador, eu não saberia como interpretar esse artigo de forma melhor do que usando a palavra rastreamento.

Se V.Exas. tiverem melhores sugestões estou disposto a considerá-las. Mas para mim não há melhor descrição do que essa do inciso. Mas então não haveria como saber se o projeto como está hoje, especialmente os arts. 20 e 21 e o inciso IV do art. 22 violam a privacidade?

O Senador alega que não temos como saber. Se buscarmos algum precedente para ter alguma medida de como avaliar a afirmação do Senador, poderemos encontrar uma situação em que se discutiu e se polemizou acerca de uma lei sobre informática ameaçando ou não a privacidade de cidadãos, especificamente, o mesmo Senador e o mesmo assessor e a privacidade mais importante numa democracia, a do sigilo do voto.

Pois bem. O Projeto de Lei nº 1.703, de autoria do Senador, foi aprovado sem nenhuma audiência pública no Senado e na Câmara, apesar de todos os esforços envidados por mim e por outros preocupados com o teor daquele projeto de lei. Certamente porque os Srs. Senadores consideram o Senador Azeredo um especialista na área não julgaram necessária audiência pública sobre aquele projeto de lei.

Aquele projeto de lei instituiu o registro do voto virtual para substituir o voto impresso como medida fiscalizatória aos partidos políticos para que fosse revogada a lei proposta pelo Senador Roberto Requião e pelo Senador Romeu Tuma, que vigeria em 2004 e que exigia a impressão do voto para efeito de fiscalização. O registro virtual do voto foi objeto de uma resolução de maio de 2004, do TSE, a Resolução nº 21.744, que proibiu os TREs de emitirem e entregarem aos partidos políticos, para o fim a que era devido, de fiscalização, os tais registros virtuais do voto, que é uma lista dos votos registrados na urna de forma embaralhada, por conta de um questionamento que foi levantado por um partido político junto ao TSE de que o registro virtual do voto poderia violar o sigilo do voto do eleitor, permitindo aos candidatos rastrearem a identidade do eleitor.

Se V.Exas. quiserem saber os detalhes, basta fazerem uma busca no Google pelo termo cunhado pelo autor do requerimento explicando como é possível, através do registro virtual do voto, violar o sigilo do voto. Basta buscarem pelo termo *"voto de cabresto pós-moderno"* que os senhores encontrarão, se o fizerem entre aspas,

cerca de 15 citações explicando o que levou o TSE a impedir que os Tribunais Regionais emitissem registros virtuais do voto por seção eleitoral.

Neste momento que lhes falo está em trâmite no Tribunal Regional de Alagoas um pedido de impugnação da eleição que deu vitória em primeiro turno a um candidato que as pesquisas até 3 dias antes consideravam como tendo a eleição perdida. O candidato cotado pelas pesquisas para ser eleito não consegue o registro virtual dos votos porque há um resolução que o impede.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Dr. Pedro, para sua conclusão, por favor. Depois passarei a palavra ao Senador.

O SR. PEDRO ANTÔNIO DOURADO DE REZENDE - Quando vejo num projeto de lei a tipificação do crime de acesso indevido culposo pergunto: quem das pessoas que acessam a Internet não pode ser enquadrada no crime de acesso indevido culposo? O que é acesso indevido? Não sei.

Sobre os questionamentos que não vou poder continuar a apresentar escrevi a respeito e publiquei no jornal *O Popular* e nos portais do Instituto Brasileiro de Direito e Informática e no meu portal. Estão à disposição. Na saída, há algumas cópias desse artigo onde procuro explicar minhas críticas.

Gostaria apenas de terminar, Deputado Greenhalgh, dizendo que um colega, profissional da informática há mais de 30 anos, fez numa carta aberta sobre o projeto de lei e a enviou a um Senador. Ele cita Lao-Tsé, 560 anos A.C.: *A medida em que restrições e proibições se multiplicam num império, quando o povo é sujeito à governança excessiva, o país descamba na confusão. Deve-se governar uma grande nação como se cozinha um pequeno peixe: sem exagero.*

Sras. e Srs. Deputados, senhoras e senhores que me ouvem, o único propósito das minhas críticas, quaisquer que sejam os adjetivos endereçados a elas, é evitar que esta Casa, a pretexto de combater crimes hediondos, cometa exageros que serão muito difíceis de serem reparados, uma vez aprovada e posta em marcha, como foi o caso da eliminação do voto impresso no nosso sistema eleitoral, diante de uma sociedade já acostumada com eleição como se fosse *video game*.

Muito obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Sr. Pedro Antônio Dourado de Rezende, professor do Departamento de Ciências da Computação da Universidade de Brasília.

Concedo a palavra ao Senador Eduardo Azeredo, que a pediu porque foi citado nominalmente.

O SR. SENADOR EDUARDO AZEREDO - Quero apenas esclarecer a questão do inciso IV do art. 22:

> *"Art. 22.....*
>
> *IV - informar, de maneira sigilosa, à autoridade criminal competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores ou Internet sob sua responsabilidade;"*

São denúncias normais que, se o provedor receber, teria que passar à autoridade competente.

O voto digital foi aprovado pelo Senado, pela Câmara e sancionado pelo Presidente Lula. De maneira que considero que isso não merece maiores comentários.

Trata-se de projeto que respeitou o avanço tecnológico do Brasil e, pelo que eu saiba, acabamos de ter uma eleição de 120 milhões de eleitores sem que nenhuma irregularidade tenha sido cometida. Acho que o sistema eleitoral brasileiro, pelo contrário, merece nosso aplauso.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado.

Vamos em frente.

Peço aos próximos expositores atenção quanto ao tempo de uso da palavra. No começo dos trabalhos somos tolerantes. Depois de determinado momento, temos de demonstrar certo autoritarismo, começamos a olhar para o relógio.

Quando eu estudava na faculdade de Direito, um grande professor chamado Manoel Pedro Pimentel ensinava-nos sobre o comportamento do júri. Ele sempre dizia uma coisa que não está escrito em nenhum livro de Direito: *"Quando você estiver na frente de um júri fazendo uma sustentação oral, olhar os jurados e eles*

começarem a se mexer, e se ao expor um argumento eles fugirem do seu olhar, mude rapidamente de argumento, porque o corpo fala, o corpo dos jurados fala".

Trouxe essa lição para minha vida parlamentar. Usei muito na tribuna do júri. E vou voltar a usar, porque fui mandado de volta para casa pelos eleitores de São Paulo. Vou voltar a fazer exposições para o júri, reabilitar esse princípio.

Digo isso porque noto que as pessoas começaram a se mexer, sinal de que o assunto tornou-se um pouco enfadonho. É necessário, portanto, que, ao fazermos as intervenções, respeitemos o tempo, sejamos breves, sobretudo para mantermos a atenção dos "jurados".

Tenho a honra e a satisfação de passar a palavra ao Sr. Demi Getschko, conselheiro e representante de notório saber em assuntos de Internet. Ele é um dos dois brasileiros que integram o Conselho Gestor Internacional da Internet. Foi quem trouxe a Internet para o Brasil.

Está aqui para falar conosco o pai da Internet. Mas não revelo quem é a mãe nem a idade dele.

Sr. Demi Getschko, fico muito satisfeito por ter atendido ao nosso convite para participar deste seminário. Já tinha ouvido falar muito de V.Sa. Como disse, é uma grata satisfação tê-lo conosco.

Com a palavra o Sr. Demi Getschko, pelo tempo de 10 minutos, para fazer as suas considerações.

O SR. DEMI GETSCHKO - Eu é que agradeço o convite, Deputado Luiz Eduardo Greenhalgh, Senador Eduardo Azeredo e demais Parlamentares. Sinto-me muito honrado de participar deste evento.

Sr. Presidente, vou fazer uma apresentação curta. Tenho aqui vários *slides*. Vou comentá-los à medida que forem exibidos. A idéia é tentar fazer um corte nesta discussão, ressaltar o que, digamos, é o espírito da Internet, os conceitos que nortearam a Internet até agora, e ver como podemos avançar mantendo esse espírito sempre em mente.

(Segue-se exibição de imagens.)

Não vou exibir algumas transparências, apenas fazem parte da documentação — estão à disposição.

A definição do que é uma rede de Internet, em maiúsculo ou minúsculo, que indica uma rede coordenada, como é o caso da Internet global, ou uma rede que usa a tecnologia chamada TCP/IP — existe essa distinção — não é importante neste momento. Também não é importante aqui identificar máquinas e serviços, que têm a ver com números, IP. São formas de rastrear delitos, crimes. São importantes para a investigação, para entender o mecanismo, mas não na discussão do projeto de lei, nosso objetivo.

Além dos números, existem os nomes das máquinas, que têm mais a ver com aspectos administrativos da rede. Ou seja, se possui o mesmo nome, pertence à mesma administração.

As próximas 3 ou 4 transparências servem apenas para mostrar que o Brasil, de alguma forma, participa desse esforço desde o começo da onda da Internet, e ele é bastante ouvido lá fora. Devemos, então, prestar atenção na repercussão, no exterior, das posições assumidas pelo Brasil. Exemplo disso é a forma de gestão interna. O modelo brasileiro é exemplar em vários sentidos. Todos os segmentos sociais participam do comitê, e de alguma forma regulam a Internet com orientação segura, porém com mão leve, sem ser impositiva.

As datas mostram que começamos por volta de 1988. Essa curva no *slide* mostra que decolamos em 1994/1995, quando lá fora também aconteceu a grande subida. Então, estamos em fase com o desenvolvimento lá fora.

Esse ponto do *slide* mostra os órgãos que administravam a Internet clássica — o IAB, o ISG. Por que eles estão aí? Para mostrar como foi gerada a governança inicial na Internet, como foram gerados os padrões, as formas de comportamento na rede, e que de alguma forma sobrevive. Uma coisa muito interessante ocorre na Internet: passamos por ciclos de extrema preocupação e depois resolveu-se e voltamos a manter a coisa como era mais ou menos originalmente.

A Internet absorveu ondas de novos usuários, como a WEB, que não existia na Internet original, as páginas, os conteúdos gerados pelos usuários, a interação, as comunidades, e mesmo assim ela consegue manter várias idéias que estão na sua origem e que consideramos caras para nós que gostaríamos de preservar.

Como comentei em analogia àquela administração clássica da Internet, o Brasil tem um bom exemplo a mostrar, que é o comitê gestor. Não vamos entrar nos

detalhes de como foi constituído. Existe um decreto presidencial que cuida da *raiz.br* na distribuição de nomes e números e propõe pesquisas, programas de desenvolvimentos — também não vou entrar em detalhes para não perdermos tempo com esses números.

Mais um *slide* na mesma tendência mostra, por exemplo, máquinas por domínio, máquina pelo ponto br. Somos o sétimo colocado entre os países — os Estados Unidos estão evidentemente descontados —, mas é uma posição importante — 1,5% da população de máquinas do mundo está aqui. Em domínios, temos mais ou menos a mesma figura. Atingimos 1 milhão no mês passado. Na composição atual do comitê gestor, tem gente do Governo, do setor privado, do terceiro setor e da academia numa composição muito rica, heterogênea, e que permite ao comitê representar os interesses da sociedade brasileira de alguma forma.

O CG tem um braço executivo, que é o NIC. Citei porque o Dr. Antônio Tavares mencionou na sua apresentação. O NIC tem, por exemplo, debaixo dele, o CERT, que é o que cuida da parte de segurança e tem a ver com o nosso projeto, porque gera também ferramentas que combatem ou permitem rastrear delitos.

As atividades do NIC estão aqui, não vamos perder tempo com isso também. A atuação do CERT, acabei de comentar, articula ações no tratamento de incidentes, desenvolve boas práticas para usuários e administradores de redes, fomenta criação de grupos equivalentes em outros lugares do País, tem uma formação de grupos de respostas incidentes que estão se espalhando pelo País e tem alguns cursos do Programa da Carnegie Mello e tem algumas atividades específicas quanto a *spam* e *honey pots*, que são armadilhas para prender atividades maliciosas na rede.

Esse é um texto de um professor da USP. Coloquei-o aqui, porque temos de ter em mente que a Internet nos trouxe alguns valores e modelos de sociedade de negócio que às vezes não percebemos o quão amplo e importantes são daqui para frente.

Todo desenvolvimento de *software* livre, por exemplo, foi conseguido, porque houve uma rede que permitiu a colaboração de milhares de pesquisadores sobre o mundo. Todo desenvolvimento do conteúdo que nos espanta hoje da WEB e da

Wikipedia é gerado pela contribuição de milhões de pessoas. A colaboração e a nova forma de pensar produção de riqueza que a Internet representa é um negócio muito importante. Essa é uma coisa que temos de ter em mente e, na medida do possível, preservar.

Uso duas frases antigas da Internet para mostrar esse espírito: a chamada Lei de John Postel, que diz que temos de ser liberais no que aceitamos e conservadores no que fazemos. Quer dizer, temos de aceitar certo grau de anarquia ou de mau comportamento, temos que nos preservar de fazê-lo, de aceitar um nível de *spam*, mas deveremos evitar e gerar. Em suma, essa seria uma regra se todos usassem. A Internet espera que isso seja seguido.

A segunda é a divisa do IETF, gerador de padrões da Internet, que diz que acreditamos em consenso — no final, essa palavra "consenso" foi bastante citada hoje, porque é o que norteia a criação de todos os padrões da rede e todos os paradigmas que ela segue. Como se consegue esse consenso? Cito o exemplo do conselho dos *top-level domain* europeus, os pontos países da Europa, o ponto IT da Itália, o ponto DE da Alemanha, o ponto K da Inglaterra. Eles se reuniram num negócio chamado CENTR, Conselho dos Top-Level Domain Nacionais da Europa, e descrevem, num documento de 2003, o Best Practices, guia de melhores práticas, o que eles consideram princípios básicos da Internet. Dizem que a Internet tem de ser auto-regulada — há que se constituir uma autoridade de baixo para cima, porque ela é constituída de milhares de redes cooperativas; ter consenso e transparência, fundamentais para a auto-regulação. Há que se ter ainda cooperação baseada em confiança e justiça.

Como se aplicam leis na Internet? Trechos do W3 Consortium, um consórcio que cuida dos padrões WWW, citam algumas dificuldades de aplicação de leis. Na rede, para todos nós, as fronteiras de países são difíceis de definir. A legislação local não é claramente aplicável, porque não se sabe exatamente o que é o local. Até tipificação de crime pode ser complicada, porque as legislações locais variam, e o criminoso pode se mover, saindo de um lugar onde aquilo é crime para um outro onde não o é. Então, essa é uma complicação que a Internet traz. Sempre temos de ter em mente isso.

Em segundo lugar, qualquer coisa que seja escrita em papel é rapidamente tornada obsoleta pelo dinamismo da rede. Então, talvez devamos escrever princípios e não detalhes, pois estes sempre acabam sendo superados.

Qualquer política que se faça deve ser uniforme. Se queremos combater *spam*, devemos ter uma política uniforme, se possível, com acordo entre todos os atores. Eliminar todo o *spam* brasileiro, por exemplo, significa eliminar apenas 1,2% de *spam* que uma máquina recebe no Brasil; continuamos com 98%, o que não resolve muito. Se todos fizerem a sua parte, resolvemos o problema. Então, há necessidade de colaboração e de uma política uniforme. Esse é o motivo dos fóruns de governança, tratados em Genebra — esperamos que evoluam.

Mitch Karpor foi o inventor do Lótus 1, 2 e 3 dos velhos tempos. Ele escreveu uma frase que diz que a arquitetura é, na verdade, a política. Quer dizer que a arquitetura é que define a legislação sobre a rede, porque a arquitetura traz embutida o comportamento.

O que devemos fazer no Brasil? É fundamental, por exemplo, preservar arquivos, mas também que eles tenham referência de tempo única. O comitê gestor assinou um acordo com o Observatório Nacional — o Tavares citou de passagem — e vamos distribuir tempo legal na Internet para que todos os provedores e usuários possam associar eventos a uma hora que seja única. Se se reporta a um evento com 3 minutos de diferença, por exemplo, pode significar 300 usuários para frente ou para trás, pois os números de IP podem ter mudado completamente.

A manutenção de *logs* é fundamental. O serviço deve ser configurado de forma segura. Deve haver política de uso aceitável, como dito pelo Tavares, quanto a, por exemplo, aceite de contratos e o uso desses contratos para resolver problemas.

Existem algumas recomendações técnicas que vão ficar disponíveis para os interessados.

Qual a sugestão para resolver *cybercrimes* ou outros problemas na rede? Primeiro, temos de combinar soluções diferentes e tecnologias. A tecnologia é fundamental para resolver boa parte dos problemas. Há que se investir em treinamento, atualizações profissionais, educar usuários, explicar como funcionam

os ataques, a engenharia social, fraudes, etc. Há que se cuidar também dos vetores de disseminação.

Neste ponto, cito um detalhe do projeto, que prevê que comete crime quem dissemina vírus. Vírus é uma boa tipificação, que não existia até agora. O que significa disseminar vírus? Posso disseminar vírus e não saber. Minha máquina pode estar contaminada e eu não saber. Sou um criminoso, por não ter tomado cuidado? Existem muitas máquinas zumbis por aí e certamente não são criminosas, mas vítimas, porque foram invadidas. Então, é importante que isso seja mais ou menos bem definido.

Cito um trecho de John Perry Barlow, muito criativo, escrito em março de 1994 — é um pouco antigo, mas dá para refletir:

> *"A proteção que devemos ter deve-se basear muito mais em ética e em tecnologia do que em leis. Devemos buscar formas não invasivas de identificar os participantes de transações, aumentando a confiabilidade delas. Criptografia será a base de proteção de informação e deve ser uma técnica largamente usada e disseminada."*

Para dar um exemplo, o E-bay é uma sucesso comercial, faz muitos negócios com fluxo de milhões de dólares. Ele tem uma forma de tentar tratar os participantes das transações: tenta identificar a pessoa, faz um depósito no cartão de crédito, para ver se identificam que o cartão é seu; tem uma política de reembolso, caso você não receba o que comprou. Cada participante na rede tem a sua forma de se proteger e proteger seus usuários. É difícil imaginar que alguma coisa geral vá proteger a rede como um todo, ou seja, cada um tem de saber onde o sapato aperta. Os bancos têm a sua tecnologia para proteger-se contra roubo de senhas, contra fraudes, como o teclado alfanumérico, onde se escreve o nome de trás para frente, etc. Ou seja, há várias formas de garantir que você, de alguma forma, seja identificado, sem que isso seja intrusivo, violador de alguma privacidade.

Tenho sugestões específicas sobre esse projeto. Sempre que possível, devemos usar a legislação existente, pois poucos delitos são realmente novos. Em sua grande maioria, trata-se de nova forma de praticar velhos delitos. A Internet é fortemente baseada em colaboração e auto-regulação. Devemos buscar formas de

aplicar esses princípios em nossas relações. Como qualquer ambiente, a Internet reflete o mundo real e, portanto, existem crimes e riscos. Quem entra nesse mundo sabe que está exposto a riscos. Quem vai ao centro da cidade às 10h da noites sabe que corre risco. Há situações de maior ou menor risco. Os usuários têm de ser educados e ensinados a conviver com eles. Não adianta querer uma superproteção, porque isso não resolverá nada, já que não existe em lugar nenhum do mundo real.

Sempre que houver novos delitos — e aí aplaudimos várias iniciativas que estão no projeto —, isso deveria ser tipificado. Pode ser que realmente a legislação seja necessária. Estranho, por exemplo, quando se fala em novos delitos, que associemos a tipificação com um controle de acesso. Darei um exemplo da vida prática que me vem à cabeça. Pode-se ter a carteira roubada dentro de um ônibus, o que é crime. Uma coisa é dizer que é um crime, outra, é dizer: *"Para entrar no ônibus, tem de mostrar a carteira de identidade."* O que isso resolveu? Provavelmente, nada, porque continuará tendo sua carteira roubada e teve o trabalho adicional de mostrar sua carteira de identidade ao entrar no ônibus. O crime existe e tem de ser tipificado e punido. Agora, o cidadão inocente tem de carregar um peso a mais por causa disso? Não sei se é uma boa idéia. Podemos chegar numa biblioteca e consultar um livro; agora, se eu pegar o livro e for embora com ele, eu o terei roubado. Agora, quando entramos numa biblioteca, ninguém vai perguntar qual o registro, o CPF. O mesmo ocorre num parque de diversões ou num local público.

A tipificação dos crimes está misturada com o controle de acesso. Não vejo o que tem o controle de acesso a ver com crimes.

Tenho aqui as últimas perguntas. O que é acessar a rede? Quando se fala em controle de acesso, se houver um *hotspot* público, há violação; se você deixou seu filho entrar no computador, é um crime. Qual exatamente a tipificação disso? Como compatibilizar acesso autenticado com inclusão digital? Se se quiser incluir uma cidade digitalmente, deve-se pedir a todo mundo que entre e tenha que mostrar uma assinatura. E o sujeito que está viajando, passou pela cidade não vai poder usar a rede? São coisas complicadas.

Esse fator evanescente que cito aqui é aquela história de que, se se espreme de um lado, corre-se para o outro. O exemplo é o do Brasil: temos o ponto br que

funciona bem e é um sucesso porque tem uma legislação um pouco mais restrita do que o ponto com, mas não é restrita em excesso. A Espanha restringiu o domínio ponto es para quem tinha marca e patente. Conclusão: tinha zero domínios no es. O pessoal precisa estar interessado em embolsar 10 dólares por registro, mas também não tão fechado, a ponto de espantar os usuários. Graças a Deus, temos um br que tem um milhão de domínios. Então, é fundamental saber que a Internet é volátil. A rede interpreta a censura como um defeito e o contorna.

Finalmente, acredito que não vamos melhorar o índice dos crimes prejudicando o acesso aos inocentes. Duvido que um criminoso se identifique, entre na rede e pratique um crime. Estamos querendo que o sujeito diga: *"Estou entrando aqui porque pretendo causar um dano."* Não acho exatamente que seja esse o caminho.

Termino com uma frase de Maquiavel, dizendo que o inovador sempre tem como inimigos aqueles que tinham vantagem com as velhas instituições. E há poucos defensores, porque ele não tem estrutura que o suporte; é fraco porque os adversários têm as leis aplicadas aos seus interesses e os que o apóiam não acreditam que vá dar certo. Os que estão do lado inovador, em geral, correm um sério perigo — eu não gostaria de correr esse perigo.

Obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado.

Passo a palavra ao Dr. Thiago Tavares Nunes de Oliveira, Presidente da SaferNet do Brasil.

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Boa-tarde a todos. Cumprimento-os na pessoa do Presidente da Comissão de Direitos Humanos e Minorias, Deputado Luiz Eduardo Greenhalgh.

Gostaria de parabenizar esta Comissão pela iniciativa de requerer e aprovar a realização deste seminário com o objetivo de debater as iniciativas legislativas em curso no que se refere à regulação da Internet. A Comissão de Direitos Humanos e Minorias tem tido em 2006 uma atuação protagonista no que se refere ao combate aos crimes cibernéticos contra os direitos humanos. Nada mais legítimo e adequado do que esta Comissão submeter esse requerimento, aprová-lo e realizar este seminário com esse objetivo.

(Segue-se exibição de imagens.)

Minha apresentação começa a partir da ótica de uma entidade da sociedade civil sem fins lucrativos, que tem como missão institucional defender e promover os direitos humanos na Internet. Sendo assim, não há ninguém na sociedade civil mais interessado em combater os crimes cibernéticos contra os direitos humanos do que nós. Evidente que sempre fortaleceremos e apoiaremos qualquer iniciativa razoável que tenha como objetivo essa finalidade.

Como premissa dessa discussão, trago um pouco da natureza do crime cibernético, o que já foi dito pelos palestrantes que me antecederam. Temos a possibilidade de usuários cometendo crimes contra vítimas em outro país, usando a infra-estrutura de um terceiro. Ou seja, a natureza do crime cibernético é essencialmente transnacional. Como lidar com esse fenômeno a partir de legislações e jurisdições nacionais?

Do ponto de vista legislativo, a iniciativa sempre reiterada é a da Convenção do Cybercrime, do Conselho da Europa, à qual houve a adesão de 43 países. Porém, muitas vezes esquecemos de olhar quem da Convenção ratificou o seu teor nos seus ordenamentos jurídicos internos. Temos 43 adesões hoje e apenas 17 ratificações; dessas, muitas são com reservas e ressalvas na aplicação de vários artigos da Convenção, como é o caso dos Estados Unidos, que aderiram, ratificaram com12 ressalvas. Os outros países em laranja, como Alemanha, Itália, Espanha, Portugal, Reino Unido, Suécia, aderiram, mas não ratificaram a Convenção.

Nosso desafio é saber como enfrentar os crimes cibernéticos contra os direitos humanos sem restringir o direito humano à liberdade de comunicação e expressão.

Trago alguns informes que podem ajudar-nos nesse nosso processo de reflexão. Este é um estudo feito anualmente pelos Repórteres Sem Fronteiras, organização da sociedade civil que atua no mundo inteiro e tem sede em Paris. A instituição Repórteres Sem Fronteiras monitora o grau de liberdade de expressão e liberdade de imprensa no mundo e faz um *ranking* desses países em relação à liberdade que cada um deles dá à sua imprensa e aos seus cidadãos no que se refere à expressão. O Brasil, no último relatório, de 2006, infelizmente caiu de

posição: hoje ocupa o 75º lugar no *ranking* dos países com maior liberdade de expressão e opinião.

Na semana retrasada, a mesma ONG, Repórteres sem Fronteiras, publicou estudo inédito elencando os 13 países inimigos da Internet no mundo. Treze países são totalitários, têm regimes não democráticos, limitam e censuram o conteúdo da rede e o acesso à mesma, impedindo o livre acesso e o livre fluxo das informações. Esta ONG também elencou os inimigos da rede, ou seja, muitos chefes de Estado que atentam contra esse princípio fundamental da liberdade, do direito à comunicação e à livre informação.

Eles fizeram um estudo que, para nós, é extremamente relevante. Gostaria de chamar a atenção para essa constatação que os Repórteres Sem Fronteiras identificaram. Dentre os modelos de combate a crimes cibernéticos está a opção pela restrição ao acesso à rede, exatamente o que está sendo discutido aqui sobre o projeto substitutivo, ou seja, combater os crimes cibernéticos impondo restrição de acesso à rede. A ONG Repórteres Sem Fronteiras identificou que nos países que fizeram essa opção existe uma correlação direta entre censura e falta de liberdade de imprensa.

Aqueles 13 inimigos da Internet, marcados em vermelho, são também os países que mais reprimem a liberdade de opinião, de expressão e o livre fluxo de informações. A ONG RSF também identificou que os países que estão discutindo ou que aprovaram propostas de limitação de acesso à rede também ocupam posições de destaque no *ranking* que limita de alguma maneira a liberdade de expressão e a liberdade de imprensa. Esse estudo está publicado no *site* www.rsf.org.

O mesmo estudo aponta que, só em 2006, 59 militantes dos direitos humanos, entre jornalistas, escritores e advogados, foram presos por suas manifestações contra o Governo em Estados autoritários, como a China, por exemplo. A China mantém hoje 61 internautas presos por terem se manifestado contra o regime totalitário chinês, ou seja, há patrulha ideológica, patrulha política da Internet.

A RSF lançou, diante dessa situação, um manual ensinando como o internauta deve fazer para criar um *blog* anônimo na Internet, como usar a Internet

de forma anônima e fugir do sistema de censura e restrição de acesso feito nesses países. Esse manual também está livremente publicado no *site* deles.

Vou me ater à proposta do substitutivo do Senador Eduardo Azeredo. O contexto brasileiro atual é este: temos um usuário criminoso, que se conecta à rede através de um provedor de acesso e usa um provedor de conteúdo para traficar um crime. O caso mais comum é o de pornografia infantil. O sujeito acessa a rede e, uma vez garantido tal acesso, usa um provedor de conteúdo para disseminar imagens de pornografia infantil. O rastreamento é feito de forma inversa: a partir da identificação dos log de IPs desse provedor de conteúdo, chega-se ao provedor de acesso e, através dele, pode-se chegar à máquina utilizada para a prática do crime, e, portanto, à identificação de quem estava utilizando aquela máquina naquele dia.

A versão atual do substitutivo, no seu art. 154-A, cria um tipo penal novo, que é o de acessar indevidamente redes de computadores, dispositivo de comunicação ou sistema informatizado, e prevê uma pena de 2 a 4 anos de reclusão e multa. Diz ainda que incorre na mesma pena quem permite, facilita ou fornece a terceiro meio não autorizado de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, e também que permite acesso ao usuário sem a devida identificação e autenticação. Nas modalidades em que o crime seja praticado sem intenção, ou seja, que esteja configurado o crime culposo, a pena é de 6 meses a um ano e multa.

Evidente que nós, como entidade de defesa dos direitos humanos, preocupamo-nos muito com a interpretação que pode ser dada a esse artigo. Entendemos que esse artigo não atende aos princípios gerais do Direito — e cito aqui apenas o princípio da taxatividade, que diz que a norma penal deve ser específica, objetiva e não deve dar margem a uma interpretação dúbia ou equivocada. Não conseguimos restringir o que vem a ser acesso indevido, que pode ser uma infinidade de condutas, praticamente qualquer coisa. Não concordamos com o argumento dos defensores do projeto, que pretendem deslocar para o Poder Judiciário o poder discricionário de decidir o que vem a ser acesso indevido ou não. Não concordamos que haja uma norma penal que transfira ao Poder Judiciário esse poder discricionário de se definir o que é um acesso indevido à Internet, dispositivo

de comunicação ou sistema informatizado. Isso pode ser utilizado contra os direitos humanos fundamentais e de forma arbitrária no Brasil.

Trago um exemplo. Na sexta-feira saiu uma pesquisa de uma empresa de segurança, que identificou que 49% dos computadores zumbis da América Latina estão no Brasil. Computador zumbi funciona da seguinte forma: há um usuário comum da Internet e um criminoso; esse usuário comum está acessando normalmente a rede, usando a rede para as suas atividades normais, como trabalho, estudo e pesquisa, comunicação, etc. Um criminoso, através do envio de um vírus ou um código malicioso, acaba instalando um *software*, um programa espião na máquina desses usuários. Através da instalação desse programa espião na máquina desses usuários, esse criminoso passa a ter controle efetivo sobre ela. Como eles fazem? Praticam esses crimes através dessas redes de computadores zumbis.

Nós, da SaferNet, neste ano, já fomos vítimas de 2 redes zumbis, uma com 100 mil máquinas e outra com 60 mil máquinas. É um ataque que não dá oportunidade de defesa porque o objetivo é tirar o servidor do ar, é derrubá-lo. De fato, eles conseguiram; nosso servidor ficou 23 horas fora do ar por conta de um ataque da rede zumbi. Fomos atrás do *log*, do *firewall* e chegamos a pouco mais de 100 mil endereços IPS, dos quais havia máquinas de mais de 20 países: da Itália, da Espanha, etc. Ou seja, máquinas de usuários comuns, porque o usuário não sabe que está infectada e sendo utilizada para a prática de crime.

A partir da interpretação do que está colocado no art. 154-A, esse usuário que está usando a rede de forma lícita e teve sua máquina infectada por um programa espião e integrada a uma rede zumbi pode ser considerado criminoso na modalidade culposa, por acesso indevido. Afinal de contas, o ataque, para todos os efeitos, está partindo dessa máquina que integra a rede zumbi. Alguém pode dizer: *"Mas cabe ao usuário o dever de manter o seu antivírus atualizado, o dever de comprar programas antispyware, sistemas de proteção, de instalar firewall",* etc. Ainda que o usuário assim o faça, não resolveremos o problema, porque existem falhas no *software*.

Notícia recente, de antes de ontem, mostra que na nova versão do Internet Explorer foi descoberta uma falha com poucas horas depois do lançamento, ou seja,

de alguma maneira, está-se transferindo a responsabilidade de eventuais falhas no produto para o usuário. Ainda que ele queira, não tem como se proteger.

Senhoras e senhoras, de acordo com a última pesquisa de sexta-feira, 10% dos internautas paulistas e 8% dos cariocas poderiam ser processados pelo crime culposo do art. 154-A, caso esse projeto de lei fosse aprovado e estivesse em vigor. Segundo estudo publicado, sexta-feira, pela Symantec, esses usuários têm suas máquinas infectadas como parte da rede zumbi.

Vejam o cenário que podemos traçar do que está por vir, do que pode ser colocado dentro desse guarda-chuva genérico chamado “acesso indevido”, um tipo penal, uma norma em branco, um crime de mera conduta. Ou seja, independe qual o objetivo do acesso, se causou ou não um dano. Basta acessar indevidamente — não se sabe o que vem a ser um acesso indevido, pode ser qualquer coisa — que o sujeito já praticou, já consumou o crime e tem de responder por uma pena de 2 a 4 anos, equivalente ao homicídio culposo ou acidente de trânsito.

O *modus operandi* do crime cibernético é incompatível com o que está sendo proposto no projeto de lei sobre o acesso à rede. O criminoso normalmente se vale de um provedor de acesso e também de serviços prestados por provedores de conteúdo, provedores de serviços.

O *modus operandi* clássico, tradicional do crime cibernético é o uso dos chamados *proxies*, servidores externos utilizados pelo criminoso para praticar crime de forma anônima, ou seja, dificultar o rastreamento desse crime. Isso é largamente utilizado pelo sujeito. Quando ele quer praticar um crime, normalmente se conecta ao provedor de acesso a um *proxy* e dispara o ataque. Quando se rastreia o IP ou os astros, chega-se ao *proxy,* que, por sua vez, não registra o *login* de quem o acessa.

A pergunta que mais me inquieta é a seguinte: como identificaremos o usuário que acessa a Internet por um provedor internacional? Ou seja, o sujeito que quer praticar o crime, não quer deixar rastro e quer furar o bloqueio do sistema de cadastro proposto. É simples: basta ele discar 00, operadora, código do país, código da cidade e número do telefone que se conecta ao provedor de acesso internacional que preferir. A partir dessa conexão, ele pode acessar um servidor *proxy* ou acionar uma rede zumbi e continuar praticando seus crimes. Onde está o registro desse

acesso? Em outro país, que não prevê o mesmo sistema de cadastramento que estamos discutindo aqui.

O cadastro, por si só, não é solução automática para o problema. Se assim o fosse, os bancos não teriam tantos problemas com contas fantasmas, com contas laranjas, com tantos crimes financeiros praticados no sistema bancário a partir de cadastros falsos. O cadastro de um sistema bancário é muito mais rígido do que esse proposto no projeto de lei. Ainda assim os cadastros bancários não conseguem conter a criação de contas fantasmas e o uso de laranjas para cometimento de crimes financeiros.

Este *site* nazista, que pratica crimes bárbaros de racismo, neonazismo contra direitos humanos, está sendo investigado, há 2 anos, pelo Ministério Público Federal de São Paulo. Logo na página inicial há informação de que os servidores estão armazenados nos Estados Unidos e que não estão submetidos à legislação brasileira. Esses criminosos se esquecem de que o princípio da obliqüidade garante à autoridade brasileira competência para julgar crimes praticados no Brasil por brasileiros ou contra brasileiros. Ainda assim é o uso de uma estrutura internacional para a prática de crimes. O *site* continua no ar.

Este outro *site* é sobre venda de pornografia infantil. Chamo a atenção dos senhores para o item 6, que diz o seguinte: *"Nosso site é ilegal em todos os países e por causa disso temos problemas, de vez em quando, com o nosso servidor. De vez em quando, nosso servidor fica fora do ar e fica inacessível, mas nós, rápida e efetivamente, resolvemos o problema e experiências similares nos permitem dizer que isso não excede 24 horas."* Ou seja, conteúdo criminoso migrando de um país para outro numa velocidade praticamente instantânea.

Este *site* aqui vende pornografia infantil. Quem a compra paga através de cartão de crédito.

Sugerimos ao Senador Relator incluir um inciso no art. 241 do ECA: criminalizar a conduta daquele que intermedeia o pagamento para compra de conteúdo ilegal, ou seja, aquele que está, de alguma maneira, garantindo intermediação de pagamento para compra e venda de conteúdo ilegal.

Estes números aqui, da Central Nacional de Denúncias, mostram que cerca de 1% das denúncias são referentes a provedores nacionais e 99% são referentes a conteúdos hospedados no exterior.

Há aqui uma grande dificuldade: o conteúdo ilegal hospedado no Brasil é facilmente retirado do ar e o provedor é notificado para que preserve as informações e as forneça mediante requisição judicial. No caso dos provedores de conteúdos internacionais, há uma resistência, haja vista a postura da empresa Google em relação aos crimes do Orkut, o qual, sozinho, responde por 93,6% das mais de 240 mil denúncias que recebemos este ano.

Este aqui é o exemplo de uma comunidade de pedófilos, que continua no ar, cujos criminosos estão trocando informações sobre crianças e narrando suas experiências e abusos sexuais cometidos contra elas.

O Ministério Público Federal de São Paulo, diligentemente, requisitou ao juízo a quebra do sigilo de dados telemáticos desses usuários; a Justiça Federal de São Paulo deferiu o pedido, e a empresa Google Brasil se recusa a cumprir as ordens judiciais. Ora, se temos uma empresa estrangeira se recusando a cumprir uma ordem judicial, quiçá uma legislação.

Isto aqui se refere ao modo como o processo está sendo feito, os impactos das rotinas do usuário e a questão do cadastro.

Trouxe alguns eslaides que mostram de que maneira o projeto, se aprovado da forma como está, impactará na vida cotidiana do usuário.

Muitos usuários, nas residências, compartilham conexão. Então, quem teria de fazer o cadastro? Apenas o assinante da linha? O assinante da conexão? Ou todos os membros da família que acessam à rede? Como ficam os telecentros e infocentros? Como ficam as pessoas que compartilham, de alguma maneira, sua senha de acesso à Internet no ambiente de trabalho? Todas teriam de se identificar? Todas teriam de ter acesso autorizado? Como fica a situação das crianças e adolescentes, que são inimputáveis?

É comum que haja nas empresas acessos públicos à rede. Aqui na Câmara, por exemplo, existe uma rede *Wi-Fi*. Através dela se consegue conectar à Internet. Como ficaria isso?

Todos esses exemplos podem estar, de alguma maneira, enquadrados nesse guarda-chuva chamado “acesso indevido”. No caso de membro de uma família ou usuário de infocentro, haveria ainda um agravante, a formação de quadrilha, uma vez que são três ou mais pessoas se reunindo para praticar um crime.

Encerro minha participação com a citação do Beccaria : *“É melhor prevenir os crimes do que ter de puni-los. O meio mais seguro, mas ao mesmo tempo mais difícil de tornar os homens menos inclinados a praticar o mal, é aperfeiçoar a educação.”*

Agradeço imensamente a todos pela atenção e ao Presidente pela tolerância.

Muito obrigado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado, Dr. Thiago Tavares Nunes de Oliveira, Presidente da SaferNet Brasil.

Concedo a palavra à Dra. Ela Wiecko Castilho, Procuradora Federal dos Direitos do Cidadão, representando aqui o Ministério Público Federal. Desde já, agradeço a V.Sa. a colaboração, a presença, a exposição, as opiniões e as opiniões do Ministério Público sobre o tema.

A SRA. ELA WIECKO VOLKMER DE CASTILHO - Sr. Presidente, senhoras e senhores, serei breve. Realmente, não tenho discordância nenhuma de tudo o que foi dito até agora.

Fica muito claro que o art. 154 é altamente problemático. O custo dessa identificação, com necessidade de cadastro presencial e uma figura penal culposa, trará benefício para facilitar a persecução penal.

Pelos estudos criminológicos e por todo estudo que se faz do sistema penal, cuja característica intrínseca é a seletividade, posso afirmar que esse benefício será praticamente impossível de comprovar. Em regra, a legislação restritiva é criminógena e faz com que novas condutas nocivas sejam praticadas à sociedade.

Diferentemente das questões abordadas aqui, explorarei um pouco alguns problemas do ponto de vista penal, na condição de professora de Direito Penal.

Chamo a atenção para o art. 163, que menciona dano por difusão de vírus eletrônico, digital ou similar. Na verdade, isso não é crime de dano, porque a conduta, aqui definida, é de criar, inserir ou difundir vírus em dispositivo de comunicação, etc., com a finalidade de destruí-lo. Então, essa conduta é meramente de perigo e não de dano. O parágrafo único diz que a pena é aumentada de sexta

parte se o agente se valer de nome suposto ou da utilização de identidade de terceiros. Não tem nenhum aumento de pena no caso de realmente haver um dano. O art. 266-A diz respeito à difusão maliciosa de código e, no §2º, diz que é isento de pena o agente técnico ou profissional que, a título de resposta ao ataque que seu sistema está sofrendo, manipula o código malicioso detectado em proveito próprio de seu preponente sem risco para terceiros.

Vejo isso como um exercício regular de Direito. Portanto, não é um caso de isenção de pena. Devo deixar claro que isso não é crime. A expressão "isento de pena" é antiga, do Código de 40, que às vezes é utilizada para a situação de exclusão de crime, mas é, de qualquer forma, uma expressão que pode se referir à causa de exclusão de crime como apenas uma causa de exclusão de pena.

Vejo uma impropriedade, quando se fala no art. 356 e se acresce um novo tipo penal como sendo 356-A. Não há previsão de pena. Sequer diz assim: será a mesma pena ou incorre na mesma pena. É uma impropriedade, quer dizer, tipo penal sem pena não é crime.

Chamo a atenção também quando se fala no aumento de pena para os crimes contra a honra. Se não estou enganada, o Superior Tribunal de Justiça já tem algumas decisões no sentido de reconhecer que determinadas condutas ofensivas à honra praticadas pela Internet em portais noticiosos, por exemplos, são consideradas crimes de imprensa e não pelo Código Penal comum. Então, estamos criando uma desproporcionalidade de penas, quer dizer, as pessoas vão fugir e dizer: estou praticando um crime de imprensa, crime contra a honra pela imprensa e não pelo Código Penal comum, por conta dessa desproporcionalidade de pena que agora está sendo proposta.

Talvez eu devesse ter começado por aí, mas há uma impropriedade muito forte quando se cria o Capítulo 7-A e o coloca no Título 1 da parte especial do Código Penal, porque se refere a crimes contra a pessoa, e as condutas definidas como crime no Capítulo 7-A não o são. O objeto jurídico, pelo que consigo deduzir da leitura, já que não está expresso, é a segurança dos sistemas de informação da rede de computadores. Isso está muito mal situado.

Fico me perguntando por que até hoje os crimes de violência sexual não conseguem passar para os crimes contra a pessoa e esse tipo de crime consegue

ser trazido para o Título 1, que reconhecidamente é o portal de entrada do Código Penal, aquelas condutas mais importantes, quer dizer, violadoras dos direitos humanos, dos direitos fundamentais.

Voltando ao que disse no início, depois de tudo que foi abordado aqui, tenho a impressão de que essa lei não ajudará a controlar o acesso indevido, a evitar o acesso ilícito. Pergunto-me o seguinte: por que nesse projeto de lei se fala tanto em autoridade competente, mas não sei quem é a autoridade competente? Imagino que exista mais de uma, porque determinadas matérias ficam mais subordinadas à fiscalização de um Ministério, de uma agência ou de outra. Isso não fica claro.

Sendo assim, comete-se até uma inconstitucionalidade, dizendo-se que o regulamento, a ser expedido por uma autoridade competente, que não sei quem é, estabelecerá uma série de obrigações, inclusive um sistema de fiscalização. Concordo que aqui há uma mistura indevida. Poderia até existir, numa mesma proposta legislativa, a criação de tipos penais e normas administrativas. Há muitas leis assim, mas acontece que aqui há um déficit de normas para montar uma estrutura administrativa de fiscalização que poderia ser utilizada em primeiro lugar, porque não devemos partir logo para a resposta penal se não temos sequer uma resposta administrativa. Essa é uma crítica que faço. O Senador não está mais aqui, mas não está também explicado isso na parte inicial do relatório.

Para terminar, Deputado, há um artigo indicado na parte inicial e que não consta desse texto distribuído para nós que se refere ao crime de não guardar dados de conexões e comunicações realizadas. Pergunto-me se isso foi retirado ou se realmente, na correria, não entrou nesse texto.

Termino minhas observações e espero não ter ultrapassado os 10 minutos.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Dra. Ela, muito obrigado. Suas considerações, como sempre, são extremamente ponderadas, judiciosas e profundas. De fato, já havia visto uma diferença entre a versão distribuída no Senado, para ser analisada na CCJ, e a versão distribuída hoje. Não quero dizer que tenha havido má-fé. Quando se é Relator de uma matéria polêmica, faz-se o relatório, depois uma penúltima versão e assim por diante. A última observação da Dra. Ela leva em conta a última versão do relatório do Senador Eduardo Azeredo.

Às 17h50min, passarei a palavra ao Dr. Sérgio Luís Fava, Perito Criminal da Polícia Federal, que, neste seminário, representa a Dra. Dinamar Cristina Pereira, Delegada da Divisão de Direitos Humanos da Polícia Federal.

Como se sabe, a Polícia Federal é o órgão investigador e repressor dos crimes na Internet. Aqui há uma polêmica muito grande. Já fizemos duas audiências com participação dos delegados da Polícia Federal. De vez em quando, temos sucesso, chega-se à autoria da responsabilidade criminal de quem pratica pedofilia, prostituição infantil, tráfico de drogas, de armas, de órgãos humanos, crimes contra a honra e, de outro lado, também há a idéia de que esse setor na Polícia Federal é extremamente ineficaz, insuficiente, ineficiente, não por conta da condição dos seus funcionários, mas da não-observação da importância que esse assunto tem na Polícia Federal e na estrutura pública.

Sempre recebo informações de delegados da Polícia Federal que tratam desse assunto, dizendo: Deputado, sou um delegado para não sei quantas mil denúncias; somos dois investigadores para não sei quantos mil casos. De qualquer forma, o Estado brasileiro tem de dar condições de trabalho, de investigação à Polícia Federal. É inconcebível que o Brasil tenha, a cada 30 dias, mil *sites* novos de pedofilia e 53% desses sites de crianças e adolescentes entre 9 e 13 anos. Pasmem os senhores e o Brasil, que está nos assistindo: 13% são referentes a crianças de zero a três meses de idade. O Brasil tem de acabar com isso. As pessoas têm de usar a Internet com responsabilidade.

Passarei a palavra ao próximo convidado, agradecendo-o por sua presença. O Presidente, de vez em quando, quer falar.

Dr. Sérgio Luís Fava, obrigado por sua presença. V.Sa. começa sua fala às 17h53min.

O SR. SÉRGIO LUÍS FAVA - Gostaria de agradecer ao Deputado Luiz Eduardo Greenhalgh pelo convite feito à Polícia Federal. A nossa instituição recebe muitas reclamações da sociedade, mas é um dos órgãos que não tem competência exclusiva para tratar desse tipo de crime, diga-se de passagem. Também as polícias estaduais têm a sua competência no que diz respeito a investigações e combate a crimes da Internet. Compete à Polícia Federal fazer a busca de vestígios do delito,

tendo em vista que recebemos denúncias. Portanto, a Polícia Federal faz o rastreamento.

(Segue-se exibição de imagens.)

Compete à Polícia Federal esse trabalho de investigação. Gostaria de mostrar algo que já foi falado. A minha intervenção é mais no sentido técnico e não no jurídico.

Essa história todo mundo já conhece. Se esse usuário quiser acessar a Internet, terá de obter um IP através do seu provedor. O número IP todos conhecem. São aqueles 4 números separados por um ponto. Esse IP que estou usando é fictício. Neste momento, o que temos? Esse provedor consegue registrar o momento da conexão. Isso já é feito por uma parte dos provedores, mas não por todos.

Vejamos agora um outro usuário fazendo o mesmo trabalho. Tenta-se fazer uma conexão, o provedor também fará o registro dessa conexão. A partir desse momento, esse usuário passa a ter acesso à Internet. Esse é um esquema bem simplificado de como isso funciona. O que ele fará na Internet?

Provedor de acesso é aquele que oferece conexão à Internet. Esse conceito ainda hoje não está perfeitamente compreendido. Por exemplo, aqui na Câmara dos Deputados, há alguns cabos como esse. Isso aqui é o fornecimento de acesso à Internet, ou seja, também a Câmara dos Deputados é um provedor, assim como outras centenas, milhares de empresas que também oferecem serviços de conexão a seus empregados, às pessoas que lá trabalham.

Já ouvi, numa discussão, alguém alegar que os provedores de acesso nacionais perderiam alguma coisa caso houvesse um cadastramento de usuários. Pois bem, para acessar a Internet, o provedor obrigatoriamente tem de ser nacional, a não ser no caso citado pelo Thiago, em que a pessoa se dispõe a pagar uma ligação internacional para conectar um provedor internacional. Muitos provedores nacionais de acesso não sofreriam qualquer tipo de restrição caso houvesse cadastramento. Isso não afastaria seus clientes. Eles podem ser pagos ou gratuitos.

Exemplos de provedores: órgãos federais, estaduais ou municipais, *cybercafes*, entidades religiosas, hotéis, aeroportos, universidades. Qualquer entidade que ofereça a seus usuários acesso à Internet é provedora. Esse é um conceito que deve ficar claro. Vejamos: uma empresa siderúrgica pode ser

provedora para seus funcionários; um órgão estatal também. Muitas vezes há cobrança da Polícia Federal para que obtenha resultados. O que houve? Identificamos que a origem de certo *e-mail* criminoso veio de determinada empresa. Essa empresa não tinha registro de quem fez aquele acesso. As empresas de outra natureza, e não só as provedoras de acesso, as mais conhecidas, também precisam passar a se preocupar com isso, e o projeto tem de contemplar esse tipo de coisa. Curiosamente, talvez as outras entidades também tivessem de fazer parte da Associação Brasileira dos Provedores, porque também são provedoras. É importante essa visão de modificação.

O problema vem agora. Se já estou conectado e tenho meus IPs, usarei a Internet para quê? Para acessar, por exemplo, *e-mails*. As ferramentas mais utilizadas no caso de pedofilia, de racismo e de ameaças pessoais são *blogs*, *chats*, Orkut e outros tantos serviços que oferecem hospedagem de *sites*. Posso criar um *site* gratuitamente, sem maiores informações. O que deveria ocorrer? Quando eu fizesse esse acesso a um tipo de serviço, ele teria também de registrar esse uso. Mas isso nem sempre ocorre. Muitas vezes esse serviço está no exterior, em outros países.

É importante saber que o provedor de acesso, aquele que no início deu acesso à Internet, em geral não tem conhecimento desses acessos aqui. Então, o projeto deve contemplar esse fato, porque o provedor de acesso passa a ser um mecanismo de passagem. Ele habilita uma passagem, registra a conexão inicial, mas o que o usuário faz depois é registrado pelos provedores de serviço.

O grande problema é que existe grande oferta de serviços; ou seja, é possível, sem muita dificuldade, encontrar provedores gratuitos no exterior para hospedar uma página. Esse provedor não exige nada do usuário, que cria ali sua página. Essa é uma das fontes para os *sites* móveis de pedofilia. Instala-se num país, num *site*. Se for tirado do ar, vai para outro local, e assim por diante. Esse provedor de serviço, na maioria das vezes, não é o mesmo provedor de acesso. Contrata-se um provedor para ter acesso à Internet, mas quem lhe fornece o serviço é um outro completamente diferente. Podem ser pagos ou gratuitos. Se houvesse reação dos usuários contra o cadastramento, eles poderiam buscar organizações de provedor de serviços no exterior. Essa seria uma possibilidade.

De qualquer forma, isso mostra que talvez a identificação obrigatória do usuário não seja um mecanismo muito eficiente para identificação desses vestígios na Internet. Então, precisamos discutir o assunto, porque é possível cadastrar-se no provedor de acesso. Isso já existe. Os provedores, na sua maioria, já fazem esse registro, ainda que o tempo de armazenamento dos dados não seja o ideal, o que está em discussão nessa lei.

Por fim, encaminho algumas sugestões. Deve-se destacar bastante o conceito de provedor, o que fará com que empresas e universidades também se enquadrem nesse mecanismo. Também as universidades públicas e privadas de qualquer natureza vão ter de guardar seus *logs* de acesso, de conexão por 3 anos. Muitas vezes isso passa despercebido. Essa é uma alteração que julgo importante no projeto de lei.

Outro ponto bastante importante: devem ser guardados os dados de conexão do que for feito no Brasil e também o acesso aos serviços. Sempre fazemos idéia de que na Internet há pessoas boas e ruins. Lembrem-se de que ninguém, em princípio, está isento de cometer crime. Eu não estou, ninguém aqui está.

Esses registros podem permitir que a Polícia Federal trabalhe. Muitas vezes chegamos a alguns deles e não temos como progredir. Muitas vezes pode parecer que há ineficiência, desleixo por parte da polícia, mas na realidade falta o registro das informações. Como já foi muito bem analisado neste seminário, temos de fazer a nossa parte.

Muitas vezes as pessoas instalam suas páginas ilícitas no País porque não há legislação. Vamos fechar aqui para que também outros locais fechem. Internet é um trabalho de cooperação. O fato de um país não agir dessa forma não é motivo para que não ajamos. Vamos fazê-lo para que, no futuro, outros países também tenham essa atitude.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Muito obrigado.

A minha intervenção sobre a Polícia Federal fez com que fosse bem objetiva a exposição do Sr. Sérgio Luiz Fava, Perito Criminal da Polícia Federal na área de direitos humanos. S.Sa. também trata das investigações sobre crimes na Internet.

Tenho a honra de passar a palavra ao Dr. Renato Opice Blum, advogado em São Paulo e Consultor Jurídico da FEBRABAN.

A FEBRABAN é uma vítima: milhões de reais são desviados, *hackers* invadem contas e transferem dinheiro — de acordo com a informação que tenho, cerca de 400 milhões por ano. Mas os bancos já tem prejuízo da ordem de 1 bilhão. Portanto, precisam de um sistema de segurança muito grande para seus clientes e usuários. Os bancos são, contraditoriamente, em função dessa situação toda, o ramo de prestação de serviços mais informatizado que existe.

Agradeço antecipadamente a participação ao Dr. Renato Blum, a quem concedo a palavra.

O SR. RENATO OPICE BLUM - Sr. Deputado Luiz Eduardo Greenhalgh, em nome da FEBRABAN, agradeço-lhe a oportunidade de participar da reunião com este seleto grupo.

Estamos tendo aqui uma prévia do que vai acontecer quando essas questões forem ao Judiciário. Parece-me que há uma linha com a qual todos concordam. Vou partir dela e chegar a uma palavra específica: consenso. Parece-me haver consenso quanto ao consenso. Não podemos perder tempo com aquilo em que há consenso. A posição da FEBRABAN quanto às situações em que ele existe é favorável. Aliás, é e vai ser favorável às iniciativas que colaborarem com a repressão aos crimes eletrônicos.

Somos dependentes das novas tecnologias. Existem situações extremas com as quais nos preocupamos. Elas envolvem Direito, que não é uma ciência exata pela sua própria natureza.

Tenho de falar da minha área de atuação. Não existe lei perfeita. Se existisse, haveria um problema com a classe dos advogados: poderíamos dispensá-los deste debate pelas inúmeras interpretações que podem ser dadas a determinados fatos na aplicação de um dispositivo legal. Essa imperfeição legal, que encontramos em qualquer lei, é resolvida ou levada à análise do Poder constituído — no caso, o Judiciário —, que não pode recusar-se a julgar determinado fato devido a eventual inexistência de legislação sobre o assunto.

Nesse ponto, cito pesquisa acadêmica que fiz. No Brasil há mais de 5 mil decisões judiciais que tratam de situações envolvendo ilícitos praticados por meios eletrônicos e pela Internet. Há decisões em que a questão da autoria foi intensamente debatida e apurada, mas, em razão da falta de determinadas medidas

e registros, não foi possível chegar ao responsável pela prática do crime. É essa situação que nos preocupa. Ela tem ligação direta com o interesse social.

O Deputado falou a respeito da situação que os bancos enfrentam. O Poder Judiciário tem posições interessantes quanto a problemas que envolvem tecnologia, eventuais fraudes e usuário. É com isso que a FEBRABAN se preocupa. Parte desses valores que estamos discutindo aqui pode estar indo para o crime organizado. Isso tem impacto no interesse social. A questão é muito delicada, e a FEBRABAN quer colaborar.

Se faço uma ligação para São Paulo, o acesso à rede de comunicações fica registrado? Se fica, por quê? Por que, no mundo inteiro, os automóveis são registrados? Por que os carros têm placa? Gostaria que a situação fosse distinta. O cidadão que eventualmente ultrapassa a velocidade limite deveria ir ao órgão de trânsito e confessar que não cumpriu determinado comando legal. Infelizmente, não é isso que ocorre no Brasil. E quem nos socorre? A legislação, que representa a necessidade de adequação legal em algumas situações, em especial no cadastro de conexão do sujeito que usa o telefone ou compra um telefone celular pré-pago. A lei determina isso e, em tese, deve representar os anseios da sociedade.

Peço licença para passar *slides* práticos de diversas situações.

(Segue-se exibição de imagens.)

Vejam esse caso e a gravidade da circunstância. Morte de jovem é assistida em fórum na Internet. Um jovem de 16 anos, morador do Bairro São Geraldo, em Porto Alegre, planejou a hora e o local de sua morte e compartilhou o momento de seu suicídio com outras pessoas em um fórum virtual na Internet. Além do *blog*, ele participava de fóruns virtuais de discussão. Grupos debatiam a questão do suicídio. Foi num desses fóruns que esse jovem encontrou pessoas que o incentivaram a levar adiante a idéia. Instigação ao suicídio é crime contra a vida. Além de darem a ele dicas sobre a forma considerada mais eficiente para se matar, os participantes acompanharam em tempo real o momento da sua morte.

Trouxe trecho de decisão judicial, das 5 mil que citei, a respeito de caso que ocorreu em Porto Alegre. Determinada pessoa — vítima — ajuizou ação de indenização contra fulano, narrando que passou a receber diversas ligações telefônicas no aparelho de seu consultório e no telefone celular, objetivando sua

contratação para a prática de programas sexuais. Tal fato teria se originado de uma divulgação publicitária na Internet, onde aparecia fotografia de uma moça em posições eróticas, com a indicação de seu nome, profissão, número de telefone e, inclusive, indicação da faculdade em que estudou. Ela relatou que passou a ser importunada constantemente pelas ligações telefônicas, inclusive com o conhecimento do fato por terceiro, espalhando-se o boato de que a autora era garota de programa, o que a fez retirar-se do clube de esportes ao qual era associada. Citados no processo, os réus alegaram que, embora possuidor do endereço eletrônico que supostamente teria enviado as mensagens, não foi o requerido responsável pelo envio do material, não tendo qualquer motivo para querer prejudicar a ex-namorada. Salientaram a inexistência de legislação no Direito brasileiro que regule as condutas realizadas via Internet. Difusa a possibilidade de atribuição da autoria, e do ponto de vista criminal também. Inclusive, a própria demandante poderia ter realizado a remessa dos e-mails com o intuito de prejudicar o ex-namorado, liquidando com sua possibilidade de casamento e com sua vida profissional. Esse tipo de situação pode trazer falsa compreensão e eventual prática de injustiça, o que não podemos permitir.

Na mesma seqüência, há decisão do Tribunal de Justiça do Rio de Janeiro. O direito ao anonimato, que tanto se discute, mas que a Constituição veda no art. 5º, inciso IV — ela garante liberdade de expressão, mas veda o anonimato; não temos sanção, mas há previsão — constitui um dificultador. É por isso que esse direito está sendo tão questionado. Não é tão direito assim. Aliás, é, ao contrário, uma restrição. Incentivar a clandestinidade na rede significa dizer que ninguém é obrigado a nada nem é responsável por nada. Não sou eu quem afirma isso — neste momento, não é a FEBRABAN —, mas o Tribunal de Justiça do Estado do Rio de Janeiro. Os provedores, como portas de entrada e saída da rede, são os que têm a possibilidade de averiguar os dados dos internautas que sejam seus clientes, propiciando que se investigue a prática de atos irregulares. Confesso que fiquei alegre quando o Tavares relatou aqui que os provedores estão se preparando para a guarda de registros durante 3 anos, como recomenda o Comitê Gestor.

Essa é uma referência à lei estadual de São Paulo, quanto à obrigação de provedores — vamos chamá-los assim — de *lan houses* e *cybercafes* paulistas

cadastrarem e guardarem os registros de seus usuários por 5 anos. Em tese, essa lei decorre do anseio popular do Estado. Existe lei municipal em sentido equivalente, na mesma linha.

Na seqüência, tentando trazer essa situação de representação dos anseios sociais — vamos legislar ou não, em que ponto e dentro do consenso; em relação àquilo que estiver fora do consenso, vamos trazer subsídios para a discussão —, temos um exemplo de crime eleitoral, o art. 72 da Lei Eleitoral:

> *"Art. 72.....*
>
> *I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;*
>
> *II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado (...)."*

Temos aqui a situação do vírus com finalidade específica. Pena: reclusão — pena mais grave — de 5 a 10 anos. Ou seja, o legislador entendeu que era uma situação grave. Na mesma linha, em lei mais recente, encontramos o termo "crimes falimentares". O que têm eles a ver com discussão envolvendo dados eletrônicos? Há também a situação do art. 168, que atribui conduta ilegal e criminosa àquele que destrói, apaga ou corrompe dados em computador ou sistema informatizado. Vejam como é interessante a definição de sistema. Há também a quebra de sigilo empresarial de forma indevida, que ocorre muito nos meios eletrônicos. Na mesma seqüência, vemos o legislador preocupado com isso. O Código Penal, com a alteração da Lei nº 9.983, de 2000, está há 6 anos em vigor. Que tipo de crime podemos acrescentar e discutir? Aquele que permite ou facilita o acesso indevido e aquele que utiliza indevidamente o acesso restrito. É claro que aí há conotação para sistemas de informações ou banco de dados da administração pública. A pena é de 6 meses a 2 anos.

Na seqüência, temos o peculato eletrônico. A pena é pesada: de 2 a 12 anos para aquele que altera informações, dados e recebe vantagem indevida em razão

dessa alteração. Outra norma prevê a mesma circunstância, só que não há o recebimento da vantagem. A pena é um pouco menor, é claro.

Uma situação retrata o consenso sobre a gravidade do crime de pedofilia — situação patológica. Do ponto de vista jurídico, estamos falando em tarado infantil mesmo. Trata-se da antiga redação de outra norma legal, que reclamou aprimoramento, até em função dessas discussões em vários processos. Na antiga redação: fotografar ou publicar. Na nova redação, em novembro de 2003: aquele que apresenta, produz, vende, fornece, divulga ou publica por qualquer meio, inclusive a Internet. Uma situação curiosa: vemos, no inciso II, co-responsabilidade de quem assegura os meios ou serviços para o armazenamento e aquele que assegura, por qualquer meio, o acesso à Internet daquele tipo de conteúdo.

Existe um detalhe que deve ser sempre lembrado: faz-se necessária a existência do dolo para essa conduta. O que é dolo? Liberdade, vontade, ação livre, voluntária. É diferente da culpa, em que há negligência, imprudência ou imperícia, numa situação menos grave.

O que está havendo no mundo, quanto a essa questão legislativa? Trouxe pequeno resumo. Em Portugal, há lei específica — Lei nº 109; nos Estados Unidos, há o Computer Fraud and Abuse Act; na Inglaterra, há o Computer Misuse Act; no Canadá, há no código penal específico a Seção 342; no Chile, há também previsão específica, assim como na Holanda, na Austrália, no Peru, na Itália, na Venezuela, na Espanha, na Alemanha, na Áustria, na França e na Espanha.

É importante fazer a ressalva técnica de que os países da Europa estão sob o comando das diretivas da União Européia, que tem várias diretivas sobre situação que envolve ilícitos por meios eletrônicos, inclusive quanto à guarda, à identificação e à eventual responsabilidade dos entes transmissores. Existem situações específicas de isenção dessas responsabilidades também.

Em relação ao código penal espanhol, trouxe casos mais curiosos. Há o do sujeito que usa tarjeta pirata, cartão pirata de televisão; aquele que facilita o acesso a um serviço de radiodifusão ou a um serviço interativo de forma indevida; aquele que, sem ânimo de lucro, facilita a terceiros o acesso por meio de comunicação pública; e aquele que fabrica, põe em circulação ou tem qualquer meio especificamente destinado para facilitar a supressão não autorizada e a

neutralização de qualquer dispositivo técnico para proteção. Isso é apenas um *overview* do que acontece.

Na Inglaterra, há a condenação pela criação de vírus, que se discute no Brasil, no substitutivo. Não estou falando em disseminação, mas em criação. A Procuradora Ela lembrou a questão do crime de perigo.

Aqui temos um pequeno resumo das situações de que a Convenção de Budapeste trata. Vai haver entre os signatários essa troca de informações. Como vamos reprimir situações de ilícitos eletrônicos que envolvem a extraterritorialidade, a transposição de fronteiras? Há alguma lei internacional para isso? Lei internacional não vai existir, mas existirão convenções e tratados. Essa será a forma jurídica adequada para esse tipo de tratamento.

Destaco ainda a importância do projeto quanto à adequação e à preparação do Brasil para que se promova sua adesão à Convenção de Budapeste, inclusive, de acordo com a Lei Complementar nº 95, em especial, na sua parte final.

Aqui temos um resumo de algumas situações mais importantes: dano pela difusão de vírus, que vai ficar de forma clara; difusão maliciosa de código; acesso indevido — assunto polêmico, como todo dispositivo legal que vai dar margem à discussão, pois é uma questão natural do direito; obtenção, manutenção ou fornecimento de informação eletrônica ou digital; violação e divulgação de informações; falsificação de cartão de crédito, situação importante da qual pouco se falou, que inclui a clonagem de telefonia celular e que vai ter um aspecto interessante no resultado final, na aplicação e na dosimetria da pena.

Por fim, trago uma questão que merece esclarecimento e até discussão. Hoje, se alguém monitorar transmissão de dados, perfis, o que o sujeito acessou e que *e-mail* ele mandou, sem ordem judicial, pratica crime. Isso está no art. 10 da Lei nº 9.296. A situação vai mudar com a discussão de hoje? Não. Até porque não há previsão de controle de fluxo nem de perfil. Estamos discutindo — pelo teor e pelo alto nível da discussão — a questão que envolve o cadastro e não a interceptação. Ressalto que interceptação é crime e vai continuar sendo, salvo se for feita com ordem judicial.

Peço desculpas pelo adiantado da hora, Deputado. Espero ter colaborado, em nome da FEBRABAN, e agradeço-lhe novamente o convite.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Obrigado.

É evidente que a exposição da FEBRABAN não é excludente de responsabilidade pela responsabilidade objetiva, nem sequer com esse projeto. E não é interesse do Senador Eduardo Azeredo transformar aquilo que é responsabilidade objetiva das instituições bancárias em responsabilidade subjetiva dos autores dos crimes da Internet.

São 18h25min. Estamos aqui desde as 14h25min; portanto, há 4 horas. O que proponho? Os nossos expositores que não moram em Brasília têm hora para sair. Então, em vez de abrirmos a palavra para 3 pessoas fazerem perguntas, vamos agir de outra forma. A não ser que haja contrariedade do Plenário. O Senador Eduardo Azeredo disse na sua exposição que concorda em não discutir os arts. 20 e 21 do seu substitutivo. Significa que, com o projeto do Deputado Luiz Piauhylino, o relatório do Deputado Nelson Pellegrino e as incorporações do Deputado Julio Semeghini, o projeto que foi aprovado por unanimidade na Câmara dos Deputados e que está no Senado Federal — é incontroverso o consenso sobre ele — será aprovado rapidamente. Assim, dotaremos o Brasil, talvez antes do final deste ano legislativo, de uma legislação que vai abranger 80% das questões. E continuaremos a discutir o cadastro, que é a questão controversa do projeto.

Lembro o que disseram o Senador Eduardo Azeredo e o Deputado Luiz Piauhylino. O primeiro relatório do Senador Eduardo Azeredo foi para aprovar o projeto como ele veio da Câmara dos Deputados — na Casa havia consenso. Depois disso, determinou-se a apensação de diversos projetos que estavam na CCJ. Foi aí que se estabeleceram novas idéias.

Há idéias novas que não são contraditórias nem conflituosas. A idéia do *phishing*, por exemplo, não tem nenhum problema. Conflituosa é a norma penal ampla de interpretação — acesso indevido, por exemplo. O que é acesso indevido? O que é cadastro geral? Aquilo que diz respeito à polêmica que se estabeleceu aqui. A intervenção do Senador Eduardo Azeredo pauta um consenso, uma iniciativa, um atendimento: a aquiescência do Relator no sentido de aprovar aquilo que é consensual.

O objetivo deste seminário é pedir à Assessoria da Comissão de Direitos Humanos que retrate as intervenções e as sumule, que estabeleça aquilo que era consenso para que tratemos rapidamente do assunto.

Ao mesmo tempo, sobram as outras questões: do cadastro; do crime de dano; do crime de perigo; as judiciosas observações da Dra. Ela acerca da norma penal em aberto, de seu uso indevido, de seu acesso indevido. Quer dizer, há necessidade de maior definição e do cadastro propriamente dito. Na minha opinião, isso fica para prosseguimento da nossa discussão. Até porque a ABRANET disse que está se preparando para modificar a relação contratual entre os provedores. Há experiências que estão sendo estabelecidas em outros países. Temos condições de fazer isso.

Espero que esta Legislatura, de apagada e vil tristeza — se me permitem a licença poética —, de 4 anos, não termine sem que tenhamos dotado o Estado brasileiro de uma legislação que está caminhando desde 1996. Que possamos estabelecer algum consenso nesse sentido.

Penso que não vamos abrir a palavra a V.Sas., mas sumular as intervenções de cada um e estabelecer um diálogo com o Senador Eduardo Azeredo sobre o que é consenso. Foi dito aqui que a palavra chave é “consenso”. Então, vamos deixar que o Senador Eduardo Azeredo submeta à Comissão de Justiça do Senado Federal aquilo que é a parte consensual que veio da Câmara dos Deputados, do Deputado Luiz Piauhylino, com as contribuições do Deputado Julio Semeghini, e mais algumas questões que são incontroversas, a fim de que sejam aprovadas agora. Que se dê força ao Senador Eduardo Azeredo para fazer esse jogo na Comissão de Justiça, porque, se houve apensação de outros projetos, os autores deles vão achar que seus projetos são de consenso. A sugestão é essa. Todos estão de acordo?

A SRA. ADA LEMOS - Não.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Por favor, identifique-se e explique suas razões no microfone.

A SRA. ADA LEMOS - Sr. Presidente, é muito louvável que V.Exa. queira buscar um ponto mínimo de convergência para a questão se fechar. Ela tem de se fechar em algum momento. Realmente, esta discussão não pode ficar *ad eternum*, tem de ter um fim. Mas acredito que o Senado Federal deva decidir isso. Uma das

grandes discussões é que os Senadores, afinal de contas, detestam ser homologadores das matérias que vão desta Casa para lá. E há muito ainda que se discutir no Senado.

Então, sugiro a V.Exa. que, em relação às questões institucionais que regem a diplomacia entre ambas as Casas, não trate o assunto como algo fechado daqui. Mesmo porque vários Senadores também vão querer opinar, discutir, fazer suas próprias audiências públicas. Sei muito bem, e V.Exa. também pode supor, que vistas serão solicitadas, que a Comissão de Direitos Humanos do Senado também convidará a Dra. Ela para falar. Então, esse curso tem de ser um pouco mais flexível.

Essa é a sugestão de alguém que convive com esta Casa há mais de 30 anos. O assunto é extremadamente sensível, sério e tem de ser resolvido da melhor forma possível, mesmo que se gaste mais tempo. É preferível que seja dessa forma, porque as leis só vigem quando há equilíbrio.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Diga o seu nome, por favor, e o seu local de trabalho.

A SRA. ADA LEMOS - Meu nome é Ada Lemos. Tenho 2 portais: Parlamento Livre e COMSOLI — Consórcio de Municípios para Soluções Livres. Já trabalhei muitos anos no Parlamento; tanto nesta Casa quanto no Senado.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Apenas para ficar registrada a participação de V.Sa. no nosso seminário desde o início, assim como a outras pessoas que estão aqui. Isso demonstra que V.Sa. é uma pessoa interessada no assunto e no funcionamento do Parlamento. Pedi a V.Sa. que dissesse o seu nome e o local onde trabalha para efeito de gravação do nosso seminário.

A SRA. ADA LEMOS - Para completar, todos os Parlamentares que aqui estiveram me conhecem há muitos anos — o Senador Eduardo Azeredo, o Deputado Julio Semeghini, o Deputado Luiz Piauhylino — e sabem que realmente estou preocupada com a melhor forma de se fechar algo tão importante.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Sem querer estabelecer polêmica com V.Sa., afirmo que o encaminhamento que dei vai ao encontro de suas preocupações. O Senador Eduardo Azeredo, no início da sua

intervenção, disse que estava aberto para rediscutir a questão dos arts. 20 e 21. E o Deputado Luiz Piauhylino, ao final da sua intervenção, afirmou que achava que deveria ser aprovado aquilo que fosse consensual, retirando-se aquilo que não fosse consensual. E incluía no consensual não o seu projeto, mas os acréscimos que não foram contestados, dos projetos do Senado. Apenas restringia a polêmica aos arts. 20 e 21.

Ora, se alguém diz que está de acordo com a aprovação e que tem dúvidas quanto aos arts. 20 e 21 — o Deputado Luiz Piauhylino também disse isso, e o Relator da matéria afirmou que está disposto a verificar tais artigos —, significa que tudo aquilo que é consenso não é consenso desta Casa, mas da Comissão de Constituição e Justiça do Senado.

Essa é a minha sugestão, para que o seminário tenha um objetivo concreto e possa contribuir com a Comissão de Constituição e Justiça e a relatoria, dando algum tipo de resposta à sociedade ainda nesta Legislatura. De qualquer forma, ao fazer a súmula deste seminário, vou dizer que não significa que ele esteja sendo feito a toque de caixa, que há prevalência exclusiva do projeto do Deputado Luiz Piauhylino ou do que foi aprovado na Câmara, mas que pode ter acréscimos. É só isso.

A SRA. ADA LEMOS - E muito menos ingerência desta Casa no andamento dos trabalhos da outra Casa.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Sim, direi isso.

A SRA. ADA LEMOS - Mesmo porque, se lá eles quiserem ter outra dinâmica, vão ter, independentemente de sugestões desta Casa.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Vou dizer-lhe uma coisa.

A SRA. ADA LEMOS - Muito obrigada, Sr. Presidente.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Agradeço-lhe a intervenção, mas o assunto nem de ingerência é. Até porque...

A SRA. ADA LEMOS - Cometi um preciosismo, Sr. Presidente. Obrigada.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Agradeço-lhe a retificação.

Vamos adiante.

Todos estão de acordo? Façamos uma súmula deste seminário e discutamos junto com o Senador Eduardo Azeredo, para que possamos avançar na aprovação deste projeto o mais rapidamente possível. Está bem?

(Não identificado) - Deputado, peço ao Tavares, sem nenhuma polêmica, que me encaminhe a palestra dele, porque realmente será a primeira contribuição que receberei da ABRANET. Poderei, então, incorporar a sugestão dele.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Estou aqui com os CDs dos palestrantes para que façamos um texto. Se estivéssemos no começo da Legislatura, faríamos um livro deste seminário, com a palestra de cada um, com as intervenções. Mas estamos no final da Legislatura. Então, o que vamos fazer? Atribuir ao Dr. Márcio Araújo e aos Assessores da nossa Comissão a tarefa de providenciar rapidamente a degravação do seminário, a fim que de possamos fazer uma súmula e discuti-la com o Senador Eduardo Azeredo e com os demais Senadores. Mas creio que urge uma resposta do Parlamento a essa questão.

O SR. ANTÔNIO TAVARES - Não é verdade, e não vamos fazer polêmica. Tenho documentos aqui em que o senhor reconhece isso. Não vamos fazer polêmica.

(Não identificado) - Eu não recebi.

O SR. ANTÔNIO TAVARES - Não vou assinar embaixo de tudo que...

(Não identificado) - Repito que não recebi esse seu material desde o início da discussão.

O SR. ANTÔNIO TAVARES - Está bem. Então é melhor o senhor trocar de provedor.

O SR. PRESIDENTE (Deputado Luiz Eduardo Greenhalgh) - Agradecemos aos convidados, aos expositores e aos demais presentes a permanência neste seminário. Agradecemos também à imprensa da Casa e à imprensa de fora pela cobertura. Os jornalistas dos principais meios de comunicação ficaram aqui até pouco tempo. Eu os observei daqui.

O assunto é palpitante. O Brasil precisa de uma legislação a respeito do tema. Estamos amadurecendo essa legislação, mas não temos condição de truncar a expectativa do povo brasileiro. Então, vamos fazer essa súmula da forma mais

isenta possível. Conversaremos com o Senador. Até porque, se S.Exa. não aceitar essa conversa, ficaremos em uma situação difícil.

Está encerrado o nosso seminário.