



Especialistas analisam riscos da urna eletrônica

10/09/2006

Já integra o senso comum da política brasileira a noção de que a votação eletrônica, implantada no Brasil há 10 anos, banuiu a possibilidade da fraude eleitoral — um câncer que comprometeu as eleições no país desde a instalação da República. Mas para um grupo de estudiosos do voto eletrônico, contudo, o sistema é tão infalível quanto o Papa.

Para o advogado **Paulo Gustavo Sampaio Andrade**, editor do site *Jus Navigandi*, a certeza de que a urna eletrônica é 100% segura lembra a idéia que se fazia do Titanic e das torres do World Trade Center antes do desastre. “Se o sistema eletrônico eleitoral é imune a fraudes, considerada uma suposta perfeição técnica e a natureza biológica das pessoas envolvidas” — compara ele — “o sistema financeiro já teria adotado o projeto e contratado as pessoas que criaram e utilizam o sistema eleitoral eletrônico para pôr fim aos inúmeros golpes existentes, por exemplo, nos caixas eletrônicos e nos bancos via internet”.

Essa indagação não perpassa o Tribunal Superior Eleitoral. Na semana passada, o presidente do TSE, ministro **Marco Aurélio**, reafirmou a confiança na votação eletrônica: “uma das experiências mais exitosas do país, na medida em que logramos afastar o manuseio das cédulas”, a partir das eleições municipais de 1996. “De lá para cá, não tivemos nenhuma impugnação de substância, de peso” contra a lisura das urnas, reafirmou.

Embora insista em que “as eleições no Brasil são seguras e transparentes”, com o advento da votação eletrônica, ele admite que a segurança tecnológica pode ser reforçada. O sistema, explica o tribunal, é um conjunto de ferramentas criado para garantir um processo eleitoral limpo — previsto em resolução com força de lei, para responder às questões levantadas por membros de partidos ou representantes de órgãos como a OAB e o Ministério Público.

De acordo com **Giuseppe Dutra Janino**, secretário de Tecnologia da Informação do Tribunal Superior Eleitoral, os partidos políticos, representantes da OAB e Ministério Público podem acompanhar o desenvolvimento do sistema desde a concepção dos programas até a última versão. Tudo é feito seis meses antes das eleições, para, em caso de contestação, viabilizar as correções e melhorias.

Depois, vem a assinatura digital e a lacração do sistema — fase que a Justiça Eleitoral iniciou nas duas últimas semanas. Os programas são submetidos a um algoritmo matemático. Essa “senha” verifica tudo o que está instalado na urna e gera no final um identificador, que é a assinatura digital.

O dado de cada candidato também é protegido por assinatura eletrônica. “Faz-se uma conferência quanto ao conteúdo da programação”, explica Janino. Mas não é só isso, diz o texto. “O TSE faz um ‘resumo’ de todo programa instalado. Chamamos isso de *hash*. É o controle matemático do que está inserido na urna. Depois de todos os testes, esse ‘resumo’ é colocado

na internet. O representante do partido está credenciado para acessar sempre que achar necessário. O *hash* só é feito para afastar a alegação de não integridade do produto”, esclarece.

Quando as urnas são distribuídas para os Tribunais Regionais Eleitorais seu conteúdo fica inacessível. Na véspera da eleição, é promovido um sistema de votação paralela. Os TREs sorteiam algumas sessões eleitorais, levam as urnas e reconstituem uma eleição. Tudo monitorado. No final desse processo, os técnicos verificam se o que foi digitado na urna corresponde com o total de votos impresso no comprovante.

Questionamentos

O procedimento informado pelo TSE é discutido por um grupo que defende que não há, no Brasil, um software capaz de assegurar uma eleição limpa, como anuncia o tribunal.

Paulo Gustavo Sampaio Andrade identifica dois problemas básicos no sistema. O primeiro é verificar se o voto digitado foi realmente computado para o candidato correspondente. O segundo item é a possibilidade de violação da identidade do eleitor.

“O mesário digita o número do título em um teclado conectado à urna. A urna responde se o eleitor está devidamente cadastrado. Existe a possibilidade de a informação sobre o título ser associado ao voto. Ou seja, pode-se saber quem votou em quem”, afirma.

Segundo Paulo Andrade, essa não é uma acusação infundada. “Há 10 anos discute-se a segurança do voto no Brasil. Todos os pesquisadores, brasileiros e americanos, são unânimes em dizer que o sistema não é confiável. Não dá para fingir que está tudo certo”.

O que o advogado indica como sistema ideal é o voto impresso. Isso não significa dizer que haverá manuseio de papel pelo eleitor. O voto será apenas exibido em um visor. Se o eleitor verificar que está tudo certo tecla “Confirma”. O papel é depositado em uma caixa, anexa à urna. A medida serviria para apurar possível fraude no sistema ou refazer a contagem de votos, caso fosse necessário.

“O grande problema é que hoje não há auditoria. Além disso, dois essenciais programas não são colocados à disposição do partido: o sistema operacional e o módulo de segurança, usando justificativas incabíveis. Esse método de fazer segurança por obscuridade não vale. Segurança se faz com publicidade. Tem de comprovar que os programas colocados nas urnas de todo o país foram os mesmos testados pelo pessoal do TSE. O problema é que todo mundo acha o sistema lindo. Mas ninguém tem conhecimento técnico para aferir isso.”

Para **Amilcar Brunazo Filho**, engenheiro e supervisor do Fórum do Voto Eletrônico, grupo que discute a segurança da votação digital, a indicação de que o sistema eleitoral é duvidoso é o fato de que no mundo inteiro se tem mais cautela. Estados Unidos e Venezuela também estudam esse sistema de voto, mas com a possibilidade de fazer auditoria. “Não a auditoria que o TSE admite fazer. Mas sim a contagem de voto por voto.” Para Brunazo, “o que o TSE chama de auditoria é colocar alguém em frente à urna. Isso não é o processo de exame de um sistema, mas sim um artifício. Um show”.

Para justificar seu argumento, Brunazo cita o caso da empresa Microbase. Fornecedora do VirtuOS — sistema operacional que equipa parte das urnas eletrônicas — a empresa divulgou nota de esclarecimento dizendo que seu software nunca foi auditado.

“A legislação em vigor exige a auditoria de todos os programas-fonte do Sistema de Eleições Eletrônicas, mas a regra nunca foi adequada e rigorosamente obedecida pelo TSE, de modo a dar a necessária e devida credibilidade ao processo de Assinatura Digital e de Lacração dos Sistemas para as Eleições Oficiais”, diz a direção da empresa na nota.

A Microbase ainda afirma que “denúncias de fraudes eleitorais estão sendo comprovadas de modo irrefutável. Denúncias que, de algum modo, podem vir a nos envolver como fornecedores de uma peça importante do ‘software’ utilizado nas Urnas Eletrônicas”.

Também sustenta que há “descompromisso do TSE na condução de certos aspectos importantes que envolvem as Eleições Eletrônicas”, o que resultou, “inclusive, em nossa denúncia à lide, numa ação judicial milionária de ressarcimento pela eventual apropriação indébita de ‘propriedade intelectual’ do Sistema de Votação Eletrônica”.

Outras vozes

Hélio Freitas, advogado do PT, especialista em Direito Eleitoral, aposta na segurança do voto eletrônico. Ele conta que no ano de 2000, advogados dos partidos pediram para o Tribunal Regional Eleitoral paulista selecionar algumas urnas para a simulação de votos. A solicitação foi aceita. Feita a contagem dos votos, não se teria constatado qualquer irregularidade.

“O sistema foi bem desenvolvido. O Brasil é pioneiro nessa questão. Só existiu fraude no sistema passado. Minha única ponderação é sobre o sistema de envio de votos dos TREs para o TSE. Isso se dá por mais deficiência minha do que do sistema. Advogados de partidos não fazem qualquer reserva ou questionamento sobre o processo. Todos elogiam muito”.

Para **Alberto Rollo**, presidente do Instituto de Direito Político Eleitoral e Administrativo, não dá para dizer que o sistema é 100% seguro, como também não se pode levantar a questão de possibilidade de fraude sem apontá-la objetivamente. Rollo diz que poderia haver duas possibilidades de o sistema apresentar falhas: a primeira na computação dos votos. A segunda seria a instalação de um vírus. Mas não enxerga motivos para crer que haja brechas para isso.

“No final das eleições, o representante partidário recebe um documento oficial do TSE com o número de votos. Se houver divergência com o resultado divulgado, ele pode confrontar a informação. No caso do vírus é ainda mais difícil. Sete programas são instalados na urna eletrônica. Se for instalado um vírus teremos então oito programas. A fiscalização vai constatar a fraude. A eleição estará nula. É simples.”

O que Alberto Rollo defende como medida eficaz é a fiscalização de pelo menos 1% nas urnas eletrônicas. Hoje, na cidade de São Paulo, por exemplo, só duas urnas são levadas para a votação paralela. “Isso não comprova nada. Se há dúvida, o melhor é que se faça o teste em uma pequena porcentagem. Isso já acabaria com várias alegações de fraude”, acredita.

Questões pendentes

Na linha dos especialistas que se dedicam a desmistificar a idéia de que o sistema eletrônico eleitoral é, por natureza, imune a fraudes há ponderações que não se pode ignorar.

Afinal, crer que no país do Mensalão, dos Anões do Orçamento e da delinquência habilidosa que enlouquece os técnicos encarregados de conter invasão de sites, clonagem de telefones e cartões de crédito, haja um sistema milagroso à prova de falhas ou truques, seria ingenuidade.

Paulo Andrade raciocina: “o sistema eletrônico não tem o condão de tornar *bonzinhos* os fraudadores”. A trilha natural de quem sabe o valor de uma vitória eleitoral, diz o advogado, é aperfeiçoar-se para explorar os espaços existentes. Espaços que, acusa, o TSE não se esforça para bloquear.

A crença generalizada da infalibilidade da “eleição eletrônica”, diz Andrade, desmobilizou os partidos políticos (e os fiscais por eles designados) que se acomodaram e diminuíram o rigor da fiscalização — situação calcificada pela falta de investimento em técnicos e técnicas de precaução para eventuais desvios.

O livro [Fraudes e defesas no voto eletrônico](#), de Amílcar Brunazo Filho e Maria Aparecida Cortiz (All Print, São Paulo, 2006) elenca 12 maneiras pelas quais pode ser fraudada a eleição eletrônica (do cadastro eleitoral à totalização).

Paulo Andrade selecionou cinco hipóteses de fraudes:

A — Possibilidade de fraudes na votação

Votação é a colheita dos votos individuais de cada eleitor. Nas urnas eletrônicas brasileiras, os votos individuais somente existem virtualmente. Não existe nenhum documento impresso que materialize a existência de um voto individualmente considerado.

Fraude nº 1 Possibilidade de clonagem de urnas eletrônicas:

1.1. Como ocorre esta fraude: consiste em trocar as urnas eletrônicas verdadeiras, registradas pelo TSE, por urnas eletrônicas “clonadas”, também verdadeiras mas não registradas pelo TSE. Enquanto os eleitores votam na urna “clonada”, a urna verdadeira é alimentada por votos fraudulentos em outro lugar. Depois da votação, o presidente da seção deve emitir o boletim de urna e conduzir todo o material no local da totalização dos votos em seu próprio carro. No caminho, porém, ele a trocará pela urna verdadeira, com os votos e o boletim de urna fraudulentos. Há outras variações, em que a votação fraudulenta pode ser feita em outro horário.

1.2. Quem pode fazer esta fraude: exige participação do presidente da seção + algum agente interno da Justiça Eleitoral (ou empresa terceirizada) que forneça a urna “clonada”.

1.3. Como evitar esta fraude: os fiscais devem exigir uma via do boletim de urna, no momento em que este for impresso pela urna eletrônica, ainda dentro da seção eleitoral, para compará-la com a outra via do boletim de urna que será entregue pelo presidente da seção à Justiça



Eleitoral, para totalização. Problemas: 1 — este cuidado é constantemente omitido pelos partidos e pelos fiscais, confiantes de que o sistema é 100% seguro; 2 — neste ano, o TSE baixou a Resolução nº 22.154/2006, que desobriga os mesários de fornecer uma via do boletim de urna aos fiscais dos partidos.

1.4. Exemplo desta fraude: [Guarulhos, 2004](#).

Fraude nº 2 — ***Possibilidade de engravidamento de urnas eletrônicas:***

2.1. Como ocorre esta fraude: num momento em que a seção eleitoral estiver com pouco movimento, no final da tarde, os mesários, em conluio e na ausência de fiscais, podem votar no lugar de eleitores que ainda não compareceram. Para tanto, basta digitar o número do título de um eleitor que ainda não compareceu, que consta dos cadernos em que os eleitores assinam sua presença. Se, por acaso, algum eleitor cujo título tenha sido digitado fraudulentamente aparecer nos últimos instantes da votação, basta escolher outro número de título de eleitor que não tenha comparecido e digitá-lo para liberar a votação do que compareceu.

2.2. Quem pode cometer essa fraude: os mesários em conluio (até mesmo algum fiscal pode ajudar na fraude); a fraude se torna mais fácil se for na eleição proporcional (para deputado ou vereador), pois cada um dos presentes vota no seu candidato.

2.3. Quem pode evitar esta fraude: os fiscais. Problema: 1 — os partidos confiam na “urna 100% segura” e enviam apenas um representante para várias seções, quando enviam; 2 — os fiscais, também crédulos, se ausentam das seções por várias horas.

2.4. Exemplo desta fraude: [Marília, 2004](#).

B — Possibilidade de fraude na apuração:

Apuração é a soma dos votos de uma única urna.

Nas urnas eletrônicas brasileiras, a apuração é feita dentro da própria urna eletrônica, pela soma dos votos em sua memória.

O único documento da apuração é o boletim de urna, impresso pela urna ao final da votação, que nem sempre é entregue aos fiscais.

Fraude nº 3 — ***Possibilidade de fraude no programa original da urna***

3.1. Como ocorre esta fraude: os programas originais das urnas eletrônicas, gerados pela Justiça Eleitoral e distribuídos para todo o Brasil podem já — em tese — conter arquivos que determinem o desvio de votos, de forma genérica para todas as votações.

Trata-se de uma fraude de largo alcance, que pode eleger um candidato a qualquer cargo. Uma fraude já existente no software original da urna pode desviar votos para um partido político de forma genérica (votos para legenda em candidatos a deputado) ou então atuar de forma específica (por exemplo, quando a foto do candidato contiver um determinado texto oculto que

funcione como senha).

3.2. Quem pode fazer esta fraude: programadores desonestos que trabalhem ou prestem serviços à Justiça Eleitoral, com acesso privilegiado ao código-fonte dos programas. Também poderia ser inoculada, sem conhecimento do TSE, por atacantes externos que consigam invadir os computadores da Justiça Eleitoral (utilizando vírus, cavalos-de-troia etc.).

Fraude nº 4 — *Possibilidade de adulteração dos programas originais das urnas eletrônicas:*

4.1. *Como pode ocorrer esta fraude:* os programas originais de uma certa quantidade de urnas podem ser fraudados de forma que desviem os votos, atingindo uma quantidade determinada de seções eleitorais. A fraude seria feita pela introdução de um programa que desvie votos, por vários métodos: regravação da BIOS com programa fraudado, inicialização por memória externa ou disquete fraudados etc.

4.2. Quem pode fazer esta fraude: qualquer pessoa de dentro da Justiça Eleitoral ou de uma empresa que lhe preste serviços, que tenha acesso a um grupo de urnas eletrônicas (as quais, aliás, passam vários anos armazenadas em depósitos em vários lugares do Brasil), mediante conhecimentos médios de informática e disponibilidade de algum tempo para conhecer o sistema.

As observações a seguir valem para ambos os casos acima (3 e 4):

3+4.3. *Como ocultar estas fraudes:* o próprio programa fraudulento pode ocultar pistas, mediante fraude na verificação da integridade dos programas da urna e apagamento dos arquivos de registro de utilização da urna (logs). Eventuais lacres físicos rompidos podem ser facilmente substituídos, pois existe grande quantidade disponível. *Fraudar é bem mais fácil que descobrir a fraude.*

3+4.4. *Facilitadores dessa possibilidade de fraude:* as urnas brasileiras não permitem auditoria da contagem de votos (recontagem). Desta forma, as urnas dependem unicamente da confiabilidade de seus programas de computador. Problemas: 1 — os programas das urnas eletrônicas jamais foram exibidos de forma integral para os partidos políticos; 2 — a parte do sistema das urnas que é exibida é composta de mais de 50 mil programas, que deverão ser analisados em tempo exíguo, utilizando os computadores do próprio fiscalizado (Justiça Eleitoral), que podem ser viciados; 3 — seria necessário garantir que os programas fiscalizados são os mesmos que serão instalados em mais de 400 mil urnas espalhadas por todo o Brasil — e isso não ocorre na prática, por três motivos: a) carência de fiscais, b) falta de treinamento dos fiscais, c) a verificação da assinatura digital é feita pela própria urna que é fiscalizada, que pode ser viciada.

3+ 4.5. *Como evitar essas possibilidades de fraudes:*

a — Auditoria dos programas originais das urnas eletrônicas: para conferir se o programa gerado pelo TSE não contém vícios. Todos os programas da urna devem ser públicos, para que seja possível aos fiscais verificar se não contém algum comando desonesto.



Problemas: 1 — são mais de 50 mil programas para serem analisados em um prazo exíguo; 2 — o TSE **jamais** permitiu acesso a todos os programas das urnas eletrônicas, ou seja, **jamais** houve uma verdadeira auditoria independente das urnas eletrônicas;

b — *Conferência da autenticidade dos programas de cada uma das urnas eletrônicas*: para verificar se o programa do TSE, que foi auditado no item anterior, é idêntico ao que é instalado em cada uma das urnas eletrônicas.

Problemas: 1 — Se a providência anterior (a — auditoria dos programas originais das urnas eletrônicas) não for realizada adequadamente, de nada adiantará conferir se as cópias são idênticas ao original, pois a fraude pode estar embutida no programa original (caso da fraude nº 3), 2 — na prática (por incrível que pareça), os programas continuam sendo modificados pelo TSE depois da auditoria, tornando-a inócua; 3 — a assinatura eletrônica não é adequada para demonstrar que o programa não foi alterado (conforme conclusão de [Ronald Rivest](#), criador da assinatura eletrônica); 4 — é humana e tecnicamente impossível aos fiscais conferir a carga de quase 400 mil urnas em todo o Brasil (falta pessoal e treinamento).

c — *Mecanismo de impressão paralela do voto*: para suprir eventuais falhas das medidas acima (a e b), o Fórum do Voto Eletrônico (secundado por diversos estudos internacionais específicos sobre votação eletrônica) propõe que o voto seja impresso pela própria urna e conferido visualmente pelo eleitor; após confirmação, seria depositado — sem contato físico — em uma urna de saco plástico. Problema: tal medida chegou a ser transformada em lei em 2002, mas nunca chegou a ser implantada oficialmente porque o TSE conseguiu usar de seu poderoso “lobby” para revogá-la no ano seguinte, antes de entrar em vigor em 2004 (foi feito apenas um teste nas eleições de 2002, que foi convenientemente “sabotado” pelo TSE para gerar a idéia de que não deu certo).

3+ 4.6. *Exemplo destas fraudes*: um teste simulado feito clandestinamente no Paraguai, com urnas brasileiras cedidas pelo TSE ([gravado em vídeo](#)), demonstra como é possível adulterar os programas oficiais da Justiça Eleitoral brasileira para que, digitando o número de um determinado candidato, o voto seja gravado (=apurado) pela urna em nome de outro candidato.

Contudo... no Brasil, o TSE vem sistematicamente se recusando a fazer um [teste de penetração](#), segundo normas internacionais, para verificar a possível existência de fraudes no programa das urnas (neste ano, uma petição de abril nunca foi julgada pelo TSE, e provavelmente terá o mesmo destino dos anos anteriores: só será “vista” depois da eleição e perderá o objeto).

C — Possibilidade de fraudes na totalização

Totalização é a soma das apurações de cada uma das urnas, feita nos computadores de grande porte, na sede dos Tribunais Regionais Eleitorais. (*Não confundir apuração com a totalização. Apuração é a soma dos votos de uma urna eletrônica, que é calculada pela própria urna e materializada no boletim de urna e gravada em disquete.*)

Fraude nº 5 — *Possibilidade de adulteração nos programas de totalização*



5.1. *Como ocorre esta fraude*: o próprio programa (original ou fraudado) de totalização da Justiça Eleitoral pode alterar as somas das apurações, desviando votos para determinados candidatos; ou o banco de dados em que são armazenados os votos de todas as seções pode ser diretamente alterado.

5.2. *Quem pode fazer esta fraude*: servidores da Justiça Eleitoral, empregados de empresas terceirizadas ou terceiros invasores (por acesso direto ou utilizando vírus ou cavalos-de-tróia), por intermédio da rede do TSE. As urnas eletrônicas (que fazem a apuração) não estão em rede, mas os computadores da totalização são acessíveis em rede, potencializando o risco de ataques.

5.3. *Como evitar esta fraude*: os fiscais. É possível detectar uma fraude na totalização pela simples comparação com as somas dos comprovantes impressos das apurações de cada urna (boletins de urna) — a chamada “totalização paralela”.

Problemas: 1 — Existem restrições à colheita dos boletins de urna nas próprias seções eleitorais, no momento em que são geradas (ver item 1.3), 2 — os partidos políticos, crédulos na impossibilidade de fraudes, se descuidam em exigir os boletins de urna em cada seção para uma totalização paralela, 3 — a imprensa, como já obtém os resultados oficiais com facilidade nos telões dos TREs, não se interessa mais em manter dispendiosos esquemas de totalização paralela.

5.4. *Exemplos dessa possibilidade de fraude*: [Rio de Janeiro, 2002](#) — alguns candidatos a deputado acordaram com menos votos do que tinham quando foram dormir na noite anterior — *Jornal do Brasil*, 11/06/2006;

[Brasil, 2002](#) — em certo momento da totalização do primeiro turno da última eleição presidencial, o candidato Lula surgiu no telão do TRE/RJ com 41 mil votos negativos. Como os programas de totalização somente SOMAM votos, é no mínimo estranho que um candidato possa ter votos negativos, a não ser que exista algum comando no programa destinado a subtrair votos de um candidato. A Justiça Eleitoral nega o fato, testemunhado por todos os jornalistas então presentes. Não custa lembrar que Lula não ganhou a eleição de 2002 no primeiro turno por uma pequena margem de votos.

Fonte: https://conjur.jumps.com.br/2006-set-10/especialistas_analisam_riscos_urna_eletronica/