(*Texto com* *revisão*.)

**O SR. PRESIDENTE** (Zeze Perrella.Bloco Apoio Governo/PDT - MG) – Declaro aberta a 37ª Reunião Extraordinária da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática da 3ª Sessão Legislativa Ordinária da 54ª Legislatura, que se realiza nesta data, 15 de outubro de 2013.

Antes de iniciarmos os trabalhos da nossa reunião, submeto à apreciação do Plenário a dispensa da leitura e a aprovação da ata da reunião anterior.

Os Srs. Senadores que concordam permaneçam como se encontram. (*Pausa*.)

A ata está aprovada e será publicada no *Diário do Senado Federal*, juntamente com as notas taquigráficas.

Dando início aos trabalhos desta audiência pública, a mesma é realizada em atenção ao Requerimento nº 11, de 2013, de autoria dos Senadores João Capiberibe e Anibal Diniz, na qual debateremos sobre o Projeto de Lei do Senado nº 68, de 2010, de autoria do Senador Eduardo Azeredo, que revoga o art. 5º da Lei nº 12.034, de 2009, relativo ao voto impresso conferido pelo leitor a partir das eleições de 2014.

Temos a honra de convidar para composição da mesa: o Sr. Amilcar Brunazo Filho, moderador do Fórum do Voto Seguro na internet; o Sr. Pedro de Rezende, Professor de Matemática e Criptografia do Departamento de Ciências da Computação da Universidade de Brasília (UnB).

Informamos que foi convidado, também, o Sr. Giuseppe Janino, Secretário de Informática do Tribunal Superior Eleitoral, que declinou formalmente do convite.

Destacamos, oportunamente, que esta reunião contará com a utilização do serviço de interatividade do Senado Federal, que permite aos cidadãos encaminharem perguntas e comentários aos nossos convidados e, também, aos Srs. Senadores.

Além do envio de perguntas e comentários pelo Alô Senado, no telefone 0800-612211, qualquer cidadão pode acessar o portal e-Cidadania, pelo endereço www.senado.leg.br/ecidadania, onde também irá acompanhar a transmissão ao vivo desta nossa audiência.

As mensagens serão submetidas à triagem definida nos termos do uso do portal, não com base na qualidade dos comentários ou no mérito da pergunta, mas, sim, quanto ao cumprimento de regras de respeito e urbanidade, bem como de conexão com a finalidade do nosso debate.

Sobre esta audiência pública, destacamos a relevância da realização de um debate, no âmbito da CCT, sobre a adoção ou não do sistema do voto impresso como forma de comprovação e conferência pelo eleitor.

Num breve histórico e considerando que, anteriormente, havia votação por cédulas, houve a sua substituição pelo registro digital do voto, a conhecida urna eletrônica, a partir da Lei Federal nº 10.740, de 2003.

É sabido e indiscutível que os avanços com o voto digital foram enormes, pois, além da economia de recursos, deu-se ao processo eleitoral uma velocidade nunca antes experimentada, possibilitando, na maioria dos casos, que conheçamos o resultado das eleições até mesmo algumas horas após o encerramento.

Tornou-se, então, o processo eleitoral brasileiro vanguardista e reconhecido em todo o mundo como um dos mais modernos. Entretanto, a partir da edição da Lei Federal nº 12.034, de 2009, foi instituída a impressão do voto, sem prejuízo da coleta do registro digital pela urna eletrônica, valendo essa alteração já a partir das próximas eleições, em 2014.

Tal situação criou grande polêmica, pois, de um lado, os defensores da nova medida justificavam-se pela necessidade de conferir maior segurança e capacidade de aferição ao eleitor, o que daria uma maior proteção contra eventuais fraudes no processo eleitoral. Já aqueles que eram contrários argumentaram, em suma, que seria um retrocesso e um custo exorbitante a inclusão desse sistema, implicando nova alteração de todo o processo eleitoral. Na época, o coro contrário foi respaldado pelo posicionamento do Tribunal Superior Eleitoral que reagiu e manifestou sua opinião divergente contra o que seria um retrocesso. Então, a Procuradoria Geral da República ingressou com ação direta de inconstitucionalidade, requerendo a anulação desse dispositivo, argumentando que haveria quebra do sigilo do voto, o que foi acolhido em caráter provisório pelo Supremo Tribunal Federal.

Nessa mesma linha de pensamento, o então Senador Eduardo Azeredo apresentou o PLS nº 68, de 2009, que, entre outras disposições, revoga o art. 5º daquela lei, suprimindo assim o processo de impressão do voto.

É importante esclarecermos, contudo, que qualquer alteração deliberada a partir desse projeto do Senador Eduardo Azeredo não valerá para as eleições de 2014, pois o princípio da anualidade exige que modificações no processo eleitoral sejam sancionadas em até um ano antes de cada eleição.

Mostra-se, assim, a complexidade e polêmica do assunto. Por isso valorizamos ainda mais a iniciativa do Senador João Capiberibe, atual Relator da matéria em nossa Comissão, já que os debates que teremos agora podem auxiliar este Plenário em suas deliberações futuras.

Esperamos, então, ter aqui os melhores esclarecimentos por especialista, independendo de posição.

Lamentamos, mais uma vez, a ausência do Tribunal Superior Eleitoral. Eles nos deram uma explicação, inclusive a Ministra Cármen Lúcia. Pelo fato de terem de, a qualquer momento, decidir a questão dentro do Tribunal, achavam que não ficaria bem emitir qualquer tipo de opinião, pois poderia parecer que já estavam fazendo juízo de valor antes. Então, como essa matéria pode ser discutida lá, preferiram não participar do debate.

Ditas essas breves palavras e esclarecimentos, dando continuidade aos nossos trabalhos, informo que cada um dos expositores terá o prazo individual de 15 minutos, sem prejuízo da necessidade de sua extensão. Ao final deste bloco, passaremos a palavra aos Senadores autores do requerimento e, em seguida, aos demais Senadores na ordem de inscrição. Durante o curso da audiência, esta Presidência também poderá fazer intervenções, apresentando comentários e questionamentos enviados pelos cidadãos que nos assistem.

Ouviremos, então, na abertura das exposições, o Sr. Amilcar Brunazo Filho, moderador do Fórum do Voto Seguro na internet. Com a palavra o Sr. Amilcar Brunazo Filho.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Pela ordem, Presidente.

**O SR. PRESIDENTE** (Zeze Perrella.Bloco Apoio Governo/PDT - MG) – Pois não, Senador João Capiberibe.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Queria apenas saudá-lo, cumprimentá-lo por esta audiência pública e também agradecer a presença dos convidados. Acaba de chegar o Dr. Diego Aranha, já está presente o Dr. Amilcar Brunazo, o Dr. Pedro de Rezende. Muitíssimo obrigado pela presença.

Essa história do voto impresso remonta ao ano de 2002. Eu não estava no Senado quando foi aprovada uma lei estabelecendo o voto impresso, revogada em 2003. Depois, agora, em 2009. Então, há uma história de contradições entre o Tribunal Superior Eleitoral e representantes da sociedade civil que defendem o comprovante físico do voto, não apenas o registro digital.

Como eleitor, todas as vezes que vou exercer o direito do voto, eu me encho de dúvidas na frente da urna eletrônica, porque eu tenho certeza do que digitei, mas não tenho certeza de para onde vai o resultado daquilo que eu fiz. Então, eu tenho essa curiosidade. Esta é a primeira oportunidade que tenho de participar de um debate sobre o tema. Seria muito importante que estivesse aqui um representante do TSE para esclarecer as razões que levaram o Tribunal Superior Eleitoral a essa posição tão intransigente em relação ao voto impresso.

Nós somos legisladores e para fazermos leis que, de fato, correspondam à expectativa do cidadão e, nesse caso, do eleitor é fundamental a informação. Então, vou acompanhar esse debate com muito interesse. Mesmo que não tenhamos a oportunidade de aproveitar o resultado dessa lei para 2014, é fundamental que os telespectadores, aqueles que estão assistindo a esta reunião, o eleitor que quer cada vez mais segurança de que sua decisão seja respeitada nos acompanhem aqui pela TV Senado ou pela Rádio Senado e também pelo Facebook, pelo Twitter de todos nós. O meu é @joaocapi. Qualquer pergunta pode mandar para cá que vamos encaminhá-las aos convidados para que esclareçam, da melhor forma possível, o que, de fato, está por trás desse conflito de opiniões entre o voto impresso ou o voto às cegas, aliás, o voto às cegas, que esse voto apenas digital, e o voto impresso, que permite, depois, em caso de dúvida, uma auditagem que possa esclarecer o que aconteceu nas urnas.

Era isso, Sr. Presidente.

Mais uma vez, agradeço aos senhores convidados, lamentando profundamente a ausência do TSE.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Muito bem, Senador Capiberibe!

Passamos a palavra ao Sr. Pedro Rezende, que solicitou que fosse o primeiro a fazer a explanação, Professor de Matemática e Criptologia do Departamento de Ciência da Computação da Universidade de Brasília.

Com a palavra o Sr. Pedro de Rezende.

**O SR. PEDRO ANTÔNIO DOURADO DE REZENDE** – Bom dia, senhoras e senhores!

Agradeço ao Senador Capiberibe o convite para participar desta audiência, agradeço também ao Senador Zeze Perrella a oportunidade.

Pretendo fazer uma exposição teórica sobre a evolução da votação com o advento da informatização do processo eleitoral, do processo de votação especificamente, para, ao final, fazer uma crítica do projeto de lei em exame.

Pretendo seguir esse roteiro, que começa com uma história de como evoluiu o sistema de votação eletrônica no mundo.

É muito difundida a versão de que o Brasil é pioneiro na adoção do primeiro modelo de votação eletrônica chamado Direct Recording Eletronic, que não permite recontagem cuja verificabilidade depende inteiramente da integridade do *software* usado para coletar votos na máquina de votar e no sistema de totalização que soma os boletins de urnas eletrônicas.

O país pioneiro na adoção desse modelo primitivo de votação eletrônica foi a Holanda. Em seguida, adotada pelo Brasil em 1996, cuja lei eleitoral ainda exigiu o registro material do voto, razão pela qual em 1996 as urnas eletrônicas imprimiam o voto e o coletavam numa urna de lona para seguir a lei. Mas como havia a contagem eletrônica com a totalização rápida, não foi usado o registro material para conferir a contagem eletrônica. Aquilo funcionou como um teste. Em 1997, foi aprovada a lei que extingue o registro material do voto, a primeira lei eleitoral brasileira que trata da votação eletrônica. Mais adiante vamos ver um histórico de como evoluíram as leis de votação eletrônica.

O mundo não parou aí. Com esse experimento, ou com essa introdução pioneira do primeiro modelo de votação eletrônica, países onde a democracia foi reinventada na era moderna, como França e Estados Unidos, logo perceberam que o modelo original, DRE, o primeiro que foi experimentado e que extinguiu o registro material do voto, tinha a conveniência ou a vantagem de extinguir as formas de fraudes conhecidas até então – eram fraudes de varejo e visíveis, porque manipulavam o registro material do voto ou as planilhas de soma dos votos impressos –, mas, por outro lado, ocultava as novas formas de fraudes que a manipulação via *software* permitia, essas mais insidiosas, porque, agora, possíveis por atacado e invisíveis.

E o que fica de lado quando se defende o modelo inicial, DRE, é fazer vista grossa à possibilidade da manipulação do resultado da votação através do *software*.

Então, os países que se preocuparam com isso – os Estados Unidos, por exemplo, em 2006 – aprovaram legislação que dava preferência pelo segundo modelo de votação, que surgiu a partir daí, o VVPT.

Por último, surgiu a terceira geração de modelos de votação, baseado num sistema de auditabilidade ponto a ponto, que permite o rastreamento do voto, sem quebrar o sigilo da identidade do eleitor que registrou o voto, de ponta a ponta, na cadeia de custódia do registro do voto.

Bem, sou responsável pela introdução dessa nomenclatura, que classifica os sistemas de votação baseada nos modelos de votação eletrônica que seus correspondentes dispositivos de coleta projetam: DRE, registro eletrônico puro; VVPT, é o que permite uma trilha de recontagem por registro individual, material, do voto; e E2E é End-to-End Auditable, auditabilidade ponto a ponto.

Por que essa classificação? Porque esses modelos de urna surgiram na literatura científica nessa ordem cronológica, para tentar resolver os problemas considerados mais graves da geração anterior, do modelo anterior. O DRE entrou para resolver os problemas da fraude no voto em papel, mas introduziu a possibilidade da fraude por atacado e invisível, por manipulação do *software*. O VVPT entrou para eliminar a vulnerabilidade do modelo DRE, que concentrava toda a verificabilidade da lisura do voto na integridade do *software*, o que, para aqueles que trabalham com segurança em informática, sabemos que é um processo altamente ineficiente tentar verificar a integridade de *software* num processo da dimensão da votação eletrônica no País. E temos experiência prática disso ao tentarmos auditar o *software* usado na votação eletrônica. Podemos testemunhar tecnicamente a total ineficácia do processo. Ele serve apenas para manipular o sentimento coletivo a respeito de como estão as coisas, qual o *status quo* do processo de votação; não serve a título de fiscalização, como regime eficaz.

Por isso o resto do mundo, a partir do meio da primeira década do século XXI, começou a introduzir os modelos VVPT. Mas o modelo VVPT – o TSE tem razão nisto – tem o problema de não conseguir distinguir, quando há discrepância entre a contagem eletrônica imediata e a contagem para verificação manual, onde estaria o problema, o erro ou a manipulação indevida, se na contagem eletrônica ou na contagem virtual. Então, o sistema VVPT favorece a sabotagem, porque quem sabe que vai perder a eleição pode agir da forma antiga, manipular registro material, para provocar uma discrepância na contagem e, assim, lançar a dúvida.

Qual seria a saída?

Vou tentar explicar como evoluíram, porque a terceira geração justamente busca resolver os problemas que o VVPT trouxe ao tentar resolver os problemas da primeira geração.

Aqui, temos um desenho da cadeia de custódia do voto. Isso eu tirei da literatura que o Dr. Amilcar Brunazo produz no Fórum do Voto Seguro. Eu acho muito interessante porque resume muito bem o processo de votação desde o cadastro eleitoral, que estamos vendo nessa ponta da cadeia de custódia do voto, onde o mesário verifica a identidade do eleitor para permitir que ele se dirija à urna e registre o voto.

O problema da urna DRE é que ela interrompe a cadeia de verificabilidade do registro do voto, da integridade do voto, no momento em que o voto está sendo coletado e somado dentro da urna, porque ninguém sabe como o voto está sendo somado dentro da urna. No final da eleição, ele produz um boletim de urna, uma planilha eletrônica com os totais por candidato, por cargo, em votação, mas sem que ninguém tenha – ninguém de fora, que não tenha conhecimento de como o *software* que está rodando ali está fazendo sua tarefa, se corretamente ou não – como saber se a soma está correta.

Então, saem os BUs, que são totalizados e somados numa outra planilha global para dar o resultado final da eleição. Esse processo ainda pode ser verificado se o registro material do BU, que é o Boletim de Urna impresso, puder ser conferido com o resultado total por amostragem, por exemplo.

Em 1997, foi aprovada uma lei que tirou do eleitor o direito de fiscalizar a contagem dentro da sua seção eleitoral em troca da possibilidade de ele poder auditar o *software*. O mundo logo percebeu que essa troca não era vantajosa. Enquanto isso, no Brasil, a gente mantinha o modelo DRE sob o argumento de que o que tínhamos era muito bom porque ninguém conseguia provar que havia fraude, mas, por outro lado, também ninguém consegue provar que o resultado está correto.

A segurança do processo eleitoral é baseada puramente na confiança na autoridade que executa o processo, ou já que a fiscalização permitida não tem nenhuma eficácia em termos de auditoria do processo de votação *per se*.

Já escrevi mais de 70 artigos, dei mais de 40 entrevistas, desde o centro acadêmico da faculdade da esquina até o *Los Angeles Times*, explicando o porquê dessa ineficácia. O mundo desistiu do modelo DRE já na primeira metade da década de 2000 devido a essa ineficácia intrínseca de se concentrar a verificabilidade do processo de votação na verificabilidade da integridade do *software*.

O que temos no Brasil é uma estratégia de promover a segurança do ponto de vista da percepção do usuário, do eleitor, de que temos um sistema seguro, já que ninguém consegue provar que tenha havido fraude em alguma eleição. Então esta é a maneira de manter o sistema de votação de primeira geração: manipulando a opinião pública sobre a condição de proteção que aquele sistema oferece. Enquanto isso, estão sendo cerceados os direitos de fiscalizar nas outras etapas do processo de custódia do voto.

Com a identificação biométrica, o eleitor perde a capacidade de verificar, ao contrário do que a propaganda afirma de que o eleitor que está votando é mesmo aquele em cujo nome a urna foi liberada já que a identificação biométrica, ao contrário do que faz parecer a propaganda oficial, não é um processo determinístico, é um processo probabilístico, portanto, propenso a erro de natureza intrínseca do mecanismo, que é verificação da identidade por aproximação de padrões.

Então, por exemplo, o fabricante do equipamento usado hoje na urna eletrônica que identifica a biometria das impressões digitais afirma que a identificação biométrica com o equipamento utilizado dá em torno de 1% de falso negativo, ou seja, o caso em que o eleitor está cadastrado, mas a sua identidade biométrica não é reconhecida. Como o direito de votar não deve depender da tecnologia e sim da democracia, tem de haver um mecanismo de contingência para permitir o eleitor votar nesses casos de falso negativo. Com seções eleitorais com 300 eleitores em média, dá em torno de 3%, segundo o fabricante, de eleitores que precisam ser liberados para votação através do sistema antigo de senha.

Então, a biometria não acrescenta nada na segurança da identificação do eleitor por causa da necessidade do mecanismo de contingência para liberar aqueles casos de falso negativo. E o eleitor que quer fiscalizar se está havendo fraude de cadastro, se algum eleitor está votando por outro, não tem como saber se uma alegação de falso negativo de quem bota o dedo lá mas não está cadastrado – ele diz que está mas não está – se o mesário estiver favorável à fraude, vai levar a palavra do pretenso eleitor ao pé da letra e libera a urna para votar com a senha, como era antigamente, antes da biometria.

Então, na primeira eleição em que foram divulgadas estatísticas do uso da biometria, em vez de 1% de falso negativo, houve 7% de uso da senha para liberar a votação – sete vezes acima do que foi previsto pelo vendedor da identificação biométrica.

Também com a negação dos juízes eleitorais em alguns casos e dos mesários em outros de fornecer boletim de urna impresso, os partidos estão sendo cerceados no direito de fiscalizar a totalização a partir de uma resolução do TSE de 2006 que restringe a impressão de votos aos primeiros que chegarem, um tal de comitê interpartidário. Isso, depois, foi corrigido, mas ainda existem iniciativas de tribunais regionais e de juízes eleitorais de zonas específicas que negam o direito de um partido que queira uma versão impressa do boletim de urna no momento em que encerra a votação receber isso do mesário assinado pelo mesário.

Então, os países que acham que essa não é uma situação adequada para democracia partiram para o sistema de segunda geração em que os problemas passam a ser aqueles que eu já citei. Há uma interrupção aqui na capacidade do eleitor. Essa linha de baixo aqui...

(*Soa a campainha*.)

**O SR. PEDRO ANTÔNIO DOURADO DE REZENDE** – Isso foi para mim?

(*Intervenção fora do microfone*.)

**O SR. PEDRO ANTÔNIO DOURADO DE REZENDE** – Essa linha de baixo aqui é a linha da fiscalização. E a linha de cima é a custódia do voto, o.k?

No sistema de segunda geração, há uma interrupção aqui dentro da urna, porque o registro material do voto, que permite a recontagem nesse processo aqui, não há como a contagem manual do voto impresso indicar onde estaria a discrepância, se na votação eletrônica ou se na própria manipulação no registro do voto.

Com o sistema de terceira geração, os registros de voto, tanto o eletrônico, como o registro material, são entrelaçados para que, quando surja uma discrepância, o mecanismo aponte onde houve o desvio ou onde houve a manipulação indevida, se na contagem eletrônica ou na contagem manual.

Existem, que eu saiba, apenas dois sistemas de terceira geração em uso hoje. Um sistema altamente complexo que emprega várias camadas de criptografia usado nos Estados Unidos, produzido por um grupo de especialistas criptógrafos de primeira linha, que se debruçaram sobre o problema, chamado Scantegrity e um modelo introduzido em 2006 pela primeira vez na Argentina, feito por um engenheiro que estudou uma publicação produzida pela Fundação Alberto Pasqualini, do PDT, a partir de um seminário organizado na Câmara.

Lá em 2002, colhemos todas as denúncias de suspeitas de fraude que havia no sistema de votação eletrônica. Esse engenheiro da Argentina passou três anos estudando essa publicação que não ganhou o papel, foi apenas para a internet, porque disseram ao Brizola, na época, que seria bom ele não publicar aquilo, porque o Partido dele poderia sofrer retaliação. E botamos na internet. Dez anos depois descobrimos que o engenheiro argentino estudou todas aquelas denúncias e procurou fazer um sistema de votação usando um *chip* de RFD embutido na cédula que recebe a impressão do voto – isso aqui. Se vocês olharem tem uma RFD dentro da cédula, que permite a contagem automática do voto eletrônico e o registro material na mesma cédula. Quem quiser dar uma olhada nisso aqui, depois faremos circular.

Então, esses são os sistemas de terceira geração.

Enquanto isso, a gente tem de entender o que está acontecendo na discussão no Brasil, porque 96% da população confiam no sistema de votação que temos, mas 15% não confiam nos políticos que esse sistema elege. Fica perdido aí um elo de ligação entre os dois números, que é o fato de que o sistema de votação que temos é regido por leis cujos políticos eleitos por esse sistema aprovam.

Então, a minha hipótese de como se dá esse discussão, sobre se evolui ou não o sistema de votação, se o que temos é adequado ou não, ele segue uma lógica de como o processo de modernização eleitoral se insere no processo político da democracia em questão. Eu vejo três caminhos para a informatização do voto: um, em que a tecnologia eleitoral é manipulada como fim em si mesmo; um, em que a tecnologia eleitoral é um meio para um fim – controlar o risco de fraude, por exemplo; e um, em que a tecnologia eleitoral se torna cavalo de batalha para disputa de espaço de poder entre os três braços ou os três poderes do regime republicano.

E acredito, pela discussão de como evoluíram as leis no Brasil, que pretendiam avançar o nosso sistema de votação para a segunda geração, mas não conseguimos chegar à terceira porque sequer conseguimos passar para a segunda as leis que são aprovadas para nos colocar como sistema de segunda geração são revogadas por uma legislação seguinte, e isso vem-se alternando desde 1965, a última com essa ação direta de inconstitucionalidade que o Senador Zeze Perrella leu aqui na introdução da nossa apresentação.

Então, esse é o histórico de como foram modificadas as leis do nosso processo eleitoral, para ficarmos voltando para um sistema de primeira geração.

Aqui, alguma literatura sobre o que eu afirmei a respeito da evolução do processo de votação em outros...

Como eu disse, a partir de 2005, já havia uma recomendação para se partir para os sistemas de segunda geração nos Estados Unidos.

E, na França, o outro berço da democracia, os Municípios têm o direito de escolher o regime de votação que vão adotar. E apenas 3% dos Municípios na França adotam votação eletrônica. Os outros 97% preferem usar registro material do voto apenas. Mesmo assim, ficamos sabendo o resultado da eleição presidencial da França no mesmo dia. Por quê? Porque, na França, a votação é voluntária – não é obrigatória, como no Brasil ; a apuração da seção eleitoral é feita na própria seção eleitoral; vai um boletim de urna eletrônico para apuração instantânea e vai um registro material do boletim de urna para lastrear a votação eletrônica e para, em caso de votação apertada, poder haver mecanismo de recontagem em nível de totalização. Com isso, eles conseguem fazer uma apuração tão rápida quanto a nossa, mas lá o eleitor é civilizado, está preocupado com o processo e quer fiscalizar a votação no local em que o voto é registrado, na seção eleitoral.

No Brasil, nós somos adestrados a entender processo de votação como *videogame*: quem manda é quem faz a máquina e quem faz as pesquisas. O eleitor é passivo, fica vendo as pesquisas na televisão, como se aquilo fosse uma corrida de Fórmula 1. A única ação a que ele tem direito é, no dia eleição, chegar até uma máquina, apertar um botão e voltar para a tela para ver o resultado aparecer na televisão. Ele não tem mais interesse em fiscalizar, até porque alguém botou na cabeça dele que não vale a pena, porque os políticos não merecem a confiança dele. Mas é a democracia que adoece dessa forma.

Bem, a propaganda vem desde 97. Começou comparando o computador com algo que torna o céu o próprio céu e não o inferno, e, agora, temos aquela foto ali da segurança por obscurantismo como parte de um vídeo de propaganda institucional de que o sistema – o mesmo modelo desde 97 – é o melhor que podemos ter.

Mas talvez isso não seja uma situação adequada. Por quê? Porque isso concentra muito o poder no operador eleitoral. Vivemos uma espécie de ressaca da República Velha. Lá, o processo de votação, o processo eleitoral, era concentrado no poder de executá-lo, de regulá-lo, e de julgar o resultado no Poder Legislativo.

Com a Revolução de 30, houve um movimento pendular. Retirou-se todo esse poder do Legislativo e colocou-se no Judiciário. Mas isso continua sendo um problema, porque o Brasil é o único País do mundo, onde o órgão que julga o resultado do processo eleitoral é o mesmo que executa. Como alguém vai produzir prova contra si mesmo num processo de impugnação de votação? Como ele vai fornecer provas que ele detém para o autor da ação, para que ele possa enquadrá-lo num caso de inépcia ou de má-fé? Não vejo lógica nisso.

Então, o que nós temos? Notícias de que há violação da lei em vigor, que rege o cadastro eleitoral, começando a surgir finalmente no Estado de São Paulo – cadastro eleitoral sendo vendido. Mas essa notícia aqui é mais curiosa pelo seguinte: não estou falando do caso do Serasa, mas de outro, em que os dados vendidos, fornecidos pelo TSE, para o Sindicato das Funerárias, são os títulos de eleitor de gente que morreu. Essa troca de cadastro entre entidades que não são eleitorais com a Justiça Eleitoral está prevista na lei, mas apenas numa direção, porque o TSE pode usar de outras instituições.

Aqui é o contrário. Imaginamos que a funerária poderia estar fornecendo dados de quem morreu naquele ano, o Sindicato das Funerárias, para o TSE tirar do cadastro, mas a colaboração está em outro sentido. Por que alguém vai pagar R$27,00 para ter o número de eleitor de um defunto? Quem é candidato em eleição é capaz de juntar os dois pontos e entender para o que serve isso.

Então, por que a Justiça Eleitoral está violando a lei, dizendo que o cadastro eleitoral é de uso exclusivo? Ela está contando com o fato de este projeto de lei ser aprovado, regularizando assim essa situação. Mas essa situação interessa à sociedade brasileira, à democracia brasileira? Acredito que não, porque este não é o menor dos problemas: a venda de número de título de eleitor de defunto.

Aqui, está o aditivo de um contrato, um acordo de colaboração técnica entre o TSE e a Polícia Federal. Esta é encarregada de investigar casos de denúncia de fraude eleitoral. Ela vai ter boa vontade, se ela pode ter um cadastro de dados biométricos colhidos para controle de acessos ao sistema de votação, quando ela só tem o direito de coletar dados de investigados para fazer perícia forense?

O problema do uso da biometria é que ele tem duas utilidades totalmente distintas diante do ordenamento jurídico num Estado de direito. Uma é o uso para controle de acesso, como se tem atualmente no processo de votação brasileiro: a pessoa, primeiro, fornece os dados biométricos seus para se cadastrar e, logo em seguida, num momento conhecido do eleitor, ele apresenta, de novo, seus dados biométricos para serem identificados numa situação controlada, em que ele está ciente, concordando com a sua identificação.

No caso em que a biometria vinha sendo usada antes de a tecnologia favorecer o uso da biometria para o controle de acesso, que é o uso forense, o material é colhido – por exemplo, no registro civil – e, depois, na identificação, ele é colhido em situações fora de controle de quem vai colher e de quem vai ser identificado – por exemplo, impressão digital deixada numa porta no caso de um arrombamento.

Então, para uso forense, valem os direitos de defensa. Com esse compartilhamento de dados de controle de acesso para uso forense, é atropelado o princípio constitucional de que um acusado não pode ser obrigado a produzir prova contra si mesmo.

Então, este artigo aqui do *Wired* tem a crítica de uma colunista que explica: olha, esse negócio de compartilhamento de dados que o Governo colhe, por uma obrigação civil, para controlar acesso, por exemplo, à urna, com órgão do Estado encarregado de fazer investigação criminal, atropela o princípio constitucional da não autoincriminação. Mas isso está sendo feito hoje com esse contrato pela Justiça Eleitoral, ao arrepio da lei, que deveria regular o uso do cadastro eleitoral.

Por isso, sou contra o projeto de lei que está sendo examinado nesta Comissão, por conta dessas distorções que ela emprega e introduz no ordenamento, no equilíbrio, dos poderes republicanos. A tecnologia permite isso. Por isso, legislar sobre tecnologia é tão perigoso.

Então, líderes de dois Poderes da República – um do Judiciário, outro do Executivo – estão atropelando um direito que o Poder Legislativo constitucional deveria proteger no ordenamento jurídico. Como um todo, que está virando de ponta cabeça com essa concentração de poderes no processo eleitoral, como é que pode uma resolução de um órgão estatal atropelar uma lei ordinária aprovada nesta Casa pelo Legislativo e sancionada pelo Executivo, que diz que o uso do cadastro eleitoral deve ser de uso exclusivo da Justiça Eleitoral?

Então, estamos nessa situação. E o perigo vai além. Por quê? Porque o interesse nesses dados biométricos é maior por parceiros da Polícia Federal, que é controlada pelo Ministério da Justiça. Estamos diante de uma situação que ninguém mais pode esconder de que há um plano, um projeto, para instalação de um governo totalitário global a partir do controle de fato, através da tecnologia, de tudo que diz respeito à comunicação, meio de prova eletrônica para o Judiciário, a partir do controle da tecnologia por uma potência hegemônica.

A matéria que diz que o FBI tem interesse em construir agressivamente uma base de dados global com dados biométricos está aí. Existe parceria da Polícia Federal com o FBI para compartilhamento de dados. Então, temos de examinar essa lei ora em discussão neste Plenário com muito cuidado, porque há muita coisa por baixo desse dispositivo que o projeto de lei contém, que dá autoridade ao TSE de decidir para quem ele entrega o cadastro de biometria.

O valor do cadastro biométrico do TSE, do ponto de vista estratégico e militar, é altíssimo. Por quê? Porque a votação, no Brasil, é obrigatória. Todo cidadão maior de 18 anos é obrigado a fornecer os dados biométricos. O cidadão não tem o direito de se recusar, sem afrontar a legislação, a entregar dados biométricos à Justiça Eleitoral se essa lei passar.

Há outro projeto de lei, que está correndo na Câmara dos Deputados, que vai chegar provavelmente a esta Comissão – já me disponho a discuti-lo –, que regulamenta o uso de biometria dentro do Governo brasileiro, onde não se distingue o uso de controle de acesso e forense, que deve ser trazido à tona numa legislação que procura regulamentar o uso da biometria, por essas questões que já levantei na minha apresentação.

Muito obrigado. Peço desculpas por ter estendido o meu tempo.

Aqui, apenas para completar, o abuso em relação à legislação não é só um compartilhamento de dados biométricos. Há aqui uma notícia do jornal de Goiânia desta semana de que funcionários da Justiça Eleitoral estão usando os poderes que eles têm de manipular esse cadastro para plantar provas falsas contra autoridades com quem eles tenham alguma desavença.

Não sei como isso vai ser investigado: se pela Polícia Federal, que está recebendo de graça um banco de dados biométricos de todo cidadão brasileiro, não vai ter muito estímulo para investigar quem está nessa parceria com eles. Existe, para mim, aí claramente um conflito de interesse nesse convênio, nesse contrato do TSE com a Polícia Federal.

O exemplo está aqui nesta notícia-crime do jornal *O Popular* desta semana.

Muito obrigado a todos.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Muito bem, professor.

Vamos ouvir, agora, então, o Sr. Amilcar Brunazo Filho, moderador do Fórum do Voto Secreto na internet.

Com a palavra o Sr. Amilcar.

**O SR. AMILCAR BRUNAZO FILHO** – Bom dia, Senadores e Senadoras. Eu quero agradecer o convite, para a minha presença, neste debate sobre o Projeto de Lei nº 68, ao Senador João Capiberibe. Agradeço também ao Presidente Zeze Perrella por esta oportunidade de me manifestar mais uma vez a respeito desta questão do voto impresso ou do voto não impresso, e, agora, neste projeto de lei, com a introdução da biometria também no processo eleitoral.

Então, vou fazer uma análise estrutural do Projeto de Lei do Senado nº 68, para ver o que ele pretende fazer e o que ele está fazendo certo e o que ele está fazendo errado.

O Projeto de Lei nº 68, de 2010, basicamente, primeiro revoga o art. 5º e o art. 6º da Lei nº 12.034, de 2009. Nesta lei, os arts. 5º e 6º preveem o princípio da independência do software no processo eleitoral. O princípio da independência do software é aquele conceito que o professor tocou, no sentido de que migra uma urna eletrônica da primeira geração modelo da DRE para a segunda geração VVPAT. Ou seja, ele dá transparência para o eleitor poder conferir para quem foi gravado o seu voto e para o fiscal poder conferir a soma dos votos.

Então, o art. 5º da lei tem sido chamado Lei da Transparência Eleitoral, porque ele adota o princípio da independência do software. Ou seja, a máquina de votar tem de ter o seu resultado conferível, de uma maneira que não dependa de confiar no software. O princípio da independência do software formalmente significa o seguinte: se houver um erro não detectado no software do equipamento eleitoral, esse erro não pode provocar um erro no resultado, que não possa ser detectado. Então, deve existir uma maneira de conferir o registro e a apuração eletrônica dos votos que não dependa de confiar apenas no software. Esse é o princípio da independência do software, que foi adotado, então, pelo art. 5º. Ele também prevê a transparência do registro digital do voto.

Hoje, o eleitor brasileiro, quando vota na urna brasileira, ele vê o voto na tela, que ele seleciona; vê o voto, vê a foto do candidato e confirma. Depois que ele confirma, esse voto é gravado no registro digital do voto. Registro digital do voto é o conceito criado pela lei, que já foi citada aqui, de autoria do Senador Azeredo. A lei de 2003 foi que criou o registro digital do voto. Então, o voto é gravado nesse Registro Digital do Voto. É um arquivo dentro da urna; ficam gravados lá os votos, a coleção de votos.

Só que, na urna brasileira, o eleitor vê o voto na tela e confirma; depois que ele confirma, esse voto é gravado. O que foi gravado como sendo voto dele, do eleitor, o eleitor não pode ver; ele não pode conferir se foi gravado o voto dele. Essa é a falta de transparência do modelo atual, da urna eletrônica, do modelo da DRE, que foi declarado inconstitucional na Alemanha; inconstitucional, porque não permite ao eleitor conferir o destino. É o eleitor comum. Veja, o Tribunal Constitucional Alemão declarou que urnas eletrônicas que não permitiam ao eleitor comum acompanhar o registro e a contagem do seu voto são inconstitucionais por não atenderem ao princípio da publicidade do processo eleitoral.

Então, a transparência do registro digital do voto, de maneira que o eleitor possa ver o registro do seu voto, se aquele mesmo é o seu voto, e o fiscal do candidato possa conferir se o resultado, o chamado boletim de urna, é a soma dos Registros Digitais do Voto, de fato. É isso que trazia o art. 5º da Lei nº 12.034. Isso tudo era conseguido através do voto impresso, conferível pelo eleitor e pela auditoria contábil automática do voto impresso.

Há uma coisa importante a falar. Muita gente entende errado quando se fala em voto impresso na urna eletrônica, pois pensa que é um comprovante do voto que o eleitor vai receber para levar para casa. Não, isso não é possível. Se o eleitor levar um comprovante, um recibo do voto para fora, ele passa a ser sujeito à coação. Quer dizer, alguém pode exigir que ele mostre esse voto para saber se votou em quem devia, não sei o que e volta-se a uma fraude muito antiga e conhecida, que é a coação de eleitores ou o voto de cabresto.

Então, o voto impresso não significa entregar o voto para o eleitor. A ideia, no caso do art. 5º da lei, prevê que o eleitor veja o voto impresso, confirme ou cancele, conforme esteja ele de acordo com o voto impresso, e depois que ele confirmou, o voto é cortado e guardado dentro de uma sacola. O eleitor nem pega o voto na mão para levar para fora.

Esse é o conceito de voto impresso. E, depois da eleição, há a auditoria contábil automática por estatística, em que 2% das urnas são selecionados para se fazer a recontagem do voto impresso e verificar se a soma do voto impresso é igual à soma do voto eletrônico. Essa, então, é uma auditoria estatística, para ver se o voto eletrônico somou corretamente aquilo que o eleitor viu no registro impresso do voto. Hoje, a urna registra o voto, dá o resultado, e a gente não sabe se aquele resultado é a soma do que o eleitor viu. A ideia do voto impresso serve para isto: para permitir que os partidos possam conferir depois se o resultado do boletim de urna é a soma dos votos.

O art. 5º também prevê a identificação biométrica do eleitor, mas com uma ressalva muito importante, a de que o equipamento de identificação esteja separado fisicamente do equipamento de votação. Então, você se identifica numa máquina biometricamente, põe o seu dedo ou a sua foto, seja lá o que for, e recebe um passe ou algo para ir à maquina de votar. A máquina de votar não pode ter conexão com a máquina de identificar, para que o *software* que tem algum erro, algum vício ou alguma fraude possa registrar os dois dados simultaneamente: o voto e o conteúdo, o autor do voto e o conteúdo do voto.

Então, o art. 5º previa a identificação biométrica, mas com esta ressalva: a de que o equipamento de votação tem de ser separado do equipamento de identificação, como é feito, por exemplo, na Venezuela. Na Venezuela, usa-se a identificação biométrica do eleitor. Mas o que faz o eleitor? Ele chega a uma seção onde estão as máquinas de identificação biométrica, ele se apresenta e mostra que ainda não votou. Eles verificam que o cara não votou em nenhum outro lugar e que é ali que ele vai votar e dão para ele um cartão. Ele vai até outra sala onde há uma máquina de votar, escolhe a máquina de votar, põe ali o cartão, para liberá-la, para registrar o voto. Então, a máquina em que ele vota é uma, e a máquina em que ele é identificado é outra. Isso não é o que ocorre no Brasil.

Outra coisa que o art. 6º prevê nessa lei é o voto em trânsito para presidente. O PLS nº 68 revoga o art. 5º e o art. 6º e modifica os arts. 59 e 66 da Lei nº 9.504, que, atualmente, está em vigor, criando algumas condições. Primeiro, cria algumas condições para a auditoria do *software*, mas estas são inócuas, no meu entender. Depois, eu me estendo um pouco mais para explicar por que são inócuas.

Hoje, o TSE, seis meses antes da eleição, tem de abrir as portas de uma sala para os partidos, o Ministério Público e a OAB poderem acompanhar o desenvolvimento do *software* que o TSE está desenvolvendo para as urnas eletrônicas. E, 20 dias antes da eleição, esse *software*, então, é preparado, é compilado, como a gente diz, para, depois, ser levado para as urnas eletrônicas. O que esse Projeto de Lei faz é modificar: o TSE, em vez de ter de desenvolver o *software* nesses seis meses, tem de apresentar o *software* pronto em março do ano eleitoral, mas só vai compilá-lo 20 dias antes da eleição. Isso significaria que os partidos teriam mais ou menos cinco meses e meio para estudar o *software*, para ver se ele está correto ou não.

O problema é que, pela nossa experiência – eu acompanho o desenvolvimento do *software* no TSE desde o ano 2000; em toda a eleição, estou lá acompanhando o desenvolvimento do *software* –, vemos que não é possível, na prática, os partidos fazerem essa análise do *software*, porque, se dá um erro no programa, eles vão modificá-lo. Vamos dizer que eles apresentam o programa em março. Pronto! A gente vai lá, olha e descobre um erro, ou eles descobrem um erro, porque eles estão testando. Eles vão modificar o programa, eles não vão pôr o programa errado no dia da eleição. Então, esse negócio de dizer que o programa tem de estar pronto seis meses antes não quer dizer nada, pois, se houver erro, eles vão modificar o programa.

Já vi muitos casos... Tenho um documento aqui que posso apresentar no final da minha exposição. Em 2010, o TSE contratou um órgão do Ministério da Ciência e Tecnologia para fazer um estudo sobre as urnas eletrônicas, e eles encontraram um monte de falhas de segurança e propuseram um monte de modificações no *software*. Então, no mês de agosto, nós solicitamos ao TSE as modificações que foram feitas no *software* em função das sugestões do órgão do Ministério da Ciência e Tecnologia. A eleição ocorreu em outubro, a resposta não foi dada, não nos foram mostradas essas modificações. E, em novembro, depois de acabadas as eleições, o TSE respondeu. Tenho o ofício aqui para mostrar para os senhores. Eles disseram o seguinte: “As modificações que foram feitas são sigilosas. Vocês não têm direito a saber. É essa questão de segurança do sistema eleitoral.”

Enfim, então, a Justiça Eleitoral diz que o *software* está aberto, mas modifica o *software* no dia da eleição. Isso já aconteceu em 2008, isso já aconteceu em 2002, quando nós descobrimos que o *software* que estava sendo compilado – ou seja, estava sendo preparada a versão final – 20 dias antes da eleição era diferente daquilo que estava nos computadores à disposição para nossa análise. Nós encontramos um erro, em 2008, um erro de programação que gerou uma dúvida. Nós os consultamos: mas escute, isso aqui não vai dar o problema? Eles vieram com a resposta para a gente: “Não, mas isso aí é só pra vocês olharem. O que está sendo compilado é outro *software*”. Então, é a dificuldade de a gente, como fiscal de partido, acompanhar o desenvolvimento do *software*. É impossível. Mudar, falar que tem que estar pronto seis meses antes, não vai mudar nada, porque eles vão mudar no meio do caminho, e a gente vai ficar sem saber.

Essas modificações criadas pelo PLS nº 68 também voltam para o obscurantismo do Registro Digital do Voto. Ou seja, ele propõe que o eleitor vai ver o voto, vai conferir o voto eletrônico, na tela, vai confirmar, o voto vai ser gravado e o eleitor não pode conferir o que foi gravado. Ele volta a impor essa condição. Ele impõe também, no art. 9º... Eu o tenho aqui, eu posso até ler, se for o caso. O art. 66, §9º:

*§9º Cada partido político deverá utilizar um percentual do Fundo Partidário para a auditoria e fiscalização de que trata o caput, especialmente do que trata o §2º, na forma e nos limites fixados pelo Tribunal Superior Eleitoral.*

Isso aí são aqueles seis meses para a gente poder analisar o *software*. Ele está dizendo que os partidos têm que pagar, usar uma parte da verba do Fundo Partidário, para fazer a fiscalização do *software*. Isso é um processo caríssimo. O partido tem que contratar técnicos especializados em informática, deixá-los seis meses hospedados aqui em Brasília, acompanhando, estudando. Muitos *softwares*,são 17 milhões de linhas de código. Não é uma pessoa que sentadinha lá, uma semana, vai estudar isso aí. E o que acontece na prática é que nem os partidos políticos, nem o Ministério Público, nem a OAB, que têm direito a fazer essa fiscalização, fazem, porque o custo é alto. A OAB já desistiu. Em 2010 e 2012 ela não assinou o *software* porque concluiu que não dá para garantir que o *software* está livre de falhas, porque é muito caro tentar descobrir isso. Os Senadores aqui têm experiência própria, provavelmente sabem que os próprios partidos não fazem essa avaliação do *software*, não gastam dinheiro para ir lá verificar se o *software* está correto ou não.

Há algumas cláusulas que foram introduzidas nesse projeto de lei que eu acho muito perigosas. São aquelas cláusulas que entram de contrabando, que não têm nada a ver com o voto impresso, e às quais tem que ser dada atenção. Ela dá uma autorização para o TSE contratar terceiros para fazer melhorias no processo. Isso o TSE já faz normalmente. Como eu falei, ele contratou uma empresa do Ministério da Ciência e Tecnologia; ele contratou, recentemente, um professor da UnB, para tentar ajudar no problema daquele falso negativo, que está dando nas urnas eletrônicas. Enfim, ele já contrata. Já contratou a Unicamp em 2002. Ele contrata, normalmente, as entidades envolvidas com ciência e tecnologia, informática, para fazer e dar conselhos. Mas, por algum motivo, o Senador Azeredo – na época, era Senador – incluiu isso dando essa autorização para o TSE fazer essas contratações que o TSE já faz. Eu não sei por que precisa pôr nesse projeto de lei.

Quanto à identificação biométrica, o Prof. Pedro já falou. Esse projeto de lei dá autorização para o TSE usar a identificação biométrica do eleitor para que ele possa votar. O problema é que ele dá essa autorização para usar biometria, mas não impõe a condição que ele revogou lá em cima, que o equipamento de identificação tem que ser separado do equipamento de votação. Ele não impõe essa condição. Então, na verdade, ele está revogando essa cláusula que diz que se vota em um equipamento e se identifica em outro, para que não haja risco de um *software* identificar automaticamente o voto.

Ele dá ao TSE todo o poder total normativo sobre o uso da biometria. O TSE vai dizer o que usa, quando usa, como compra, que tamanho de biometria, que formato, quando vai coletar os dados. Ele dá toda a condição normativa ao TSE, ou seja, entrega do Legislativo para o TSE a regulamentação do processo de uso da biometria, e inclusive dá ao TSE o poder de compartilhar esses dados. É gozado, porque ele diz – vou ver se eu acho aqui para ler – que o dado é para uso exclusivo do TSE, mas que o TSE pode compartilhar apenas os seguintes dados... E lista todos os dados que o TSE tem para compartilhar. Vou ver se eu acho aqui. (*Pausa.*)

*Art. 4º Os dados constantes do cadastro eleitoral serão administrados e utilizados, com exclusividade, pela Justiça Eleitoral, incumbindo ao Tribunal Superior Eleitoral regulamentar as hipóteses e a forma de acesso a esses dados* [ou seja, é de uso exclusivo, mas ele pode regulamentar esses dados.].

*Parágrafo único. As hipóteses de acesso constantes no caput somente poderão ser relativas aos dados de nome, filiação, data de nascimento, sexo, dados biométricos, fotografia e número da inscrição eleitoral* [ou seja, tudo o que o TSE colhe.].

Diz, então, que o TSE pode regulamentar a cessão desses direitos. Isso dá naquilo que aconteceu: o TSE forneceu os dados para o Serasa. Ele tem um contrato, um acordo, que não foi citado aqui, com a Caixa Econômica, em que esta forneceu equipamento para o TSE e este fornece cadastro biométrico para a Caixa. Agora, por que a Caixa quer o dado biométrico que o TSE colhe de todos os eleitores brasileiros? Imagine o interesse que tem para um banco – no caso, a Caixa é uma estatal – ter um cadastro com nome, filiação, data de nascimento, sexo, dados biométricos, fotografia e número de inscrição eleitoral de todos os eleitores! E O TSE tem esse acordo com a Caixa. Ele já forneceu os dados. Por quê? Por que ele está fazendo isso? Agora, este projeto de lei está autorizando o TSE a fazer isto: a coletar os dados biométricos, regulamentar o uso deles e distribuir para quem ele quiser.

O Prof. Pedro disse muito corretamente que dados biométricos têm duas finalidades. A primeira, para o controle de acesso. Nesse caso, é preciso apenas do que chamamos de impressão digital batida: você põe o dedo e colhe uma impressão da parte frontal do dedo. Na segunda etapa, o eleitor vai pôr o dedo e a máquina vai identificar que é o mesmo. Já para uso forense, é preciso a impressão corrida. O eleitor tem que pôr o dedo, para montar o cadastro, de lado, virando o dedo até o outro lado, porque, a Polícia, quando achar o fragmento de uma impressão digital numa arma, vai pegar aquele cantinho com aquele pedaço da impressão digital e vai tentar descobrir qual é a pessoa. É um uso completamente diferente para identificação de controle de acesso e para o uso forense.

Esse projeto não está fazendo nenhuma diferença: se está dando ao TSE o poder de coletar todos os dados de uso forense, ou seja, de ponta a ponta, e dados que o TSE não usa. Isso é muito importante.

O TSE colhe, hoje, a impressão digital dos dez dedos do eleitor, impressão corrida, ou seja, completa, de lado a lado, e usa na urna eletrônica quando o eleitor vai votar, Senador Zeze, somente os dados biométricos de dois dedos. Quando ele vai votar na urna com biometria, ele põe um dedo; se a máquina o identificar, ele é autorizado a votar; se, por um motivo, ela não identificar o eleitor, ele põe o outro dedo indicador; se identificar, ele vota; se não identificar, o mesário digita uma senha e o eleitor vota.

O TSE só usa a impressão digital de dois dedos, por que ele pega dos dez dedos? Porque ele captura a impressão das dez? Eu cadastrei recentemente no banco a minha impressão digital para poder usar na liberação do caixa eletrônica e eles capturaram a impressão de quatro dedos. Para identificação de controle de acesso não é necessário mais do que isso.

Agora, o TSE está capturando dados completos, fotografia de alta resolução. Você sabe que quem se cadastra por esse cadastro biométrico que o TSE está fazendo no Brasil inteiro, o eleitor se apresenta, eles batem uma foto de alta resolução, daquelas que o computador reconhece a presença na hora que a pessoa entra no aeroporto e já sabe que aquele é o fulano de tal. O TSE captura essa foto das pessoas e não usa. O TSE recadastra a pessoa, captura as impressões digitais e entrega o título de eleitor que não tem foto. O TSE, como vocês sabem, recentemente, a partir de 2010, passou a não aceitar o título de eleitor como documento de identidade na hora da votação. A pessoa é obrigada a levar a carteira de identidade ou outro documento que tenha foto. Ou seja, o TSE captura a foto de alta qualidade, de alta resolução, e entrega um documento que nem ele reconhece como válido, porque não tem a foto do eleitor gravada.

Então, por que ele está capturando esses dados? Está claro que esse acordo que o Prof. Pedro mostrou e que ele está cedendo esses dados para a Polícia Federal, que, por sua vez, cede para o FBI. O TSE está usando o poder dele de coagir o eleitor a ter de se cadastrar para poder votar, cumprir o direito de votar, e por acordo, acordo, acordo, vão parar no FBI esses dados. O TSE mesmo não usa esses dados. Então, estes arts. 4º e 5º dessa lei estão prevendo dar todo esse poder para o TSE de capturar o que quiser, fazer o que quiser com esses dados, dar para quem quiser.

Acho que isso aqui tem ser proibido. Devia haver uma lei ou um projeto de lei, nós até já apresentamos uma proposta de projeto de lei – sugiro que o Senador Capiberibe pense no assunto – para regulamentar essa questão de como se colhem dados biométricos e como se usam, quem tem direito a colher, quem tem direito a usar, quem tem direito a compartilhar. Bom, isso daí é basicamente o que faz o projeto de lei em questão.

Eu vou falar aqui de alguns argumentos que há no voto desse projeto de lei. Eles explicam algumas coisas, por que ele sugere isso ou aquilo.

Primeiro, algo que, talvez, não seja tão relevante nessa discussão aqui, mas que para mim é muito importante, porque acompanho esse processo desde 2000. A primeira Lei do Voto Impresso foi aprovada em 2002 e foi revogada em 2003, por um projeto do Senador Azeredo. Na época, o Senador Azeredo dizia que o projeto de lei era dele. Nesse projeto de lei agora que ele está apresentando para revogar a nova Lei do Voto Impresso de 2009 – está querendo regular novamente –, ele confessa que a Justiça Eleitoral houve por bem propor a revogação da Lei do Voto Impresso, contida na lei tal, de 2002. Ou seja, ele está confessando aqui que não era dele. A lei era do TSE. O TSE deu para ele o projeto de lei que ele apresentou e que revogou a Lei do Voto Impresso em 2003.

Naquela época, a lei que revogou o voto impresso, de 2003, foi feita de maneira tão atropelada, tão rápida. Eu e o Prof. Pedro Rezende estivemos aqui, procurando o Relator, que, na época, era o Senador Demóstenes Torres, na CCJ. Ele não aceitava que houvesse audiência pública e que apresentássemos sugestões. O negócio foi tão atropelado que a lei, ao final, quando o projeto de lei foi aprovado, ficou assim: o §7º do art. 59 e o art. 8º ficaram exatamente com a mesma redação. A redação do art. 8º da Lei nº 10.408, de 2002, já existia, a Lei do Voto Impresso. E a Lei nº 10.740, que revogou a Lei do Voto Impresso reescreveu o art. 8º no §7º. E, hoje, a nossa lei, que está valendo, que está em vigor, tem dois artigos com a mesma redação. O projeto de lei foi tão afobado que nem isso que tentamos alertar o Senador Demóstenes – olha, vocês estão fazendo uma lei que vai ter dois artigos iguais – pôde ser modificado. Ele falou: “Não. Recebemos do TSE a ordem de aprovar do jeito que está a lei.”

Então, para mim isso é muito importante. Talvez não tenha muito a ver com a lei atual – vamos discutir a situação de hoje –, mas para mim foi importante porque, na época, nós batalhamos para tentar corrigir esse erro.

Bom, uma contradição que há nos argumentos apresentados aqui, na justificação do PLS nº 68. Ele revoga o voto impresso, adotando uma série de procedimentos destinados a permitir que os votos possam ser conferidos e auditados. Ora, ele está fazendo justamente o contrário disso.

O Registro Digital do Voto não dá, puro e simples, como é feito hoje, como essa lei tenta pôr, para ser conferido pelo eleitor. O eleitor vê na tela, grava e o eleitor não vê o que é gravado. Depois, ele é somado, e o fiscal não vê o que foi somado, se o resultado da soma é a soma dos votos que o eleitor viu. Ele, justamente, tira o poder de auditoria que a Lei do Voto Impresso, art. 5º, que está em vigor hoje, dá, através do voto impresso. Ou seja, o eleitor vê o registro do voto e, depois, o fiscal vai pegar os registros impressos e conferir para ver se a soma está correta.

Então, com o registro digital, que esse projeto de lei tenta fazer, como o eleitor vai saber se o Registro Digital do Voto dele tem o voto dele? Não há como. É o contrário do que está escrito na argumentação do projeto de lei. E como o fiscal poderá conferir se o Registro Digital do Voto que lhe é mostrado, no final do dia – se houver uma auditoria, você pode imprimir esse Registro Digital do Voto –, como o fiscal vai saber que aquele Registro Digital do Voto impresso é o voto que o eleitor viu no dia da votação? Não há como.

Por isso, na Alemanha, esse sistema que registra a digital do voto sem o voto impresso foi declarado inconstitucional por não atender o princípio da publicidade, ou seja, por não permitir ao eleitor saber como foi gravado o seu voto. Então, é uma contradição, porque ele usa um argumento aqui e está propondo exatamente o contrário.

Eu queria só trazer aqui um detalhe. Sempre quando se fala do voto impresso, se fala que o voto impresso vai permitir a identificação do voto, vai poder quebrar o princípio de inviolabilidade do voto. Fazem uma confusão. Inclusive, isso chegou a criar uma Adin, como foi citado pelo Senador Zeze Perrella, que foi acatada provisoriamente, não é? Está engavetada desde então, e suspendeu a vigência do art. 5º da Lei do Voto Impresso.

Quanto a essa confusão do voto impresso, que o voto impresso quebra o sigilo do voto, é o seguinte: o princípio da inviolabilidade do voto é absoluto. Significa o seguinte: ninguém, nem mesmo o juiz eleitoral, pode violar o sigilo do voto, ou seja, um juiz pode quebrar o sigilo telefônico, o sigilo bancário. No caso de ele achar que tem interesse, ele manda quebrar. O sigilo do voto, nem um juiz eleitoral ou um Ministro do Supremo pode mandar quebrar o sigilo do voto, seja lá por que condição for. Então, o princípio do sigilo do voto é absoluto, e o princípio da publicidade – aquele que a Corte constitucional alemã disse que precisava atender, a máquina eletrônica, que a máquina eletrônica, lá, que foi usada não atendia ao princípio da publicidade – fala que o voto tem de ser aberto.

Parece que há um conflito nisso aí: como vai se atender ao princípio de abrir o voto e ao princípio de fechar o voto? Mas não tem conflito, não.

O que deve ser secreto é o autor do voto. A autoria do voto deve ser absolutamente secreta. De nenhuma maneira deve ser possível se identificar quem registrou aquele voto. Agora, o conteúdo do voto tem de ser absolutamente público. O eleitor tem direito a olhar se o voto que está registrado é o dele – isso dentro da seção eleitoral. Na seção eleitoral, o eleitor tem direito a saber se o registro do voto dele é o voto dele. Então, é público isso e, na hora da conferência, da auditoria, como já era no sistema manual, antigamente, o fiscal do partido tem direito de saber se a soma dos votos, se o resultado, o chamado boletim de urna, é a soma dos votos, de cada voto.

Então, o conteúdo do voto tem de ser absolutamente público, por isso tem de ser atendido o princípio da publicidade. O eleitor tem direito a ver o seu registro do voto na seção eleitoral e o fiscal tem direito a ver o registro do voto no momento da apuração ou da auditoria, tudo isso sem quebrar o sigilo do voto, que é saber quem é o autor de cada voto.

Isso tudo é perfeitamente possível. No resto do mundo, usam-se urnas eletrônicas de segunda e terceira geração que atendem a esses dois princípios: têm o voto impresso e não quebram o sigilo do voto.

O argumento de que o voto impresso quebra o sigilo do voto é absolutamente errado e tem contraprova material no mundo inteiro.

Esses são outros requisitos essenciais para o sistema eletrônico de votação.

Essa aqui é a norma norte-americana, isto aqui já é a versão de 2009. O Prof. Pedro citou que em 2006 começou a ter a regulamentação norte-americana sobre... Depois daqueles problemas que houve em 2000, na Flórida, os Estados Unidos já passaram pelas máquinas, evoluíram para máquinas DRE, em 2004, e, em 2006, eles passaram para as máquinas VVPAT, de segunda geração.

Hoje, a norma norte-americana impõe essas condições, quer dizer, para uma máquina poder ser usada nos Estados Unidos agora – não em 2000, mas agora – tem de atender a essas coisas. Ao menos dois registros dos votos devem ser produzidos e um deles deverá ser armazenado em meio que não possa ser modificado pelo sistema eletrônico de votação, ou seja, a máquina eletrônica de votação pode fazer o registro digital do voto, mas ela pode modificar esse registro que ela criou. Então, ela tem de registrar o voto no registro digital do voto, mas tem de criar, também, um registro do voto que ela mesma, máquina, não possa alterar depois que criou, por exemplo, o voto impresso, o voto gravado num CD-ROM que se gravou uma vez não pode regravar, enfim, de alguma forma, tem de ser gravado o voto que não possa ser modificado pelo próprio programa.

Antes de deixar o local de votação, o eleitor poderá conferir a equivalência entre os dois registros do voto. A máquina vai criar dois registros do voto e o eleitor vai poder ver se os dois têm o mesmo conteúdo.

Os processos de verificação do registro do voto devem ser independentes entre si e ao menos um deles deve ser conferível diretamente pelo eleitor, ou seja, a máquina vai criar dois registros, o eleitor vai poder conferir. Um deles pode ser a própria máquina que mostre, que fale: “Olha, o meu Registro Digital do Voto é este” e mostre na tela. Então, a máquina está mostrando para ele, ele não está vendo diretamente. O outro registro ele tem de ver diretamente: ou é impresso, é material, alguma coisa que ele veja sem precisar de uma máquina interferindo na leitura.

Por fim, deve haver correlação entre os registros do mesmo voto por meio de identificadores únicos, o que, aí, já dá na máquina de terceira geração, ou seja, os dois registros do voto têm de estar inter-relacionados, de maneira que, se houver uma falha, uma fraude no *software* ou no registro material do voto, a gente possa detectar onde ocorreu essa falha.

Essas são as condições impostas, já desde 2006, 2007, nos Estados Unidos – essa é a versão de 2009 –, e esse projeto de lei, o PLS 68, não atende nenhuma dessas quatro condições. Ele está revogando o art. 5º, que atende as três primeiras.

Bom, eu não vou, aqui, falar da primeira, segunda e terceira gerações – o professor já falou.

Esta aqui é a máquina de primeira geração brasileira; aqui, dois exemplos de máquinas de segunda geração: a de cima é a máquina mexicana. Vocês podem ver, lá em cima, ali...

(…) ali está o voto impresso. O eleitor votou nessa tela – não há teclado, ele vota na tela *touchscreen*. Completou o voto; o voto é impresso; o eleitor confirma; o voto corta e cai aqui. Isso aqui é uma urna comum. O voto cai e fica embaixo. A tela é um pouco fosca para, quando cair, ser embaralhado, e o eleitor não ver exatamente onde está o voto dele. Mas ele vê que o voto está lá. É a máquina usada no México.

A de baixo é a máquina usada na Venezuela. Está aqui o eleitor coletando seu voto impresso. Ele vota num teclado que fica ao lado; aparece na tela; ele confirma; ele imprime; ele pega esse voto impresso, vai até uma urna comum e coloca lá dentro.

O art. 5º da lei que está em vigor, que está suspensa pelo STF, não prevê essa situação. Prevê a situação de cima: que o eleitor não pega o voto na mão. Ele vê, confirma, e o voto cai na urna – ele não o pega na mão. Ou seja, o modelo similar ao modelo mexicano. É o que está previsto na lei que o Projeto de Lei nº 68 quer revogar.

Essa é a máquina de terceira geração, que o Prof. Pedro citou, usada na Argentina. Essa é a *Boleta de Voto Electrónico*. Como eu falei, há um *chip* dentro dela, que é um *chip* de radiofrequência, e há o voto impresso. O eleitor coloca uma cédula dessa virgem; ele imprime, grava, e o eleitor pode ir a qualquer máquina – que na seção eleitoral há várias. Ele vai lá e só de chegar com o voto perto de outra máquina, aparece na tela o que está impresso, e ele confere se o registro digital é igual ao registro impresso.

Eu acompanhei uma eleição na Argentina, no ano de 2011, com essa máquina. A apuração é feita pela contagem disso aqui, voto a voto, na frente dos fiscais. Ou seja, acaba a eleição, os mesários chamam os fiscais, pegam todos os votos, vão aproximando da máquina e vão fazendo a apuração. A contagem é feita na sessão eleitoral. A eleição acabou às 18h – a eleição lá acaba às 18h –, às 20h15, ou seja, 2 horas e 15 minutos depois, estava tudo colocado na internet, e encerrada a apuração. Ou seja, a apuração, voto a voto, na frente do fiscal, o fiscal vendo cada voto sendo contado. Todas as cidades grandes, 400 mil eleitores. Em 2 horas e 15 minutos, eles apresentaram o resultado. Ou seja, mais rápido que no Brasil e mais transparente que no Brasil.

Então, essa ideia de que o voto impresso vai resultar em aumento de custo absurdo, que vai atrasar a votação, que vai atrasar a apuração, é tudo conversa, porque, no resto do mundo, o voto impresso já vem sendo usado – na Argentina, no México, na Venezuela. O Peru está testando; a Bélgica já vai usar, ou usou em 2012; Estados Unidos usam o voto escaneado, não impresso, mas é equivalente em termos de segurança. E todos eles apresentam o resultado rapidamente. Não há nada dessa história de que vai demorar, de que vai atrasar, de que vai dar problema. Fazendo direito, faz direito, e funciona.

Bom, senhores, então era isso que eu tinha para apresentar. Agradeço a oportunidade.

Deixei alguns endereços aí. Quem sabe, talvez, quem esteja ouvindo esteja interessado na questão do voto eletrônico. Há *sites* na internet, no Facebook, há o relatório do Comitê Multidisciplinar Independente, que estudou a urna brasileira e a urna argentina, para quem quiser poder acompanhar e estudar. Já há bastante informação na internet sobre isso.

Agradeço, então, aos Senadores esta oportunidade.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Obrigado, Sr. Amilcar.

Passamos, então, agora a palavra para o Prof. Diego Aranha. Com a palavra.

**O SR. DIEGO ARANHA** – Obrigado. Bom dia. É sempre um prazer poder colaborar com essas questões de votação eletrônica, então agradeço o convite.

Eu vou me restringir mais a questão do voto impresso, porque foi a questão em que eu me envolvi diretamente. Eu sou professor da UnB e, como primeira tarefa, como professor da UnB, eu participei dos testes públicos de segurança do *software* de votação em março do ano passado. Eu coordenei a equipe que venceu os testes.

Então, de início, eu devo descrever brevemente como os testes foram organizados. À medida que eu for descrevendo, eu vou atingir as conclusões ou os resultados, do ponto de vista de segurança, que nós obtivemos no final daquele evento.

Então, esses testes foram organizados, convocados via Chamada Pública do TSE. Nove equipes participaram – eu coordenei a equipe da UnB – num total de 27 pessoas. E esses testes foram divididos em duas fases, separadas por 12 dias. Cada fase tinha apenas três dias.

Na primeira fase, as equipes tinham a possibilidade de observar o código fonte do *software* de votação e solicitar esclarecimentos técnicos do pessoal do TSE. É claro que essas solicitações também eram protocoladas e o TSE se reservava o direito de não respondê-las.

Apenas no segundo dia dessa fase inicial de teste e de exame do código fonte a nossa equipe teve acesso ao *software* de votação, ao código fonte que é produzido pelos programadores do TSE para, de fato, executar as eleições.

Uma coisa importante que eu deveria ter falado aqui. A fase de exame começou com uma palestra de abertura em que todos os mecanismos de segurança foram descritos superficialmente. Então, foi descrito um mecanismo de segurança que, por exemplo, produz o RDV, Registro Digital do Voto, de formado embaralhado. Os votos são armazenados no RDV fora de ordem, para que não seja possível correlacionar a ordem em que a eleitor votou, a posição dele na fila de votação, com seu voto propriamente dito.

Então, quando tivemos o primeiro acesso, no segundo dia de exame do código fonte, achamos que esse poderia ser um ponto promissor para iniciar a análise. Fizemos uma primeira relação. A gente tinha 17 milhões de linhas de código para analisar, algo completamente infactível em apenas três dias.

Começamos buscando funções conhecidamente inseguras, ou construções conhecidamente inseguras, exatamente para embaralhar coisas, para trocar as coisas de ordem, calcular permutações, como a gente chama em computação. Aí, curiosamente, nós encontramos, já nos cinco primeiros minutos, uma construção conhecidamente insegura – é sabidamente insegura há 17 anos –, exatamente no arquivo que produziu o RDV. Ou seja, nós conjecturamos, levantamentos uma hipótese, naquele momento, de que o RDV não havia sido projetado, implementado, de maneira segura ou de maneira a proteger o sigilo do voto.

No final da primeira hora, nós nos certificamos de que nada interferia, de fato, nesse processo de embaralhamento dos votos. Portanto, adotamos essa como a nossa primeira possibilidade de avaliação de segurança na fase a seguir, que era a fase de testes propriamente dita e não mais a fase de exames.

Tivemos um total de cinco horas para analisar o código fonte. Então, nas quatro horas restantes nós buscamos outras possibilidades, outras vulnerabilidades no código fonte do *software* de votação para, talvez, interferir em outros mecanismos de segurança da eleição, como, por exemplo, na questão da integridade do voto e não apenas no sigilo.

Tivemos um total de cinco horas de análise do código fonte em que, na primeira hora, já tivemos uma hipótese muito forte de que o sigilo do voto não era devidamente protegido pelo *software* de votação em uso, oficial, nas urnas eletrônicas. O que nos foi dito, no início do evento, é que seria o *software* utilizado nas eleições de 2012, ano passado.

Bem, terminada essa fase de exame, após 12 dias de intervalo, começou a fase de testes propriamente dita. No final da fase de exames nós produzimos dois planos de teste, como o TSE chamou, que eram simplesmente descrições das metodologias que nós gostaríamos de colocar em prática na fase, de fato, de testes. Uma ligada ao sigilo do voto, utilizando essa vulnerabilidade até infantil que nós encontramos no embaralhamento dos votos e outra relacionada à integridade dos resultados.

No primeiro dia da fase de testes propriamente dita, nós colocamos o primeiro plano de testes que atacavam o sigilo do voto, que tentavam, de certa forma, recuperar os votos em ordem, para que, caso a ordem dos eleitores também fosse conhecida, também fosse possível correlacionar com exatidão que eleitor votou em que candidato. No primeiro dia, nós executamos uma prova de conceito. Elaboramos um certo protocolo com o TSE e conseguimos recuperar em ordem – em uma eleição simulada e a partir apenas de informação pública, de documentos públicos produzidos pela urna eletrônica que são disponibilizados aos partidos após o final da eleição –, conseguimos produzir, restaurar ou reverter o embaralhamento com eleições até 21 eleitores. Cada eleitor, nessas eleições simuladas dos testes, votava em dois candidatos, então tivemos até 42 votos em ordem.

No segundo dia, nos foi sugerido pelo TSE repetir a mesma metodologia com um volume realista de dados. Então, a gente passou o segundo dia inteiro basicamente executando o protocolo, a nossa metodologia, para uma eleição com 475 eleitores, num total de 950 votos. No final do segundo dia, após a verificação dos resultados de forma conjunta com o TSE, ficou claro que a gente conseguiu reverter a ordem de uma eleição com 950 votos, o que já chega a um volume realista. Esse número de 475 eleitores foi calculado pelo TSE aplicando a média de comparecimento das eleições de 2010 ao tamanho médio das seções eleitorais do País.

Bem, no terceiro dia nós redigimos um relatório descrevendo os resultados, em conjunto com o TSE, o relatório do evento. Assim, terminou o evento. Depois de algum tempo, houve a premiação simbólica e as repercussões.

Se ainda não ficou claro, é importante que os votos sejam armazenados fora de ordem. Porque se alguém, algum oficial de mesa, por exemplo, ou o fiscal de um partido malicioso, consegue monitorar a ordem em que os eleitores votam, ele é capaz de recuperar os votos em ordem após a eleição e, apenas examinando informação que não é privilegiada, informação pública, consegue correlacionar exatamente que eleitor votou em quem.

Outra vulnerabilidade advinda desse mesmo problema com o sigilo do voto é que um certo eleitor, ilustre ou não, que votou numa certa posição num certo instante de tempo, por exemplo, às 10h30, pelo registro cronológico dos eventos armazenados pela urna eletrônica, também é possível conhecer a posição dele na fila de votação. Ele é a posição 50, por exemplo. Então, se você consegue recuperar os votos em ordem, é possível recuperar um voto específico depositado na urna eletrônica às 10h30 da manhã, sem nenhuma ambigüidade, com exatidão. Nós recuperamos os 950 votos sem nenhum erro. Apesar de que, quando relatado na mídia, nossa abordagem tem sido apresentada como tentativa e erro. Nesse caso, houve uma tentativa e zero erro. De fato, não foi tentativa e erro.

O procedimento não tinha a nossa metodologia de ataque. A probabilidade de erro era absolutamente determinística, como dizemos, novamente, em computação, e exigia apenas o exame de documentos públicos. Portanto, a fraude do sigilo do voto era não rastreável. Essa fraude obviamente permite o retorno, em uma versão digital, do que chamamos de “voto de cabresto” no Brasil, em que o candidato ou algum interessado em fraudar a eleição pressiona os eleitores para que eles votem em certa direção e depois consegue, a partir da recuperação dos votos em ordem, determinar se votaram como o esperado; se não, ele pode aplicar as punições que gostaria.

Bem, é claro que uma base de código desse tamanho, com a vulnerabilidade tão infantil, não teria apenas essa vulnerabilidade. Nas quatro horas restantes do exame do código fonte, nós encontramos outros problemas, muitos deles, o que é mais preocupante, de projeto, e não apenas de implementação. Vários mecanismos de segurança no *software* de votação foram projetados de maneira incorreta, ou por falta de treinamento, ou por falta de entendimento de como aquela primitiva segurança deve ser usada na prática, ou por falta de auditoria externa, ou por um processo de desenvolvimento que talvez não tenha, de fato, a segurança como primeiro objetivo, por uma série de razões.

Nós produzimos, depois do final do evento, quando a repercussão dos resultados começou, um relatório de 40 páginas, que está disponível na internet, e já vai ser publicado como capítulo de um livro acadêmico internacional, porque nossos resultados tiveram repercussão internacional. Fui convidado a ministrar palestras no exterior, e esse capítulo de livro foi convidado a ser publicado em um livro acadêmico. Mas, voltando, encontramos alguns erros de projeto fundamentais, exatamente na proteção da integridade dos resultados também.

Para citar alguns exemplos, todas as urnas eletrônicas do País, em torno de meio milhão de equipamentos em operação, compartilham a mesma chave de segurança. É a mesma coisa que meio milhão de pessoas no Brasil usarem a mesma fechadura na porta da casa. É absolutamente a mesma analogia. Se esse segredo, essa chave de segurança vaza uma única vez, é possível abrir o conteúdo desse meio milhão de portas, no caso, urnas eletrônicas, e as memórias de todos os equipamentos em operação.

Além disso, essa chave criptográfica, essa chave de segurança, é armazenada às claras nos cartões de memória, que o TSE chama de carões de carga. São aqueles que instalam *softwares* nas urnas eletrônicas. Ou seja, não só o vazamento dessa chave tem impacto absolutamente devastador, por permitir abrir os cartões de memória de todas as urnas em operação no País, como essa chave ainda é armazenada às claras no cartão de memória. Se você sabe o local e sabe, talvez, o início dessa chave criptográfica ou sabe onde procurar, você consegue recuperá-la, e, de fato, sistematicamente, consegue abrir os cartões de memória do País inteiro.

Por que isso é perigoso? Porque nesses cartões de memória, na partição protegida desses cartões de memória, ficam armazenados os *softwares* de votação. Se você é capaz de abrir o cartão de memória e ler o conteúdo completo dele, você consegue manipular o *software* de votação para que ele faça a contagem de maneira desonesta dos votos para os candidatos, por exemplo. E não só fazer a contagem desonesta. Também – por que não? – fazer a contagem desonesta e produzir um registro digital do voto que seja compatível com aquela contagem desonesta. De forma que qualquer recontagem ou possibilidade de recontagem posterior vá sempre refletir a fraude que foi inserida no *software* de votação.

Esses não são erros de projetos sofisticados do ponto de vista de que são incomuns ou talvez exijam conhecimento de especialistas para evitá-los, é o tipo de coisa que eu ensino na minha disciplina de graduação, inclusive o próprio ataque ao sigilo do voto que nós montamos nos testes. Eu coloco como bônus das minhas provas na graduação e 80% dos alunos acertam com absoluta exatidão.

Então, não foi necessário conhecimento especialista, nem para encontrar essas vulnerabilidades e erros de projetos, nem para de fato atacar o sigilo do voto durante os testes.

Não é uma especulação que o voto, o *software* de votação utilizado no Brasil é inseguro. Ele é demonstravelmente inseguro. Essa foi a nossa conclusão ao final do evento, ao final do nosso contato com o *software* de votação.

Vale salientar que nós tivemos contato de apenas cinco horas com 17 milhões de linhas de códigos. Então, tivemos apenas a chance de navegar por uma fração muito pequena, apesar de estratégica, do *software* de votação.

Simplesmente, com a própria premiação que o TSE nos forneceu pela participação, pela contribuição neste teste, o *software* de votação é demonstravelmente inseguro, experimentalmente inseguro.

Nós conseguimos exercitar uma metodologia de ataque durante os testes e tivemos uma série, uma outra metodologia de ataque com relação e direcionada à integridade dos resultados, que não pode ser mais exercitada por simples falta de tempo.

Curiosamente, após os testes, nós nos disponibilizamos ao TSE para, de fato, colocar aquelas ideias, aquele plano de testes relacionado à integridade dos resultados em prática, mas não houve nenhum tipo de possibilidade de colocá-las. O que eu acho curioso, porque deveria ser de interesse do TSE entender exatamente que erros de projetos nós detectamos, nós encontramos, e se é de fato possível, como parece ser, executá-los inclusive na prática, não mais num ambiente simulado.

Então, dado que o *software* de votação é demonstravelmente inseguro ou contém erros de projetos e implementação detectados e verificados experimentalmente, a conclusão é simples: nós precisamos de um registro físico do voto, que não seja accessível pelo eleitor, como já descrito anteriormente, para permitir a verificação independente por parte do eleitor, fiscais de partido interessados de que as contagens, os resultados produzidos pela urna eletrônica, são de fato honestos.

Nós precisamos de um outro mecanismo redundante.

Essa é a prática em todo mundo. A Suprema Corte indiana decretou, por exemplo, depois de avaliar o mecanismo do voto impresso em caráter experimental, que nas eleições de 2014 todas as máquinas de votação devem ter o voto impresso. Essa foi uma decisão tomada na última semana e segue na direção de todos os equipamentos de votação eletrônica do mundo. Todos os equipamentos de votação eletrônica do mundo produzem mais de um registro do voto em mídias diferentes para permitir, exatamente, recontagem e verificação de resultados.

Não creio que seja admissível, ou não creio que as dificuldades práticas que são frequentemente citadas, sejam obstáculos apenas no Brasil. Elas não são obstáculos em outros lugares do mundo. Por que impressoras ou qualquer armazenamento, qualquer outro tipo de mídia, é problemático apenas no Brasil? Todos os países do mundo usam exatamente esse tipo de recurso.

É absolutamente consenso na academia de que – na academia internacional, inclusive, frequento eventos de votação eletrônica fora do Brasil – os países, os sistemas de votação, precisam de mais de um registro do voto para permitir exatamente essa verificação, independente de resultados. Isso é ponto absolutamente pacífico.

Outras conclusões que nós obtivemos, a partir dessa interação com o *software* de votação, é que há uma ênfase muito grande em ofuscação e não em segurança de fato. O TSE está muito preocupado em projetar mecanismos que sejam resistentes unicamente. Aqui não há informação detalhada do *software* de votação. O que nós chamamos de agente externo: pessoas que estão fora do TSE, não têm nenhuma informação e estão interessadas, de fato, em provocar algum tipo de fraude. Quando nós sabemos que é bem perigoso, especialmente num projeto desse tipo de mecanismo, o conhecimento privilegiado que agentes internos têm.

A área de segurança da computação diz exatamente que é importante projetar mecanismos de segurança que resistam até ao próprio projetista do mecanismo. Um dia, ele pode se tornar um agente malicioso, um rival daquele mecanismo. Não podemos confiar incondicionalmente nas pessoas.

No Brasil nós temos confiado incondicionalmente no TSE como uma autoridade executora das eleições e num *software* de votação demonstravelmente inseguro, experimentalmente inseguro, para executar as nossas eleições.

Então, acho que essa situação é insustentável e, de fato, nós precisamos retornar à implantação do voto impresso, seguindo a tendência mundial e seguindo também o que aponta como solução para esse tipo de problema a própria academia internacional.

Agradeço muito a atenção de vocês.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Obrigado Prof. Diego.

Registramos aqui a presença do Deputado Eduardo Azeredo, nosso conterrâneo, que só tem um defeito: é americano, mas perdoamos.

Vou registrar só um comentário do Eduardo Torrens Godinho: “O eleitor quer ver para quem foi o voto, em papel impresso. Esse papel será o voto. Os países que usam urna eletrônica imprimem o voto para que o eleitor saiba que o seu voto foi registrado corretamente e para auditoria independente do *software*. Isso qualquer fiscal faz.” – segundo ele.

O Deputado Eduardo Azeredo pediu a palavra, Senador Capiberibe, se não houver objeção.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Sr. Presidente, na verdade gostaria de sugerir que concedesse a palavra ao Deputado Eduardo Azeredo para que pudéssemos ter o mínimo de contraditório nesse nosso debate, já que a ausência de um representante do TSE prejudicou muito esta audiência pública, o que é profundamente lamentável. Insisto em lamentar, porque, de fato, fomos prejudicados pela ausência de um representante do TSE.

O Deputado Eduardo Azeredo, que é o autor do Projeto de Lei, está aqui presente e para nós é importante ouvi-lo. Essa é a minha sugestão e, em seguida, farei algumas perguntas.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Está bem, Senador. É importante a participação do Deputado e agradeço a presença, porque o contraditório é sempre importante. Estamos ouvindo praticamente um lado só, estamos ouvindo as pessoas que são contra o projeto, na verdade. Então, é bom ouvir V. Exª, para que possamos estabelecer o contraditório.

Com a palavra o Deputado Eduardo Azeredo.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Senador Zeze Perrella, Senador Capiberibe, senhores expositores – Amilcar, Diego e Pedro Rezende –, quero primeiramente lamentar não ter o contraditório, porque, em uma audiência pública, é fundamental que tenhamos os dois lados.

A proposição desse projeto foi feita em 2010, exatamente depois que havíamos tido aprovação pelo Senado do fim do voto impresso, dentro da minirreforma eleitoral, que foi feita em 2009, e a Câmara só acatou alguns poucos pontos, o ponto da internet basicamente, que é o que liberou o uso da internet, eram quatro artigos. Os outros pontos todos a Câmara deixou de analisar, inclusive o fim do voto impresso, porque não deu tempo. A Câmara recebeu em 24 horas de prazo final, tanto que muitos desses pontos estão sendo reeditados agora nessa nova tentativa de minirreforma eleitoral.

Então, só para entender um pouco o contexto do momento que foi apresentado esse projeto de não exigir o voto impresso.

Por outro lado, é importante lembrarmos que a primeira urna eletrônica de porte, num país de porte, foi a nossa, no Brasil. Essa é uma iniciativa da tecnologia brasileira, os brasileiros têm muito orgulho da urna eletrônica. Até hoje, depois de implantado todo esse tempo, não há nenhum registro que eu diria sólido de manipulação dessa urna.

É evidente que nenhuma tecnologia é perfeita. A Presidenta Dilma, depois de 11 anos do Governo do PT, está propondo um *e-mail* mais seguro ao Serpro. Para minha surpresa, fui Presidente do Serpro e achei que o Serpro já tinha um *e-mail* mais seguro. Imaginava eu que os *e-mails* do governo já fossem mais seguros do que um simples *firewall*, tipo de segurança que existe para as pessoas comuns – digamos assim. O Governo, evidentemente, deveria ter.

Então, veja bem como a tecnologia é sujeita a mudança toda hora. A Presidenta da República, depois de 11 anos, em função de uma espionagem americana, que também não é novidade, já acontece há muito tempo, que não é só americana também, resolve determinar ao Serpro que tenha um *e-mail* mais seguro.

Então, segurança total, Senador Capiberibe, nunca vai existir. Agora, o fundamental é entender que em relação a nossa urna nunca houve um questionamento com densidade. O que existe de crítica é uma coisa que um diz, que outro diz, aquela coisa apenas verbal. Não há nenhuma prova efetiva.

A urna tem criptografia, tem todos os procedimentos necessários de segurança. O grande achado da urna é que ela é separada, cada urna envia de uma vez o resultado dela mesma. Para poder haver uma manipulação, teria que haver uma conjunção de fatores, teria que juntar várias urnas, teria que haver uma quebra do programa – o programa é o mesmo –, teria que fazer uma nova versão do programa para distribuir pelo Brasil afora.

Então, ela tem uma concepção muito interessante.

“Existem países que têm o voto impresso.” Sim, certamente existem. Agora, o que é acontece é que não há dúvida de que o voto impresso é um complicador. Encarece? Não há dúvida que encarece a máquina. Os fabricantes de máquinas têm interesse, sim, que se haja o voto impresso, porque ficará mais caro. Não há dúvida de que o voto impresso tem mais chance de quebra da máquina do que o voto eletrônico. É questão de mecânica e de eletrônica. A mecânica tem mais chance de defeito do que a eletrônica. Não há dúvida de que a verificação manual é mais falha do que uma verificação feita pelo sistema eletrônico, em que há os votos colocados, os partidos têm acesso. Se não fazem o acesso, é outro problema, inclusive para o meu Partido, o PSDB. Se os partidos não verificam, é outra questão.

Agora, que eles têm o direito de verificar o programa, de analisar o programa, eles têm esse direito.

Então, considero que voltarmos com essa proposição que chegou a existir... Primeiro tivemos a implantação do voto digital. Depois, a Câmara aprovou o voto em papel. O Senado negou, rejeitou. A Câmara voltou com ele. O Supremo ou o Tribunal Superior Eleitoral, não sei exatamente qual dos dois, definiu que era inconstitucional inclusive, tanto é que não foi nunca utilizado o voto impresso. Ele nunca foi utilizado no Brasil dessa forma, como contraprova da votação eletrônica.

Considero que seja importante que possamos manter a confiança na tecnologia brasileira, que possamos aumentar os meios de fiscalização dos Partidos – eles podem verificar os programas – e que possamos estar sempre lembrando que a urna com o dispositivo de impressão seguramente será mais falha, mais cara, mais demorada e não garantirá a fidedignidade dos votos. Continuaremos tendo riscos humanos, que existem em qualquer tipo de procedimento eleitoral.

Mas eu, sinceramente, estou muito satisfeito com a nossa urna eletrônica. Acho que é uma tecnologia, um modelo fantástico que permite que, em poucas horas, tenhamos as urnas de distantes locais do Amazonas somadas às urnas de São Paulo, de Minas, de todos os lugares. O resultado dessa urna eletrônica é realmente um grande sucesso. Podemos dizer que são tecnologicamente três grandes sucessos que o Brasil tem: imposto de renda eletrônico, urna eletrônica e a Embraer. Acho que são, do ponto de vista tecnológico, os três maiores exemplos que temos.

Então, darmos um passo atrás, não considero que seja adequado, daí o objetivo, portanto, de manter o sistema simples, mais barato e que funciona.

**O SR. PRESIDENTE** (Zezé Perrella. Bloco Apoio Governo/PDT - MG) – Muito bem, Deputado Eduardo Azeredo.

Com a palavra o Senador João Capiberibe.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Sr. Presidente, acompanhei a explanação do Prof. Diego Aranha, que identificou uma vulnerabilidade que ele classificou de infantil. Fiquei mexendo com a minha experiência de eleitor, que não é tão longa, porque passamos muitos anos sem votar no Brasil, no período da ditadura. Sei que fui votar pela primeira vez já em 1982.

Em 1986, na eleição para Assembleia Constituinte, eu era fiscal de uma seção e, lá pelas tantas, eu identifiquei um voto corrente, que é aquele voto em que o eleitor não coloca a cédula na urna, ele leva a cédula com ele, mostra que votou, entrega a cédula para o outro e aí eles vão votando na mesma pessoa que comprou a consciência daquela pessoa.

E eu pedi a suspensão da apuração. Aí o juiz, mal-humorado, me chamou à parte. Era voto em papel, eram cédulas, e ele me chamou à parte e disse: “Olha, eu não pretendo ficar aqui até o final do ano. Se você impugnar esta urna, vai haver um processo, e vou ser obrigado... Eu já estou com as minhas malas prontas para ir embora. Depois, tem mais, olhe os votos da sua candidata [porque eu estava fiscalizando para o meu Partido], ela está ganhando a eleição”.

Eu disse: sim, ela está ganhando a eleição, mas há uma fraude. Mesmo que a minha candidata esteja ganhando a eleição, nós estamos diante de uma fraude eleitoral.

Eu sei que o juiz se recusou a suspender e abrir processo. E, agora, o Prof. Diego nos assegurou que, no teste das urnas de 2012, foi detectada a possibilidade da identificação do voto do eleitor por meio da listagem, o que pode repetir exatamente o voto corrente. Quer dizer, é tão elementar a vulnerabilidade dessa urna eletrônica, que nós podemos voltar a uma fraude que acontecia com o voto impresso.

Então, eu fiquei realmente impressionado com o grau de vulnerabilidade demonstrada aqui pelos expositores. E eu acho, Deputado, que nós precisamos evoluir. A tecnologia se modifica a cada dia praticamente, numa evolução fantástica, e nós também temos que evoluir para render satisfação ao eleitor.

Eu não consigo entender por que eu não tenho direito como eleitor de ver o meu voto. Eu tenho direito de votar, mas eu não tenho direito de saber para onde foi esse voto; eu não tenho a menor segurança; pelo menos é o sentimento que eu tenho quando eu vou lá à urna eletrônica, que eu digito o número do meu candidato e depois dali eu já não sei mais o que acontece.

Portanto...

**O SR. EDUARDO AZEREDO** (PSDB - MG) – O eleitor tem que confirmar, aparece o voto dele, ele tem que confirmar. Ele está só confiando que esse voto vai para a mídia eletrônica. É só isso.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – É exatamente isso. Depois que eu confirmo, eu dependo do *software.* Todos aqui, Senador, o Prof. Pedro, o Prof. Amilcar Brunazo, o Prof. Diego, afirmaram que a segurança do voto depende do *software*. Ora, o *software* é feito por seres humanos e controlado por seres humanos. Por maior confiança que tenhamos, é preferível termos controle, possibilidade de auditar essas urnas. Depois, o custo de uma fraude é infinitamente maior do que qualquer gasto que se possa ter com a simples comprovação do voto. Não há custo que pague uma fraude eleitoral, porque quem frauda eleição é quem tem muito dinheiro para fazer isso. Então, se retira a possibilidade de uma representação mais ampla da sociedade brasileira.

Já é muito restrita. Quando analisamos a composição da Câmara e do Senado, a representação dos trabalhadores, de gente do povo, é minoritária nessas Casas. Se permitirmos que não avancemos... porque o que queremos é avançar com a política junto com a tecnologia.

Vejo com muita preocupação as nossas instituições. Por exemplo, o caso do título de eleitor. Confesso que, a cada eleição, nós tínhamos uma dúvida. Em alguns Municípios, o juiz determinava que tinha que levar a carteira de identidade com a fotografia. Em outro Município, não, bastava o título de eleitor. Os mesários, muitas das vezes, criavam problema com o eleitor, porque ele estava com o título.

Ou seja, depois de não sei quanto, quase um século – a Justiça eleitoral foi criada em 1932 e esse título de eleitor eu não tenho ideia de quando ele surgiu. Mas depois que me entendi com pessoa já fazem muitos anos que..

**O SR. AMILCAR BRUNAZO FILHO** *(Fora do microfone.) –* O modelo atual é de 1986.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Não, o modelo atual. Mas antes havia um cartão grande de papel, eu me lembro que se carimbava.

De repente, o próprio TSE declara que não serve para nada. Então, mostra que a evolução do processo de votação no País é de uma lerdeza que faz com que o cidadão desconfie, porque é muito lento o processo de transformação.

Temos três modelos de urna eletrônica. Prefiro o que me dá mais segurança, que é aquele que permite ao eleitor enxergar em quem ele votou. Ele nem toca na cédula, até por que se tocar na cédula pode voltar o voto corrente. É cair direto na urna. Perfeito, porque eu vou lá, digito o número dos meus escolhidos, enxergo e ver registrado no papel. Vou confirmar, esse voto vai ficar ali e vai o registro eletrônico. Lá na frente, perfeitamente, o meu fiscal pode conferir as duas coisas.

Do jeito que é hoje, ninguém confere nada. Aliás, nem os Tribunais Eleitorais têm a menor paciência, porque é uma crença na urna eletrônica que não admitem nem a possibilidade de se pedir uma auditagem. Não se consegue auditar nenhuma eleição no Brasil, porque é inadmissível que se coloque em discussão. Ninguém está colocando em dúvida. O que queremos é aperfeiçoar o sistema. Do jeito que está, o sistema é vulnerável; e estão identificadas aqui as vulnerabilidades.

Tenho a impressão de que os professores que aqui nos informaram – vi pelos currículos que são engenheiros especialistas em segurança de informática: Dr. Amilcar Brunazo; Dr. Pedro de Rezende, Professor de Matemática e Criptografia do Departamento de Computação da UnB; e o Prof. Diego, do Departamento de Ciência da Computação da UnB. Concentram um conhecimento e chegam aqui... a não ser que estejam representando empresas queiram comercializar alguns desses novos produtos.

Esta é a primeira pergunta: os senhores têm vinculação com alguma empresa da área de informática, de computação? Os senhores trabalham para essas empresas? É uma questão que gostaria que me fosse respondida.

A questão da biometria também: qual o custo? Ninguém discutiu o custo da identificação biométrica e, muito menos, a eficiência. Estamos conhecendo aqui que ela não tem lá essa eficiência toda.

Então, é importante nós analisarmos, e essa identificação biométrica já deu origem a alguns problemas graves, como, por exemplo, o fornecimento de cadastro desses eleitores para terceiros, não é? Isso é de extrema gravidade. Por isso que as nossas instituições são colocadas sob suspeição. Quando uma instituição como o TSE abre o cadastro de eleitores para, como foi colocado aqui, um sindicato das funerárias, cadastro dos mortos, me deixa muito preocupado. Para o Serasa, que nós acompanhamos na mídia e que até agora não houve nenhum desmentido. Essas denúncias não foram desmentidas.

Portanto, nós temos que valorizar nossas instituições, criando essa possibilidade de acompanhamento, de fiscalização, de transparência, porque o Brasil tem dado saltos importantes no uso da informática para a promoção da transparência. E agora nós temos leis que nos permitem acessar todo tipo de informação. E temos leis que obrigam a exposição de gastos públicos. E o TSE precisa entender que essas vulnerabilidades aqui identificadas precisam ser consideradas e serem resolvidas.

Portanto, acho que a gente precisa conversar sobre o projeto que tramita aqui. Eu vou apresentar algumas emendas ao projeto, para que a gente possa, então, dar esse salto adiante, para a gente fazer esse avanço.

Mas eu gostaria, Sr. Presidente, senhores expositores, que os senhores me respondessem essa pergunta, para, então, eu fazer mais uma pequena intervenção.

**O SR. AMILCAR BRUNAZO FILHO** – Quanto a ter ligação com alguma empresa, o pessoal em geral diz que eu tento vender impressora, que eu seja representante de alguma empresa fabricante de impressoras.

Acho importante primeiro destacar o seguinte: a urna eletrônica já tem impressora. Todas as urnas têm. Mesmo que não use o voto impresso, elas têm impressora. Elas precisam imprimir boletim de urna, a zerésima, os outros documentos de auditoria. Então, não precisa comprar uma impressora nova. As urnas eletrônicas, como mostrei fotos da Argentina, da Venezuela, também usadas na Bélgica, do México, têm uma impressora só. Aquela que imprime o voto, do México, que eu mostro lá em cima, é uma impressora só, que imprime o BU, imprime tudo e mostra.

Então, não precisa comprar uma segunda impressora. Eu não estou representando fabricante nenhum, porque não precisa comprar impressora para fazer o voto impresso. Poderia talvez ser representante de fabricante de papel, não é? Papel vai gastar mais, disso não há dúvida. Não, eu não tenho ligação com empresa nenhuma.

Na verdade eu já estou aposentado faz mais de dez anos. Eu tinha uma empresa, quando comecei nessa discussão sobre urna eletrônica, nos anos de 1998, 2000, eu tinha uma empresa de segurança de dados, fazia sistemas de criptografia e segurança, criptografia em disco, tudo isso. Mas essa empresa já foi encerrada no começo dos anos 2000, 2002. Foi encerrada, e eu não tenho mais vinculação nenhuma, com empresa nenhuma, ligada nem a tecnologia da informação, nem a impressora, nada disso.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Com a palavra, o Prof. Diego Aranha.

**O SR. DIEGO ARANHA** – Bem, eu também não tenho nenhum tipo de vinculação, nem com empresas ou partidos. Eu sou professor da Universidade de Brasília. Recentemente fui aprovado em concurso na Unicamp, então vou me tornar professor da Unicamp no próximo ano, retornando à Universidade em que me formei. Eu tenho doutorado em criptografia pela Unicamp.

Então, imagino que estou em posição suficiente para dizer que, por mais que a urna tenha mecanismos criptográficos, dentre todos os que eu pude examinar, eu não encontrei um único mecanismo criptográfico que tenha sido projetado e implementado seguindo as boas práticas da literatura. Alguns com erros graves de projeto e implementação, conhecidos, no caso do sigilo do voto, há 17 anos.

Então, eu me considero na posição de fazer esse tipo de julgamento.

Voltando à questão de ter filiação ou relação com algum partido ou alguma empresa, é curioso porque, apesar de eu ser apartidário e ser apenas um professor concursado em universidade pública, eu não tenho a mínima possibilidade, também por falta de transparência no processo, de sequer verificar se as vulnerabilidades que eu apontei nos testes públicos de segurança foram corrigidas ou não, inclusive aquela ligada ao sigilo do voto, porque membros da Academia também não têm a possibilidade, a não ser que se filiem a partido ou se tornem partidários, de examinar como o *software* de votação tem sido construído e que mecanismos de segurança foram implementados e se eles, de fato, atingem seus objetivos ou não.

Voltando a outro comentário também, eu acho curioso supor que a urna eletrônica, o *software* de votação resista a um adversário de fraude, a um cenário de fraude eleitoral, que, muitas vezes, é muito bem financiado e muito poderoso, se ele não resistiu a apenas seis dias de um evento com um professor e com três funcionários da universidade que trabalham na área de segurança de rede, que foram apenas como curiosos, sem conhecimento prévio do sistema, avaliar a segurança deste. Então, como esperar que esse *software* resista a, de fato, um adversário muito poderoso e muito bem financiado, se ele não resistiu, em seis dias, a quatro entusiastas que participaram dos testes públicos de segurança do TSE?

Então, a falta de transparência, a falta de possibilidade de auditoria por acadêmicos ou por interessados que sejam independentes de partidos impregna e, inclusive, incentiva, na minha concepção, a algumas péssimas decisões de projeto que tenham sido tomadas, simplesmente porque não há nenhum tipo de auditoria externa qualificada que possa verificar que aquele *software* atende às boas práticas muito bem descritas na literatura.

Voltando, todas as vulnerabilidades que nós encontramos estão muito bem documentadas em documentos que passaram pelo processo de revisão por pares, que é o que a gente considera como processo científico ideal, e as nossas conclusões foram, de certa forma, confirmadas pelo processo de revisão por pares. São vulnerabilidades graves que nunca deveriam existir em *software* de votação, em *software* de infraestrutura crítica. Simplesmente elas não deveriam estar lá.

É isso.

**O SR. PRESIDENTE** (Bloco Apoio Governo/PDT - MG) – Muito bem, professor.

Com a palavra o Deputado Eduardo Azeredo.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Eu quero só complementar um pouco.

Primeiro, essa mensagem que foi mandada há nove horas, do Sr. Eduardo Torrens Godinho, pede para ter o voto impresso na mão, para ele colocar na urna. Aí, sim, é uma parafernália. Pode acontecer fraude, coronelismo, outra vez, por ter que mostrar o retrato, o povo de fora pode tirar retrato... Eu imagino, e gostaria de ouvi-los, que essa hipótese vocês dois, os dois expositores, sejam contrários. Imagino que sim. A hipótese única aqui abordada seria aquela de deixar cair. A tendência é que a que cai na urna automaticamente caia na sequência de votação. Concorda?

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP. *Fora do microfone.*) – Não necessariamente.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Não necessariamente. Então, vai ter que ter um ventilador para poder embaralhar ali dentro. O problema todo é esse. Ela vai cair na mesma sequência. Então, na hora de verificar, vai-se identificar o voto, o que é uma coisa mais grave ainda.

Agora, eu entendo, Senador Capiberibe. O Partido que começou com esse questionamento foi o PDT. Por quê? Lá em 1982, eu estava trabalhando na IBM ainda, eu era fiscal e me licenciei da IBM para ser fiscal do antigo MDB nas eleições de Minas, do Tancredo Neves. Na época, era duro realmente. A cópia do boletim que vinha, tiravam uma xerox do boletim e entregava-se para o SNI primeiro. Depois é que se entregava para os partidos. Nós éramos cinco partidos naquela época. É evidente que era um sistema extremamente frágil. Havia realmente um mapismo. Era normal ver o voto do candidato de cima ir para o candidato debaixo. A totalização era feita manualmente e depois era digitada só a totalização da urna. E isso foi continuando.

Houve situações em que havia todas as urnas da cidade com uma média de 10 votos em branco e uma determinada urna não tinha nenhum voto em branco, mostrando, que, evidentemente, foi aproveitado. Nós tivemos um caso, em Minas Gerais, em Ituiutaba, em que os votos em branco foram todos aproveitados para dois candidatos da cidade pelo pessoal que estava apurando – isso foi provado depois. Eles se convenceram de que era importante para a cidade. Então, todo voto em branco era dividido de maneira igualitária para um candidato e para outro, para ter dois Deputados.

Então, era inadmissível que continuasse esse processo antigo. Então, nós tivemos um grande avanço, sim. Eu queria insistir que existe certa paranoia nessa questão da urna eletrônica. Esses mesmos problemas que são apontados de criptografia existem no Imposto de Renda eletrônico que é feito por internet. O mesmo problema pode acontecer. Quer dizer, o que nós temos que fazer é evoluir, sim, mas evoluir na segurança, no tipo de criptografia.

Quando eu comecei a propor alterações no Código Penal na questão da tipificação dos crimes cibernéticos, eu fui criticado por alguns, tentaram ridicularizar. Depois, todos eles tiveram de rever as suas posições com os fatos. Quando eu dizia que tinha que guardar o IP, o registro do voto, diziam que isso era loucura, que era censura. Aí, o Governo mesmo propôs gravar. Só que, em vez de três anos, propôs gravar um ano, prorrogável por quanto tempo for necessário. Por quê? Porque reconheceu que é fundamental, para chegar ao autor de um delito, que se tenha o registro dessa ocorrência.

É bom haver a discussão, porque isso tudo vai evoluindo. As pessoas vão se convencendo. Essa questão toda da espionagem é mais um episódio que mostra a fragilidade brasileira em enfrentar essa situação. A culpa é dos Estados Unidos? É, porque é um país que extrapola sua espionagem. Mas a culpa é do Brasil também, que nunca soube se defender.

Então, nós não precisávamos ter essa paranoia com a urna eletrônica, quando o sistema de impressão seguramente trará outros inconvenientes. E eu reitero aqui que pode não ser o preço, mas o de falha técnica, o de demora de tempo, na hora de verificar ser muito mais vulnerável do que o anterior, quando se vai contar à mão.

Então, eu colocaria somente essa pergunta sobre se vocês atendem ou não? Se os expositores se concordam em que o papel possa chegar à mão do eleitor? Porque aí é difícil. Eu considero que teria que ser no mínimo automático.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Sr. Presidente?

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Com a palavra o Senador Capiberibe.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Eu, inclusive, quando vi as duas urnas, uma em que o voto impresso cai direto e a outra em que se deposita, não há a menor dúvida. Eu acho que aqui não há a menor dúvida sobre as nossas escolhas.

Sem dúvida, o Brasil deu um salto em todas as direções. Houve uma enorme evolução. Mas, nessa questão da urna eletrônica, quanto à segurança, nós estamos patinando, porque a segurança que nós queremos é a garantia de que o eleitor veja em quem votou, porque, sem isso... A crença é uma prática comum, mas há crenças diversificadas. Então, acredita-se que essa urna eletrônica seja correta, mas é melhor ver: votei aqui, caiu aqui. E no final juntam-se as duas pontas e tem-se algo absolutamente seguro.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Não seria, Senador, muito mais para conferência? Porque quando se vai votar na urna eletrônica, está se vendo em quem está votando, a cara da pessoa aparece lá. Então, é uma questão de ver por ver.

Eu entendo que esse papel, esse comprovante serviria muito mais para se fazer depois uma checagem se o voto que está na urna eletrônica confere com aquele do papel. Em quantidade, pelo menos.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Mais ou menos, Sr. Presidente. Sabe por quê?

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Sim.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Porque aquela fotografia que aparece ali pode ser a minha, mas aquele voto que eu digitei pode não ir para mim, porque eu dependo do *software*, do programa. Eu posso digitar 40 e pode ir para o 15. Isso é possível, até porque...

**O SR. EDUARDO AZEREDO** (Bloco Minoria/PSDB - MG) – Essa foi a fraude do Proconsult em 1982.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Não foi no voto.

**O SR. EDUARDO AZEREDO** (Bloco Minoria/PSDB - MG) – Mas para repetir isso, agora, tinha que ter a versão adulterada do *software* em todas as sessões, cada urna tem por volta de 300, 400 votos válidos, no máximo. Então, seria preciso o processo, a mesma versão do *software* adulterado teria que ser implantado no computador, com o conluio de quem está responsável por aquele processo. Quer dizer, o presidente da mesa, o secretário da mesa, teriam de estar de acordo com que uma pessoa estranha chegue e troque o *software* que foi implantado pelo TSE. Ou, então, o TSE mesmo tem que implantar um adulterado, para fraude. Aí acho difícil acontecer isso.

Daí insisto na questão da paranoia.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Mas nós temos, Senador Eduardo Azeredo... Eu entendo assim: se nós já temos as máquinas, o custo só do papel eu não acho que seria...

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – O custo... E depois o seguinte, o problema da tecnologia tampouco é tão grave, porque se pegarmos, por exemplo, essas máquinas de cartão de crédito, elas nunca quebram, senão o sujeito não recebe. Então, quase nunca quebram essas máquinas. Há a máquina do supermercado, que calcula tudo. Nós temos uma evolução fantástica! E vamos colocar essa evolução ao lado da segurança do eleitor.

V. Exª tem inteira razão, nós evoluímos, mas precisamos evoluir mais, precisamos garantir ao eleitor, garantir a todos aqueles... Tenho certeza de que, se os eleitores deste País ouvissem o que nós ouvimos aqui... porque são argumentos que não deixam dúvida. Esse argumento da identificação do voto não me parece absolutamente factível. E foi testado com 470 votos e eles acertaram todos. Então, se há uma vulnerabilidade elementar, infantil, o que mais deve haver nesse processo?

**O SR. EDUARDO AZEREDO** (PSDB - MG)– Então, eles podiam propor um sistema mais seguro de criptografia, pois são estudiosos da Academia. Eles podiam propor um outro sistema de criptografia que fosse mais seguro contra os *hackers*, os *crackers,* pois eles estão também a cada dia mudando. Existe certa complacência, há gente que acha bonito haver *hackers*. Então, é preciso haver uma atitude proativa. Por que os críticos não propõem soluções tecnológicas avançadas? Ninguém questiona o que está no *pen drive* que se pega com seu discurso; ninguém questiona se o seu discurso foi alterado; ninguém questiona se o que foi colocado na Justiça, que é a cópia do processo, que vem tudo num disquete; ninguém questiona isso. Volto a dizer, o imposto de renda não é questionado sobre esse aspecto, o aspecto da transmissão.

Então, o sistema eletrônico de votação é a base da democracia, a eleição. Sim! O que eu estou dizendo é que eu já acompanho a busca dessa coisa desde 1982. Então, é fundamental termos um processo respeitado, Senador. Agora, precisamos avançar. Quando digo avançar, falo em avançar eletronicamente. Está todo mundo avançando cada vez mais, há uma tal de computação em nuvem, mais não sei o quê. Então, vamos fazer o contrário? Vamos voltar ao processo mecânico? Não vejo sentido. O objetivo do projeto é manter a segurança necessária, mas sem esse risco que nós temos.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Não seria o caso de adicionar mais segurança? E não tem nada mais seguro do que ver para crer.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Mas a gente vê. É como o Senador Perrella está dizendo...

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Serve para auditagem, mas também serve para gerar confiança no cidadão na urna eletrônica, no procedimento.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Mas a população confia.

**O SR. JOÃO CAPIBERIBE** (Bloco Apoio Governo/PSB - AP) – Eu confesso que tenho dificuldade em entender essa resistência a pingar um voto na urna de forma concreta. Eu acredito na informática. Tanto acredito na informática e na transparência que eu sou autor de um projeto de transparência, que obrigou os órgãos públicos a colocarem na internet, em tempo real, suas despesas e receitas. E é de 2004, nós estávamos juntos no Senado. O ano de 2004 pode ser considerado como o ano de nascimento desses processos todos. Hoje não, avançamos muito mais. Desde lá que a gente vem trabalhando o voto eletrônico, tentando dar um passo adiante, porque, na verdade, o passo da modernidade, da transparência, é, de fato, convenhamos, dar ao cidadão o direito de ele simplesmente comprovar em quem ele está votando.

Era isso, Sr. Presidente, Srs. Senadores.

Obrigado pelas exposições. Obrigado ao Deputado Azeredo.

**O SR. PRESIDENTE** (Zezé Perrella. Bloco Apoio Governo/PDT - MG)– Muito obrigado, Senador.

Passo a palavra ao Sr. Amilcar Brunazo. O senhor poderia responder e ir para as considerações finais, por favor, professor.

**O SR. AMILCAR BRUNAZO FILHO** – Eu vou responder primeiro a uma pergunta do Senador Zezé Perrella e, depois, respondo a do Eduardo, porque vou ter de me alongar um pouco mais na do Deputado Azeredo.

Ele me perguntou se não poderia haver fraude também na impressão do voto, ou seja, imprimir errado, ou imprimir certo, mas conta errado, enfim, pode, sim, Senador. O objetivo de pôr o voto impresso junto com o voto eletrônico é para que um possa auditar o outro. Se houver uma fraude no eletrônico o impresso detecta; se houver uma fraude no impresso, o eletrônico detecta.

Existem também mecanismos para dificultar a fraude no voto em papel, no voto impresso. Por exemplo, o uso da assinatura digital. É uma tecnologia que a gente recomenda, a assinatura digital da urna no voto impresso; ou seja, aquele voto impresso só poderia ter sido assinado por aquela urna. Se alguém usar outra urna, outro computador, para imprimir um voto, tal conteúdo, na hora em que se colocar no meio da sacola para confundir a auditoria, vai ser detectado que aquele voto não é daquela urna, porque a assinatura dele não é válida. A assinatura digital identifica a origem.

Enfim, dá para usar tecnologia para defender o voto impresso, e o voto impresso vai defender o voto eletrônico. Se houver uma fraude no eletrônico, o impresso revela, e vice-versa.

Quanto à diferença, Senador Zeze Perrella, entre ver o voto na tela eletrônico e ver o voto impresso, há uma diferença muito conceitual, que separa completamente um sistema do outro. O voto eletrônico se vê na tela, confirma e, depois, ele grava o registro digital do voto. O voto impresso imprime, ou seja, grava no papel, aí você confirma depois de impresso. A diferença é que, no voto impresso, você está confirmando o que você viu que foi registrado, enquanto o voto eletrônico você está confirmando antes de ser registrado. O que é registrado você não vê. Essa é a diferença.

Por isso, pede-se sempre o voto impresso, porque o voto impresso o eleitor vê; o registro digital do voto o eleitor não vê.

Gostaria de responder algumas questões ao Deputado Azeredo.

Vou tentar, aqui, convencê-lo – sei que já me ouviu em outras audiências – de que o voto impresso não é um retrocesso, como o senhor sempre diz.

Como foi apresentado pelo Prof. Pedro Rezende, as três gerações, as máquinas de votar, na primeira... Antes, existia o voto manual, que era só papel. Havia um monte de problemas, como o Senador descreve. Depois, veio o voto puramente eletrônico – são as máquinas de RE –, como é usado no Brasil. Depois, no resto do mundo, testaram-se as máquinas de RE; foram testadas na Holanda, e proibidas; foram testadas na Alemanha, e proibidas; foram testadas na Argentina, abandonadas; foram testadas no Paraguai, e abandonadas; foram testadas nos Estados Unidos, e criaram uma norma para excluí-las da norma técnica.

Enfim, a urna puramente eletrônica foi testada, e a tecnologia evoluiu no sentido de passar para o voto eletrônico mais o voto impresso. Então, o voto impresso vem agregar segurança ao voto eletrônico. Nesse sentido, ele é uma evolução; não uma involução.

Gostaria de dizer que o sistema de terceira geração, o primeiro que foi criado, citado aqui o Scantegrity, o sistema E2E, ou seja, de ponta a ponta, que permite auditoria total, foi proposto por um grupo de criptógrafos muito renomados. O principal nome da equipe, o mais conhecido, é o Ronald Rivest, que é o inventor do sistema de assinatura digital.

Eu trouxe aqui, pois já sabia que provavelmente surgiria essa questão. Esse aqui é o *token* que tenho no meu banco para me autenticar; para poder dizer na minha casa que sou eu quem estou fazendo a modificação no banco. Nesse *token,* está escrito RSA. O R significa Rivest. É o inventor da técnica de assinatura digital, utilizada no mundo inteiro e usada pelo TSE para dar garantia de integridade ao *software*.

O Rivest, em 2006, escreveu um artigo dizendo que a assinatura digital não serve para dar garantia de *software* de sistema eleitoral, e ele propôs o sistema E2E, o Sistema Scantegrity é proposta dele, em que o voto é materializado; usa-se um monte de criptografia, um sistema muito complexo de ser entendido, em que o voto é materializado. Ele diz que é necessário o voto materializado para garantir a integridade do *software* eleitoral; que, apenas com o *software* eleitoral, não se consegue garantir a integridade. Então, queria dizer que quem está propondo o sistema com o voto impresso são os mais avançados tecnólogos da informação. Estamos propondo soluções novas, Deputado.

Citamos aqui o caso do voto da Argentina, agora para...

Quanto à questão do voto na mão, é o seguinte. Realmente, a proposta que eu mostrei o sistema mexicano, em que o voto é visto, cai, e o eleitor não pega na mão é o que está proposto no art. 5º da Lei nº 12.534. Está previsto que o eleitor não pegue o voto na mão.

Mas o sistema argentino é diferente – e eu gostaria apenas de citá-lo como exemplo de como a tecnologia pode mudar conceitos. Então, eu sou favorável a que, no sistema brasileiro, se use o voto não na mão, que o voto seja depositado automaticamente. Sou favorável, sim. Mas gostaria de mostrar que o sistema argentino resolveu esse problema de uma maneira diferente. A cédula eleitoral que o eleitor recebe em branco não tem nada gravado, nem no *chip* que está aqui, nem está impresso. Ele põe na máquina e vota. Ao votar, é impresso e gravado em um *chip*. O registro digital do voto e o registro impresso do voto estão no mesmo documento. Esse daqui é entregue para o eleitor, não cai automaticamente na máquina. O eleitor pega na mão, pode ir a uma outra máquina, chegar perto e ver que o registro digital do voto é igual ao voto impresso. Ele pode conferir o conteúdo do registro digital do voto. Agora, o importante: se ele levar isso para fora, para mostrar em quem ele votou, o voto eletrônico que está aqui não será contado. Então, apesar de entregar o voto na mão do eleitor, se ele não puser na urna para ser contado no final do dia, o voto dele não será contado. Então, se ele tentar vender seu voto, o voto não conta. Então, é uma outra solução. Não estou vendendo essa solução, só estou querendo mostrar...

(*Intervenção fora do microfone.*)

**O SR. AMILCAR BRUNAZO FILHO** – Teoricamente eles são instruídos a dobrar. Você vê que já está até dobrado aqui. Eles são instruídos a dobrar o voto antes de levar para o mesário, para que o mesário não possa ver.

Enfim, estou querendo mostrar que se pode pensar em outras soluções. O artigo 5º da lei que está sendo revogada pelo projeto de lei não impõe nenhuma solução específica. Ele não impõe... Por exemplo, ali diz que pode ser usada a biometria, mas a biometria não pode ser no mesmo equipamento de votação. Ele não impõe que não haja nada que controle a urna.

Há uma foto aqui, deixe-me mostrar. Está pequena, não vai dar para ver. É uma foto do modelo da urna na Venezuela, que tem um botãozinho aqui, pequenininho, que permite ao mesário liberar ou não a urna para registrar um voto só. Então, a lei não está impondo que a máquina fique sem controle, como foi argumentado na ADI nº 4543. Existem muitas soluções que podem ser feitas. Essa questão de ter uma segunda impressora, como o TSE pensa em fazer, a lei não impõe que haja uma segunda impressora; ela deu cinco anos de prazo para o TSE mudar o sistema, para que ele pusesse o sistema com uma impressora só. Não precisava comprar segunda impressora.

Por fim, eu gostaria de destacar que a fragilidade que a equipe do Prof. Diego detectou, só ela em si, que ele mostrou que podia ordenar os votos, já foi corrigida pelo TSE. Eles corrigiram, mudaram alguma coisa. O Diego não sabe exatamente o que foi feito, mas alguma coisa eles fizeram.

O importante que eu acho que revelou esse processo que o Diego participou é que, em 2000, a Unicamp recebeu o *software* do TSE para estudar e fazer sugestões. Em 2002, foi a Sociedade Brasileira de Computação que enviou um professor de Santa Catarina, um professor da Universidade Federal de Minas; e o COPPE, da Universidade Federal do Rio de Janeiro, mandou também professores para auditar os *softwares*. Fizeram os relatórios, são todos públicos. Em 2008, foi o Ministério da Ciência e Tecnologia que foi contratado pelo TSE para fazer uma avaliação, encontrou lá uma porção de falhas e sugeriu alterações.

Apesar de ter passado por todo esse escrutínio técnico, de toda a grande equipe de técnicos e tecnólogos – no caso do Ministério da Ciência e Tecnologia, foram 11 meses que eles ficaram examinando o *software* para produzir os relatórios –, apesar disso tudo e apesar de, também, como prevê a lei atual, criada pelo Deputado Eduardo Azeredo, que os partidos políticos, Ministério Público e OAB teriam direito a examinar o *software* das urnas, apesar de todo esse escrutínio, em cinco minutos ele encontrou uma falha que ninguém tinha descoberto. Como a gente vai saber que não há outras falhas?

Então, não adianta fazer escrutínio de *software*, escrutínio de *software*, escrutínio de *software*; analisar, analisar, analisar; porque pode haver uma falha que ninguém percebeu. A equipe dele achou em cinco minutos.

Isso são os problemas de se querer confiar a segurança do sistema exclusivamente ao *software*. A minha ideia, se eu conseguisse, Deputado Azeredo, seria convencê-lo de que o voto impresso não é uma involução, mas sim uma evolução. Por isso que há a segunda e terceira gerações de máquinas de votar com o voto materializado.

Existem alternativas além do voto impresso. Existe uma proposta naquela norma norte-americana que diz que o voto pode ser gravado em CD-ROM. O voto gravado em CD-ROM não pode ser alterado, depois de gravado uma vez. Então, o eleitor poderia verificar em uma outra máquina que o voto foi gravado correto. Só que esse, sim, ficaria bem mais caro. E por fim ...

*(Intervenção fora do microfone.)*

**O SR. AMILCAR BRUNAZO FILHO** – Ah, isso é fácil de resolver. É só fazer largo o suficiente que embaralha. Não é preciso pôr um ventilador lá dentro. Nisso aí não há problema. É só ter uma filinha para cair enfileirado.

*(Intervenção fora do microfone.)*

**O SR. AMILCAR BRUNAZO FILHO** – Não, é só fazer um pouquinho mais largo o negócio. Acho que isto não é problema, ou seja, cair empilhado.

Bom, eu queria agradecer, então, a oportunidade. O Senador Zezé Perrella pediu já para encerrar. Quero agradecer esta oportunidade. Espero que eu tenha contribuído e estou à disposição quando esta discussão quiser continuar.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo/PDT - MG) – Muito bem.

Passo a palavra, então, para o Prof. Diego Aranha, para as suas considerações finais.

**O SR. DIEGO ARANHA** – Obrigado.

Bem, eu gostaria de fazer algumas considerações. Primeiro, não há nada de paranoia aqui. O que o Senador Azeredo chamou de paranoia eu chamo de análise de segurança. A área de segurança computacional se dedica exatamente a isto: a modelar um atacante que tem interesse, algum incentivo econômico em corromper alguma propriedade de segurança. No caso das eleições, é óbvio, fraudar os resultados ou o sigilo do voto. E o objetivo dessa área é encontrar mecanismos que equilibrem ou aumentem o custo do atacante o suficiente para esse custo se tornar inviável na prática, não importa quão bem financiado ele é.

Então, claramente, para o caso da eleição, os mecanismos de segurança precisam ser muito mais complexos do que para outros cenários, como, por exemplo, arquivos armazenados num disquete pessoal, ou até mesmo a transmissão de declarações de Imposto de Renda, que sofrem de um problema de falta de autenticação. Mas o incentivo para se fraudar a declaração de alguém de Imposto de Renda é incomparável ao incentivo econômico de se fraudar uma eleição inteira, em larga escala, via *software*.

Além disso, também é falacioso o argumento de que é preciso atacar várias urnas no País inteiro. Há vários pontos únicos, pontos centralizados onde um ataque tem escala absolutamente devastadora. Um exemplo, um programador malicioso dentro do TSE ou de uma das suas empresas subcontratadas. Se o TSE ou as auditorias anteriores não foram capazes de detectar as vulnerabilidades graves que nós encontramos em cinco horas de exame do código fonte, o que impede um programador mal-intencionado inserir intencionalmente uma vulnerabilidade que vai ser distribuída para todas as urnas, no País inteiro, e um mecanismo de assinatura digital, se atender as suas propriedades, vai garantir que ela de fato existe em todas as urnas.

Então, existe, primeiro, um ponto único aí centralizado para fraude em larga escala. E qualquer tentativa de recontagem, via RDV, qualquer exame do boletim de urna, qualquer tentativa posterior de auditoria vai simplesmente retornar ao resultado já fraudulento. Então, esse é um ponto único de falha.

Um outro ponto de falha que é um ponto de ataque e que é talvez não tão devastador, mas ainda assim muito importante, são esses cartões de memória cujo *software* de votação é armazenado numa partição protegida, cuja chave é compartilhada no País inteiro e armazenada às claras ... Eu tinha a analogia de se ter meio milhão de cadeados com a mesma chave e, no caso, armazenar as chaves às claras é análogo a esconder essa chave embaixo do tapete de casa. Se esse cartão interceptado e adulterado, o *software* de votação continua adulterado, com base apenas em informação contida no próprio cartão, tudo que você precisa é do próprio cartão para adulterá-lo, porque o mecanismo lá é de segurança de ofuscação, aquele cartão vai inseminar uma dezena de urnas também.

Então, interceptar alguns cartões tem um impacto, é amplificado esse tipo de ataque na simples cerimônia de carga, porque esse cartão instala várias urnas.

Então, há alguns pontos ai, tanto para agentes internos da equipe de desenvolvimento do TSE, que já demonstrou não ser capaz de detectar as próprias vulnerabilidades, creio eu acidentais e inseridas no código fonte, quanto à interceptação...

**O SR. EDUARDO AZEREDO** (PSDB - MG) - Só um momento.

**O SR. DIEGO ARANHA** – Claro!

**O SR. EDUARDO AZEREDO** (PSDB - MG) – O voto impresso não resolve isso. Isso aí continua a existir.

**O SR. DIEGO ARANHA –** Já vou chegar nesse ponto.

Eu não estou falando de totalização. Estou falando da inserção de uma vulnerabilidade...

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Está-se falando da parte dos nós. O senhor está falando dos nós. Os nós têm que continuar existindo. O voto impresso só se refere à urna, aos 400 eleitores ali.

**O SR. DIEGO ARANHA** – Eu estou falando exatamente da urna.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Depois que ele foi somado, essa soma que vai para o concentrador, isso vai continuar existindo, mesmo com o voto impresso. Então, esse tipo de risco a que ele está-se referindo continuaria existindo com o voto impresso.

**O SR. DIEGO ARANHA** - Não é verdade. E eu já vou relatar como. Eu estou falando de fraude em *software*.

**O SR. EDUARDO AZEREDO** (PSDB - MG) – Eu não estou falando mentira aqui, não. Eu estou falando também com conhecimento de fraude. Desculpe-me. Eu estou dizendo, porque eu conheço bem. A minha preocupação é a mesma, é a segurança. Eu não estou fazendo nenhuma falácia aqui, não. O que eu estou dizendo são fatos reais, tanto é que não existe nenhum outro grande partido diferente, além do PDT, que pegue essa bandeira. Não existe na opinião pública uma sensibilidade com esse assunto. Então, não venha também querer desclassificar o que estou colocando, não, porque não estou falando falácia. Estou colocando com conhecimento de causa, que realmente esse processo é um processo seguro. E da maneira que está a proposta do voto impresso, ele pode melhorar um pedacinho ali, em urnas individuais.

Agora, para você fraudar uma eleição, como um todo, você tem que ter a cooptação de várias pessoas, dezenas de pessoas, centenas de pessoas, para poder inserir, instalar o *software* fraudado nas urnas.

**O SR. DIEGO ARANHA** – Voltando ao cenário que eu descrevi, ao cenário que estou descrevendo de ataque é adulterar o *software* de votação antes de ele ser instalado nas urnas. Desta forma, o boletim de urna impresso, produzido por aquela urna, já vai conter o resultado fraudulento, somado de maneira desonesta.

Então, eu digo falacioso porque é este o termo que utilizamos na Academia quando um argumento simplesmente não procede do ponto de vista técnico. Eu estou fazendo novamente uma análise de segurança, e o argumento não procede do ponto de vista técnico.

Uma entidade...

**O SR. EDUARDO AZEREDO** (PSDB - MG. *Fora do microfone*.) – E eu disse paranoia porque é o termo também político... (*Risos*.)

**O SR. DIEGO ARANHA** – Mas não é o termo apurado do ponto de vista técnico.

De qualquer forma, uma entidade que sempre se manifesta a respeito e nunca é ouvida é a Academia. A Academia se posicionou – inclusive a Sociedade Brasileira de Computação – uma dezena de vezes em favor do voto impresso, exatamente porque o voto impresso tem a possibilidade de mitigar ou reduzir a possibilidade que um ataque desse, em larga escala, via *software,* por adulteração do *software*, antes de as eleições começarem, esse ataque se passar como indetectável no dia da eleição. Simplesmente porque a produção de outro registro vai permitir, no dia da eleição, que fique claro que a soma dos votos conferidos pelo eleitor não corresponde à soma feita pelo *software* manipulado.

Então, dessa forma, o custo de ataque aumenta substancialmente, porque exige que o atacante agora não só faça uma fraude em larga escala em *software*, como, aí sim, manipule os registros físicos espalhados País afora, depositados nas urnas convencionais, para que eles sejam compatíveis com os registros digitais produzidos pelo *software* adulterado.

Então, por isso, o voto impresso faz sentido do ponto de vista da segurança. Ele aumenta o custo do ataque e, talvez, na nossa leitura, ele aumenta o custo para ser razoável, considerando o atacante que a gente tem, o adversário que a gente tem, que é um fraudador eleitoral. Até historicamente ele tem uma série de recursos difíceis de bater.

Outra grande vantagem do voto impresso é que ele reduz a pressão sobre o desenvolvimento do *software*. A pressão não fica apenas no desenvolvimento do *software*, porque agora há um registro físico, que permite verificar se o *software* se comportou de maneira correta, o que é visível, não exige nenhum conhecimento de especialista para fazer esse tipo de verificação.

No nosso relatório, nós apontamos os problemas, as vulnerabilidades encontradas, os erros de projeto, e também oferecemos soluções tecnológicas. O problema é que todas elas são difíceis de implementar. Não são soluções simples assim.

O *software* de votação atual não é um *software* simples. Ele tem em torno de 17 milhões de linhas de código. Isso é muita coisa. Isso é absolutamente incomensurável. Então, torná-lo seguro... Só para dar um exemplo, uma equipe apontada pela Califórnia para analisar o *software* de votação nas máquinas de votar usadas nos Estados Unidos tinha um *software* 100 vezes menor, 60 dias para analisar, e a conclusão deles foi que não era possível tornar aquele *software* seguro suficiente para fazer eleições. Por mais que todos os nossos mecanismos tecnológicos sugeridos nesse relatório sejam implantados, a gente não vai ter garantia de que o *software* é seguro suficiente para executar eleições. Até porque esses mecanismos vão agregar mais complexidade. Quanto mais complexidade, mais difícil é a auditoria, mais difícil é de fato detectar vulnerabilidade, especialmente com um processo de desenvolvimento que já não atende, na nossa leitura, a requisitos mínimos de segurança e transparência, como é o que existe hoje.

Então, agradeço novamente a atenção.

Muito obrigado.

**O SR. PRESIDENTE** (Zeze Perrella. Bloco Apoio Governo. PDT - MG) – Eu agradeço a presença do Prof. Diego Aranha, do engenheiro Amilcar Brunazo Filho. Acho que foram muito importantes as explanações, porque o que nós ouvimos aqui vai nos dar realmente um maior embasamento até para entender melhor essa questão.

Eu só vou registrar aqui um *tweet* que se intitula “Leis para quem”, que diz: “A urna eletrônica, como se apresenta, é um atentado à democracia e que deveria ser uma sequência natural da evolução desta urna.”

Não havendo mais nada a tratar, agradeço aos nossos expositores.

Está encerrada a reunião.

*(Iniciada às 08 horas e 27 minutos, a reunião é encerrada às 11 horas e 01 minuto.)*