Eu sei em quem votei,
Eles também,
Mas só eles sabem quem recebeu meu voto.

FRAUDES e DEFESAS
no Voto Eletrônico

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Brunazo Filho, Amílcar
Fraudes e defesas no voto eletrônico / Amílcar Brunazo Filho e Maria Aparecida Cortiz. – São Paulo: All Print Editora, 2006.

Bibliografia

ISBN 85-7718-030-1

1. Defesa (Processo civil) - Brasil 2. Fraude eleitoral - Brasil 3. Justiça eleitoral - Brasil 4. Voto eletrônico - Brasil I. Cortiz, Maria Aparecida. II. Título.

06-5379 CDD-324.660981

Índices para catálogo sistemático:
1. Brasil : Fraudes no voto eletrônico : Eleições : Ciência política 324.660981
2. Brasil : Voto eletrônico : Fraudes : Eleições : Ciência política 324.660981

Amílcar Brunazo Filho • Maria Aparecida Cortiz

FRAUDES e DEFESAS

no Voto Eletrônico

ALL PRINT EDITORA
2006
SÃO PAULO – BRASIL

FRAUDES E DEFESAS NO VOTO ELETRÔNICO

Projeto gráfico, editoração e impressão:

ALL PRINT EDITORA
www.allprinteditora.com.br
info@allprinteditora.com.br
(11) 5574-5322

Capa:
Idéia original: Fernando Barboza
Ilustração e design: Fernando Augusto Alves

Vendas em:
www.votoseguro.org/livros

Contato com autores:
amilcar@brunazo.eng.br
maria.cortiz@uol.com.br

Em Memória

Dedica-se este livro à memória do **Engenheiro Leonel de Moura Brizola**.

Desde sua experiência constrangedora com o Caso Proconsult, nas eleições de 1982, Brizola lutava pelo aperfeiçoamento, por mais confiabilidade e por mais transparência do sistema eletrônico de votação e foi com seu apoio que os autores puderam desenvolver o conhecimento do sistema brasileiro e, em nome do seu partido PDT, propor inúmeras correções que hoje estão incorporadas ao sistema.

Pela sua compreensão clara das vantagens e das limitações da nova tecnologia de informática, Brizola tornou o PDT o único partido político brasileiro tecnicamente habilitado a verificar a integridade dos programas de computador que foram utilizados na Totalização dos Votos das Capitais em 2004.

Muitos aperfeiçoamentos ainda precisam ser trazidos ao sistema eleitoral brasileiro e, para honrar o espírito lutador e incansável de Brizola, os autores continuarão propugnando as melhorias que um sistema eleitoral confiável exige.

Sentimos o passamento de um político digno e coerente e muito nos honrou desfrutar de seu descortino.

Sumário

Agradecimentos

Os autores agradecem aos jornalistas, juristas e professores universitários que têm colaborado de forma inestimável ao longo destes anos em que, como um verdadeiro Exército de Brancaleone, temos enfrentado até a difamação nascida da incompreensão e a má disposição de alguns membros da Justiça Eleitoral.

Nosso obrigado a:

Professores Universitários: Prof. Dr. Walter Del Picchia – EPUSP, Prof. Dr. Jorge Stolfi – UNICAMP, Prof. Dr. Michael Stanton – UFF, Prof. Pedro Dourado Rezende – UNB, Prof. Dr. Clóvis Torres Fernandes – ITA.

Juristas: Celso Antônio Bandeira de Mello, Sérgio Ferraz, Sérgio Sérvulo da Cunha, Américo Lourenço Masset Lacombe.

Jornalistas: Paulo Henrique Amorim – SP, Osvaldo Maneschy – RJ, Marcelo Soares – RS.

Políticos (que ousaram enfrentar a inércia e até ameaças da Justiça Eleitoral): Leonel Brizola – PDT-RJ, Roberto Requião – PMDB-PR, Romeu Tuma – PFL-SP, Sergio Miranda – PDT-MG, Jovino Candido – PV-SP, Mariângela Duarte – PT-SP, Gilson Meneses – PL-SP, Washington Neves – PFL-BA, Edivaldo Freitas da Silva – PPB-BA, Chico Leitoa – PDT-MA.

Também agradecem a todos os colegas, novos e antigos, do Fórum do Voto Eletrônico, que vêm colaborando com informações, debate de idéias, divulgação e apoio desde 1996.

Colegas antigos do Voto-E: Roger Chadel, Márcio Coelho Teixeira, Paulo Mora de Freitas, Paulo Castelani, Benjamin Azevedo, Evandro Luiz de Oliveira, Luiz Ezildo Silva, Paulo Gustavo Sampaio Andrade, Rejane Luthemaier, Leamartine Pinheiro de Sousa, Cláudio Rego e muitos outros...

Prefácio de Paulo Henrique Amorim

Não confie no computador! Ele também mente!

Em 1982, na primeira eleição direta para governador depois do regime militar, Leonel Brizola, ao voltar do exílio, se candidatou a governador do Rio. O SNI, que hoje se chama ABIN; uma parte importante da Justiça Eleitoral, que contratou uma empresa de computação chamada Proconsult; uma parte da Polícia Federal; e as Organizações Globo, através da televisão, do jornal e da rádio – todas essas instituições, através de um instrumento chamado "diferencial delta", que consistia em pegar no computador votos para o Brizola, especialmente na Baixada Fluminense e na zona oeste do Rio, e convertê-los em votos brancos e nulos, se organizaram para fraudar a eleição. A tinha como objetivo impedir a eleição de Brizola e eleger o candidato dos militares, o então deputado federal Moreira Franco. A operação levaria a um impasse entre a apuração dessa empresa, a Proconsult, e apurações alternativas, como a apuração feita pela Rádio Jornal do Brasil, que o Jornal do Brasil usava.

Foi essa a primeira vez em que se usou o computador numa eleição brasileira – aí, no caso, para totalizar os votos contados manualmente.

O objetivo da fraude era criar um impasse que ser arbitrado pela Justiça Eleitoral. E a Justiça Eleitoral daria a vitória ao candidato dos militares. Isso não é uma especulação irresponsável. Sabemos o que aconteceu em 2000, nos Estados Unidos, quando houve um impasse entre vários tipos de apuração, e uma emissora de televisão, a FOX, saiu na frente, e disse que George Bush ganhara a eleição no estado da Florida. As outras emissoras foram atrás e disseram que o Bush ganhou a eleição. Criou-se o fato consumado. Depois de instâncias e instâncias de decisão judicial, a Suprema Corte decidiu, com juízes da maioria republicana, dar a vitória ao candidato George Bush.

Recontagens muito posteriores demonstraram que Bush não ganhou na Florida.

Aqui, o papel da TV Globo era o mesmo da Fox: produzir um "já ganhou" e preparar a opinião pública para a vitória do candidato dos militares.

Desde a eleição de 1982, Leonel Brizola defendeu a tese do "cadê o papelzinho?". Cadê o papelzinho ? O que Brizola queria dizer naquela linguagem rústica de engenheiro formado em Porto Alegre, mas que usava uma linguagem de agricultor do interior do Rio Grande do Sul – ele preservava isso provavelmente por motivos políticos –, Brizola dizia que, sem o papelzinho, a eleição não pode ser recontada. Muito se disse que o Brizola era jurássico, era pré-paleocênico.

Não é verdade.

Não há nenhuma possibilidade de se conferir uma eleição no computador, se não houver o papelzinho; se não houver a contraprova física do voto que o eleitor deu.

Sobre a eleição para governador do Rio, em 1982, recomendo o livro que escrevi com Maria Helena Passos, pela editora Conrad: *"Plim-Plim – A Peleja de Brizola contra a Fraude Eleitoral"*.

Sobre como fraudar eleições no Brasil - e evitar que isso aconteça - recomendo este livro de Amílcar e Maria Aparecida, mestres na matéria e incansáveis batalhadores pela verdade do voto, no Brasil.

Porque, não se esqueça do *"papelzinho"*. Ou, como disse o professor Jorge Stolfi, ilustre catedrático de Ciência da Computação da Universidade de Campinas, num recente seminário na OAB de São Paulo: *"Hoje, quando você vota no computador no Brasil, tudo o que você faz é entregar o seu voto ao arbítrio do programador do software daquela apuração"*.

Paulo Henrique Amorim

Prefácio de Sérgio Sérvulo da Cunha

Este livro é de fazer cair o queixo.

Ele é imprescindível para juízes, dirigentes partidários, advogados e fiscais eleitorais. O teor das suas denúncias, porém, deve ser conhecido por todos os eleitores, por todos que se aproximam de uma urna eletrônica convencidos de que estão participando de um processo honesto.

No fundo, ele suscita uma questão que não é exclusiva do Direito Eleitoral: como podem ser utilizadas seguramente, pelo poder público, técnicas sofisticadas, pertinentes a domínios de conhecimento restrito?

Amílcar Brunazo Filho e Maria Aparecida Cortiz demonstram que o modelo de urna eletrônica utilizado no Brasil é vulnerável a fraudes e que tem sofrido fraudes; essas fraudes poderiam ser prevenidas e evitadas em grande parte mediante uma disciplina e uma prática mais responsável, principalmente por parte da Justiça Eleitoral.

Perante essas evidências, não mais se justifica a omissão dos partidos políticos, o silêncio de entidades como a Ordem dos Advogados do Brasil, e, sobretudo, do Tribunal Superior Eleitoral.

Passados três anos, não se deu qualquer resposta ao manifesto assinado por especialistas, juristas e intelectuais, e que se acha reproduzido nas páginas finais. O povo brasileiro merece, ao menos, uma explicação.

Santos, junho de 2006

Sérgio Sérvulo da Cunha

1. Introdução

"É até irônico que estas máquinas de votar, que supostamente deveriam resolver os problemas causados pelos sistemas eleitorais antiquados, estão simplesmente ***tornando os problemas invisíveis para o eleitor****."*

– Penny M. Venetis
Professora de Direito na Rutgers University, NJ, USA

1.1 Termo de Manutenção de Sigilo

Os autores deste livro atuam como representantes de alguns Partidos Políticos junto à Justiça Eleitoral brasileira, onde ganharam acesso a informações técnicas sobre o projeto do sistema eleitoral informatizado brasileiro.

Para tanto, tiveram que assinar um **Termo de Compromisso de Manutenção de Sigilo**[1] perante o Tribunal Superior Eleitoral, TSE, de maneira que não podem divulgar informações que obtiveram dentro daquele órgão oficial.

Desta forma, as informações sobre o sistema eleitoral brasileiro aqui apresentadas são apenas aquelas que podem ser obtidas em documentos e em procedimentos públicos como:

1. Resoluções e Instruções do TSE;
2. Descritivos técnicos incluídos nos editais de concorrência para o fornecimento de urnas eletrônicas;
3. Relatórios técnicos oficiais apresentados por entidades acadêmicas (UNICAMP, SBC e COPPE-UFRJ) [2];

1. O modelo do Termo de Sigilo pode ser visto em anexo do Relatório SBC em: *http://www.votoseguro.org/textos/relatoriosbc1.htm*
2. Estes relatórios técnicos oficiais podem ser encontrados a partir de: *http://www.votoseguro.org/textos/relatindex.htm*

4. Artigos técnicos de terceiros apresentados em Congressos de Informática e na Internet;
5. Atos públicos nas Juntas Eleitorais como as Cerimônias: de Geração de Mídias, de Carga e Lacração de Urnas-E, de Recuperação de Dados e de Oficialização da Totalização;
6. Laudos de Perícias em processos na Justiça Eleitoral.

1.2 Objetivos e Metodologia

Eleitores brasileiros são obrigados a declarar seus votos em máquinas nas quais terão que confiar nos resultados sem saber direito como elas garantem a lisura do pleito.

Por isto, destina-se este livro aos eleitores em geral e aos fiscais e delegados de Partidos Políticos, interessados em conhecer melhor os riscos do sistema eleitoral informatizado brasileiro.

Descrevem-se as formas pelas quais as falhas de segurança do Sistema Eletrônico de Eleições podem ser exploradas para produzir fraudes na votação e na apuração dos votos e quais os atos de fiscalização necessários para se procurar evitar estas possíveis fraudes.

Também se faz uma análise das características socioculturais que levaram a uma situação peculiar no Brasil, onde a grande maioria dos eleitores aceita e até se orgulha de votar num sistema eleitoral que está sendo rejeitado no resto do mundo desenvolvido por causa de suas falhas de segurança.

Considere-se que existem dois tipos básicos de máquinas eletrônicas de votar ou de urnas eletrônicas:

a. **Máquinas de Voto Real** (Urna-E Real) que emitem o voto impresso para ser conferido pelo eleitor, permitindo assim a recontagem dos votos e a auditoria da apuração eletrônica, como aquelas que são usadas nas eleições da Venezuela[3] e em mais da metade dos Estados nos EUA[4];

---

3. Ver mais em: *http://www.votoseguro.org/textos/venezuela1.htm*
4. Ver a relação atual dos Estados nos EUA que já exigem o voto impresso em Urnas-E em: *http://www.verifiedvoting.org/*

b. **Máquinas de Voto Virtual** (Urna-E Virtual) que não emitem comprovantes materializados do voto para ser conferido pelo eleitor, impossibilitando auditoria do seu resultado, como as usadas no Brasil e no Paraguai.

Desde a adoção das Urnas-E Virtuais no Brasil em 1996, a propaganda oficial insistentemente repete que o "*sistema é 100% seguro*" e que "*fraudes eleitorais acabaram*", influenciando a maioria do eleitorado brasileiro que manifesta aceitação e confiança na tecnologia aqui escolhida.

Porém, esta confiança parece cega e arriscada para uma minoria de eleitores que fundaram um **fórum de debates**[5] na Internet e outros que têm apoiado um **manifesto**[6] apresentado por Professores Titulares de importantes universidades.

São apenas um pouco mais de dois milhares de eleitores, entre eles especialistas em informática, advogados e juristas renomados, professores universitários, engenheiros, jornalistas, estudantes, preocupados em entender como se daria a segurança do seu voto informatizado.

Surge, então, a questão: Como os brasileiros aceitaram a novidade eletrônica, sem se dar conta que estão votando num sistema que não lhes permite conferir a apuração?

Para respondê-la, no Capítulo 2 se analisa **a ordenação jurídica e as peculiaridades sócio-culturais** que favoreceram o surgimento desta situação atual, na qual tantos eleitores confiam num sistema eleitoral cujas características de segurança não conhecem e nem entendem de fato.

A compreensão destes fatores sócio-culturais que afetam diretamente nossa ordenação institucional eleitoral é importante para os fiscais e delegados de Partidos Políticos, pois é neste meio cultural que terão que encontrar as soluções para os problemas que enfrentarão.

Já os fiscais, os delegados e os leitores interessados apenas em conhecer a **parte prática das fraudes e das defesas contra elas** pode seguir direto ao Capítulo 3 onde se descreve de que forma as falhas

5. Fórum do Voto-E: *http://www.votoseguro.org*
6. Alerta dos Professores: *http://www.votoseguro.com/alertaprofessores*

de segurança do sistema eletrônico de eleição podem ser exploradas em fraudes e se ensina até onde podemos nos defender.

Esta descrição das fraudes possíveis, propositadamente não será minuciosa para não dar orientações a quem apenas esteja interessado em "*aprender como fraudar*" as eleições eletrônicas, mas será clara o suficiente para não deixar dúvidas sobre a existência de riscos graves.

Ao final, nos Adendos, são postas informações complementares que podem interessar a alguns de nossos leitores.

1.3 Definição de Alguns Termos

Para esclarecer algumas confusões freqüentes relacionadas ao processo eleitoral eletrônico, apresenta-se a definição de alguns termos:

Apuração: É a contagem dos votos dados em uma urna eletrônica. É processada na Seção Eleitoral pela própria urna eletrônica logo ao final da votação às 17 h. O resultado da apuração é registrado no Boletim de Urna.

Boletim de Urna – BU: Documento que contém a relação dos votos que cada candidato obteve numa urna eletrônica. Pode estar gravado em arquivos digitais, para ser transmitido em disquetes para os computadores de totalização, ou pode ser impresso para permitir a auditoria da totalização. Antigamente era chamado de Mapa de Urna.

Totalização: É a soma dos Boletins de Urna. É processada nos computadores dos Cartórios Eleitorais e dos Tribunais e fornecem o resultado geral da eleição. Não confundir com a Apuração.

Seção Eleitoral: É o local onde o eleitor se apresenta para votar. Contém uma e somente uma urna eletrônica administrada pelos mesários. É aqui que é feita a Apuração dos Votos e é emitido cada Boletim de Urna, na forma impressa e gravado ainda em disquete.

Zona Eleitoral: É o agrupamento em torno de 200 seções eleitorais de uma mesma região contígua. Sempre é presidida por um Juiz Eleitoral. Pode haver mais de uma Zona Eleitoral na mesma cidade.

Cartório Eleitoral: É a sede física de uma Zona Eleitoral onde é feito o cadastramento de eleitores e a administração local do

processo eleitoral. É aqui que são recepcionados os Boletins de Urnas em disquetes para serem remetidos à Totalização.

Junta Eleitoral: É um grupo de cidadãos, nomeados pelo Juiz Eleitoral de cada Zona Eleitoral, encarregados de acompanhar e supervisionar os trabalhos eleitorais. A centralização e a especialização da administração das eleições, propiciada pelo voto eletrônico, tem esvaziado as funções da Junta Eleitoral.

Tribunal Regional Eleitoral – TRE: Segunda Instância da Justiça Eleitoral. Existe um em cada Estado e congregam todos os Cartórios Eleitorais do Estado.

Tribunal Superior Eleitoral – TSE: Instância judicante máxima da Justiça Eleitoral, sediado em Brasília, também é o órgão que, apesar de nomeado tribunal, é o responsável pela execução e administração do processo eleitoral.

Carga de Urnas: É a gravação dos programas de computador oficiais e dos dados da eleição (eleitores e candidatos) nas memórias internas das urnas eletrônicas. Deve sempre ser feita em cerimônia pública obrigatória onde, ainda, é feito um teste de funcionamento em uma urna depois de carregada.

Teste de Penetração: É a denominação técnica para testes de resistência contra ataques intencionais em sistemas informatizados complexos, onde se permite que pessoas capazes possam tentar burlar as defesas de segurança do sistema. A finalidade do teste é descobrir falhas de segurança ignoradas pelos projetistas. Existem normas técnicas internacionais e brasileiras que estabelecem os Critérios Básicos de Avaliação da Segurança em Sistemas Informatizados, como a ISO 15.408, que sugerem o uso de testes de penetração como ferramenta importante na determinação da confiabilidade dos sistemas.

Voto Impresso Conferido Pelo Eleitor: É uma forma de materialização do voto que diferencia as Urnas-E Reais das Urnas-E Virtuais (brasileiras). Urnas-E Reais permitem que se possa proceder a uma auditoria da apuração pela recontagem dos votos impressos. Os votos impressos podem ser automaticamente depositados em urnas comuns acopladas às urnas eletrônicas ou

podem ser entregues ao eleitor para que este pessoalmente o deposite em urnas comuns na presença dos mesários.

Zerésima: É uma lista impressa com os nomes dos candidatos oficiais ladeados pelo número zero, que é emitida pelas urnas eletrônicas imediatamente antes do inicio da votação. Equivocadamente tem sido entendida como garantia de lisura na apuração.

1.4 Pontos de Ataque – Visão Geral

Quando se conversa sobre fraudes eleitorais é comum as pessoas limitarem o debate a apenas uma ou duas formas de fraude que conhecem e dominam a *"tecnologia"*.

Mas os tipos de fraudes possíveis são inúmeros e ajudará na compreensão deste livro se tivermos uma visão ampla de todo o processo eleitoral, identificando todos os pontos do processo que são passíveis de virem a ser atacados por pessoas mal intencionadas.

A figura a seguir mostra as etapas do processo eleitoral e dos respectivos pontos de controle e fiscalização em eleição com Urnas-E Reais e com Urnas-E Virtuais.

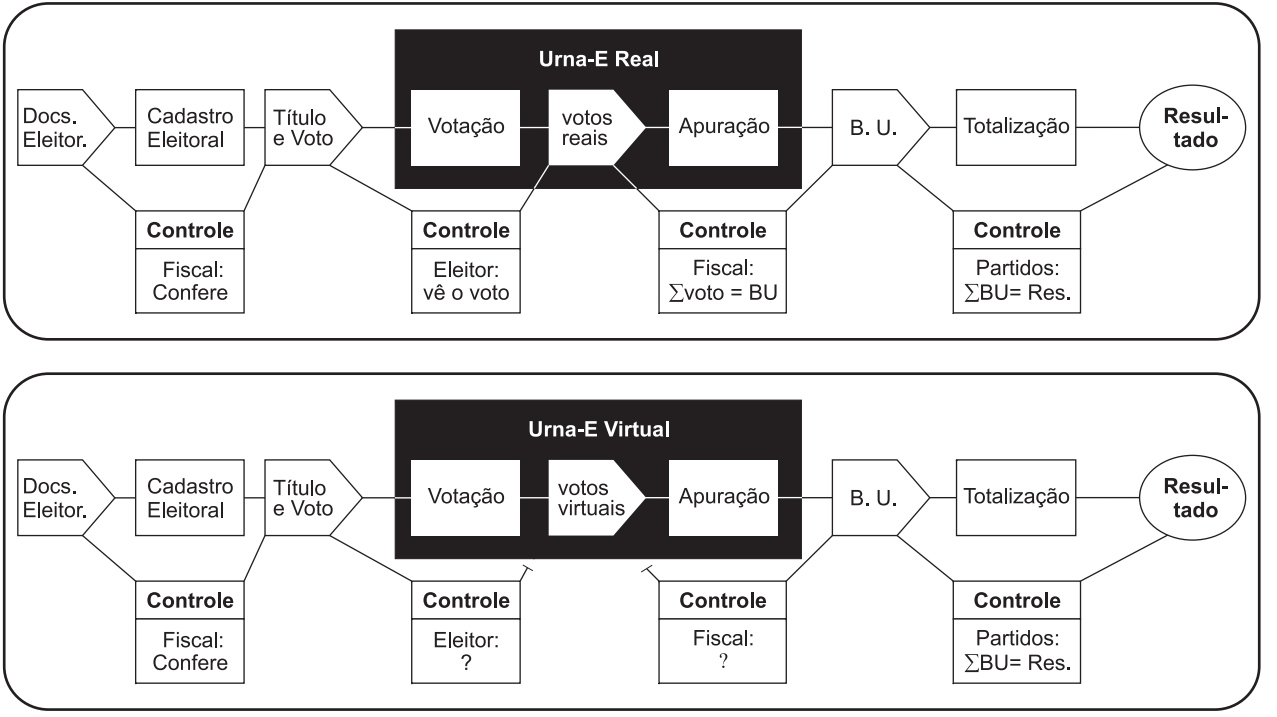
A diferença básica nos controles com os dois tipos de urnas eletrônicas é que os votos virtuais que ficam gravados nas memórias das urnas não têm como serem vistos nem pelo eleitor e nem pelos fiscais, perdendo-se assim a possibilidade de auditoria da apuração dos votos.

No demais, os dois processos se assemelham. Existem 4 etapas básicas: o Cadastramento de Eleitores, a Votação, a Apuração e a Totalização. Entre estas etapas a informação é sempre transmitida por documentos materiais ou virtuais.

Cada uma destas etapas ou documentos é um ponto de ataque onde é possível se introduzir fraudes mais ou menos abrangentes.

O cadastro, a votação, a apuração e a totalização poder ser burlados e os documentos do eleitor, os títulos, os votos, os boletins de urnas podem ser falsificados.

Como estas burlas e falsificações podem ser aplicadas e evitadas é o que se apresenta a seguir.



Controles em Urnas-E Reais e Virtuais

2. Aspectos Sócio-Culturais

"Andei sobre as águas, como São Pedro,
Como Santos Dumont, fui aos ares sem medo,
Fui ao fundo do mar, como o velho Picard,
Só pra me exibir, só pra lhe impressionar.

- Paulo Vanzolini

2.1 Um País do Zerésimo Mundo

A vontade de pertencer ao "*Primeiro Mundo*" aparece em muitos momentos na sociedade brasileira. É uma postura psicossocial eticamente aceita e também é um fator que estimula a evolução e o desenvolvimento.

Um exemplo citado com freqüência da caminhada do Brasil para o primeiro mundo seria nossa liderança mundial em eleições eletrônicas, ou seja, nossas Urnas-E Virtuais.

Desde a década de 80, a Justiça Eleitoral brasileira ensaiava o uso da informática, mas nem todos os passos foram firmes e exemplares.

Em 1982, ocorreu a malfadada tentativa do TRE-RJ de informatizar a totalização dos votos e que acabou num grande fiasco, o Caso Proconsult[7]. Tão traumática foi esta experiência, que nossa Justiça Eleitoral tem procurado renegá-la, excluindo-a de sua história oficial[8]. Oportunamente a memória nacional foi recuperada em 2005 com o lançamento do livro "*PLIM-PLIM*"[9] pelos jornalistas Paulo Henrique Amorim e Maria Helena Passos.

---

7. Ver "*Proconsult, um Caso Exemplar*", do jornalista Procópio Mineiro em: *http://www.votoseguro.org/noticias/cad3mundo1.htm*
8. Pode-se procurar exaustivamente nos sítios virtuais do TSE e do TRE-RJ, que nada será encontrado a respeito do Caso Proconsult.
9. Amorim, P.H. e Passos, M.H. – "*Plim-Plim, A Peleja de Brizola Contra a Fraude Eleitoral*" – Conrad Livros, São Paulo. 2005

Em 1986, houve a informatização do cadastro de eleitores quando, em tempos de desburocratização, se teve a péssima idéia eliminar a foto no Título Eleitoral, o que até hoje facilita a fraude da compra de voto.

Em 1996, com a adoção da Urna Eletrônica, foram automatizadas a identificação do eleitor no ato de votação, a própria votação e a apuração dos votos nas seções eleitorais.

A Urna-E Virtual brasileira foi implantada em três etapas nas eleições de 1996, 1998 e 2000, atingindo um terço do eleitorado de cada vez. Em 2000 o Brasil se tornou o primeiro país do mundo a ter 100% dos eleitores votando num processo 100% informatizado, começando pelo cadastro de eleitores, passando pela a identificação do eleitor, pela votação propriamente dita, pela apuração dos votos de cada urna e pela totalização dos votos.

E, para muitos, este é um motivo de inegável orgulho, uma prova do nosso desenvolvimento tecnológico.

Mas… para muitos outros, fica uma dúvida: Por que outros países, econômica e tecnologicamente mais desenvolvidos que o Brasil, ainda não informatizaram todo o processo eleitoral, especialmente a votação e a apuração dos votos?

Em menos de 2 anos, desde março de 2004, mais da metade dos Estados dos EUA[10] e Quebec no Canadá instituíram leis eleitorais onde se permite o uso de Urnas-E Reais, mas proíbem o uso de Urnas-E Virtuais, do tipo da brasileira, cujo resultado não pode ser recontado.

Por isto, talvez o Brasil não esteja na linha de frente do domínio da tecnologia de informatização do voto e sim tenha ultrapassado esta linha de maneira precipitada e imprudente!

O que se coloca aqui é um convite ao eleitor brasileiro para que reflita com calma, e sem ufanismo simplório, se o caminho da informatização do processo eleitoral brasileiro está sendo construído sobre bases sólidas ou se sobre mitos e ilusões.

---

10. Ver a relação atual dos Estados dos EUA que já proibiram o uso de Urnas-E Virtuais em: *http://www.verifiedvoting.org/*

O argumento da invulnerabilidade do sistema eleitoral brasileiro, tão propagandeado, é insustentável principalmente depois da publicação, em 2006, dos resultados de dois *Testes de Penetração*[11] desenvolvidos sobre Urnas-E Virtuais.

Em maio de 2006 foi divulgado a segunda parte do Relatório Hursti[12] pela ONG Black Box Voting, onde se apresentam os resultados de Testes de Penetração desenvolvidos sobre Urnas-E modelo TSx da empresa multinacional Diebold vendidos nos EUA e no Canadá. Os testes demonstraram que é perfeitamente possível se adulterar os programas daqueles modelos de forma a desviar votos numa eleição normal.

O grave para nós brasileiros, é que a empresa Diebold é também a fornecedora de 375 mil das 426 mil urnas eletrônicas que serão utilizadas nas eleições presidenciais brasileiras de 2006, as quais possuem esquema de segurança muito similar[13] aos modelos americanos.

É natural que se a Diebold soubesse como fazer Urnas-E Virtuais invulneráveis para fornecer ao Brasil, também as venderia nos EUA e Canadá. Por óbvio, se a Diebold não vende urnas invulneráveis lá, é porque também não sabe fazê-las aqui.

Um outro Teste de Penetração, realizado sobre urnas eletrônicas brasileiras do modelo 96 utilizadas nas eleições de fevereiro de 2006 no Paraguai, foi divulgado em vídeo[14], em junho de 2006. Foi um teste desenvolvido sem autorização oficial uma fez que a Justiça Eleitoral brasileira, que cedeu as urnas, não permite que eles sejam testadas abertamente.

Este vídeo do Paraguai foi desenvolvido de forma bastante didática, mostrando como um programa adulterado pode trocar o voto do eleitor depois que ele digita a tecla CONFIRMA e antes de ser gravado na memória da urna.

---

11. Ver mais em: *http://www.votoseguro.org/textos/penetracao1.htm*
12. Rel. Hursti – II: *http://www.blackboxvoting.org/BBVtsxstudy.pdf*
13. Ver comparação entre a Urna-E Virtual brasileira e a americana em: *http://www.votoseguro.org/textos/relatoriohursti1.htm*
14. Acessar a partir de: *http://www.votoseguro.org/textos/penetracao2.htm*

Mas, apesar destas demonstrações, a invulnerabilidade do sistema eleitoral brasileiro continua sendo o mote de toda a propaganda oficial, no Brasil e no Paraguai.

Poucos juízes e funcionários graduados da Justiça Eleitoral acreditam de fato na invulnerabilidade, mas entendem que manter a credibilidade do eleitor no sistema eleitoral é tão importante que justificaria mantê-los sob o jugo *goebelsiano* da propaganda enganosa.

Uma reportagem[15] de junho de 2006 publicada no Jornal A Tarde de Salvador, BA, revelou as combinações entre os presidentes dos TSE e do TRE-BA, em 2002, para manter em segredo do público uma quebra de segurança ocorrida 40 dias antes da eleição, quando desapareceram 8 mil cartões de memória das Urnas-E.

Assim, bem mais grave que as quebras de segurança no processo eleitoral é a decisão consciente da Justiça Eleitoral de escondê-las da sociedade. Uma conseqüência perversa desta prática é que acaba por adormecer o instinto de investigação dos fiscais, da imprensa e até da comunidade acadêmica.

É até curioso ver como fiscais eleitorais, que ignoram completamente as entranhas daquelas máquinas por onde correm os *bits* portadores dos votos que deveriam fiscalizar, rapidamente se declaram satisfeitos com demonstrações absolutamente inócuas de *"bom funcionamento"* do sistema.

Palavras mágicas proferidas em verdadeiros rituais tecnomísticos, como assinatura digital, resumo criptográfico (*hash*), embaralhamento pseudo-aleatório e zerésima, são pronunciados na frente de fiscais totalmente despreparados, que ignoram não só as limitações destas técnicas como também ignoram a regulamentação jurídica que as restringe ainda mais.

Zerésima é um neologismo criado pelo TSE para designar a lista impressa pela urna eletrônica, no início do processo de votação, onde o nome de cada candidato aparece ladeado com o número zero. Segundo os porta-vozes da Justiça Eleitoral, a zerésima é a "*garantia*"

15. Jornal A Tarde – "*O Segredo das Eleições 2002*", publicado em 04/06/2006, pág. 18.

de que não existem votos previamente depositados nas memórias da urna eletrônica.

Mas será mesmo uma garantia?

Se for, porque o TSE recusa sistematicamente permissão para testes livres[16], similares aos feitos nas urnas Diebold nos EUA e nas urnas brasileiras no Paraguai, que possam confirmar esta assertiva?

Mas, certamente, a zerésima não é garantia. Os testes nos EUA e no Paraguai comprovam o que qualquer programador de computador, mesmo iniciante, sabe: **é possível se imprimir qualquer coisa, como o número zero ao lado do nome do candidato, e ainda assim haver votos guardados na memória do computador**. Também é possível começar o processo de votação e apuração com zero votos para os candidatos e depois ir desviando uma porcentagem dos votos conforme estes forem sendo dados.

Cabe, assim, a pergunta:

Será que um sistema eleitoral que não pode ser testado livremente e não permite auditoria da apuração, é "coisa de Primeiro Mundo?".

Como na música do Paulo Vanzolini, que encabeça este capítulo, a ansiedade de muitos brasileiros "*só pra se exibir e só pra impressionar*" fê-los correr riscos desmedidos. Para sentirem-se no Primeiro Mundo, ignoraram a falta de garantais reais das Urnas-E Virtuais e aceitaram a Zerésima como ícone de integridade do sistema eletrônico de eleição.

Em vez de ingressarmos no Primeiro Mundo, onde idealmente apuração de eleição deveria ser transparente e auditável, a nossa Urna Eletrônica Virtual remete o Brasil, juntamente com o Paraguai, diretamente ao **Zerésimo Mundo**, onde o eleitor não pode ver o seu próprio voto e os fiscais não tem como fiscalizar a apuração.

… e o Zerésimo Mundo é qualquer coisa, uma democracia virtual talvez, mas não uma democracia verdadeira.

---

16. Ver a recusa aos testes livres na Informação 035/2004-SI/DG do TSE em: *http://www.votoseguro.org/textos/penetracao1.htm#5a*

2.2 A Seita do Santo Baite

O advento de novas tecnologias provoca diversas reações. Desde a tecnofobia até a tecnofascinação, passando pela indiferença e pela aceitação ponderada.

Em 2003, Pedro Dourado Rezende, matemático e professor de Ciências da Computação na Universidade de Brasília, escreveu um artigo sobre segurança do voto eletrônico no Brasil. Inspirado no nome do grupo místico Seita do Santo Daime, cunhou o termo *Seita do Santo Baite*[17] e o aplicou àqueles cidadãos que, maravilhados com a tecnologia, apostam seu dinheiro em Máquinas de Jogos de Azar e depositam seus votos em Urnas-E Virtuais sem se aperceberem de que tais máquinas podem burlar tanto o resultado do jogo como da apuração dos votos.

A respeito da similaridade entre máquinas eletrônicas de jogos de azar e as Urnas-E Virtuais brasileiras que lhes foram oferecidas pela empresa Diebold-Procomp, o Juiz Federal Manuel Blanco da Província de Buenos Aires na Argentina disse:

"O voto eletrônico é só uma idéia extravagante. Para o resultado do escrutínio é como jogar numa máquina caça-níqueis"[18].

Uma característica dos fiéis da Seita do Santo Baite é que para serem "*modernos*" aceitam a tecnologia por pura fé, longe de entenderem como funciona e os riscos que traz. Não sabem, por exemplo, que computadores não são capazes de sortear ou embaralhar nada, e que somente podem calcular valores por rotinas significativamente chamadas de pseudo-aleatórias.

Até a perda de direitos civis, duramente conquistados em gerações anteriores, é cegamente tolerada como no Brasil onde se aceitou o fim do direito à conferência da apuração.

Carl Sagan, astrônomo, divulgador científico e autor do famoso "*2001, Uma Odisséia no Espaço*", que não dá para ser chamado de

17. Ver em: *http://www.cic.unb.br/docentes/pedro/trabs/azeredo.htm*
18. Reportagem "*Prueba Piloto En Municipios Bonaerenses*", Jornal O Clarín de Buenos Aires, em 24/09/1999.

tecnofóbico, em outro livro seu, "*O Mundo Assombrado pelos Demônios*" [19], escreveu sobre os riscos da tecnofascinação:

"Nós criamos uma civilização global em que elementos mais cruciais – os transportes, as comunicações e todas as outras indústrias, a agricultura, a medicina, a educação, a proteção ao meio ambiente e até a importante instituição democrática do voto – dependem profundamente da ciência e da tecnologia.

Também criamos uma ordem em que quase ninguém compreende a ciência e a tecnologia. É uma receita para o desastre. Podemos escapar ilesos por algum tempo, porém mais cedo ou mais tarde essa mistura inflamável de ignorância e poder vai explodir na nossa cara."

Os defensores do uso de Urnas-E Virtuais, leigos ou informatas, argumentam que o voto impresso é um "*retrocesso tecnológico*" e que as modernas tecnologias de informação, como Criptografia e Assinatura Digital, seriam suficientes para dar-lhes garantia de uma eleição honesta. Curioso é notar que mais de 99% destes defensores nem mesmo conhecem quais são os recursos criptográficos utilizados e nem quais são suas limitações técnicas.

Do outro lado, a favor das Urnas-E Reais e da impressão do voto, se encontram justamente os maiores especialistas mundiais em Criptografia e Assinatura Digital, inclusive os principais inventores nestas áreas, como Ronald Rivest[20], Bruce Schneier[21] e David Chaum[22].

O Brennan Center for Justice da Faculdade de Direito da New York University montou uma grande equipe composta pelos maiores expoentes mundiais na área de segurança de dados, de criptografia

---

19. Sagan, Carl – *O Mundo Assombrado pelos Demônios* (The Demon-haunted World), Cia. das Letras, 1997, São Paulo. Cap. 2.
20. *Ronald Rivest*, um dos inventores da técnica de Assinatura Digital. Ver: *http://www.votoseguro.org/textos/rivest-voting1.pdf*
21. *Bruce Schneier*, o mais premiado inventor de sistemas criptográficos. Ver: *http://www.schneier.com/crypto-gram-0404.html#4*
22. *David Chaum*, inventor do sistema patenteado de Dinheiro Virtual. Ver: *http://www.chaum.com/*

Sobre seu sistema eleitoral criptográfico, ver referência em: *http://www.votoseguro.org/textos/chaum-voting1.htm*

e do voto eletrônico, e em junho de 2006 apresentou o Relatório Brennan[23] onde a principal recomendação é a adoção do voto impresso conferido pelos eleitores como forma de atenuar os riscos de fraude em máquinas eletrônicas de votar.

Também não dá para taxar de tecnofóbicos estes superespecializados técnicos em segurança de dados, que recomendam a materialização do voto como única forma de obter defesas eficazes contra fraudes informatizadas em eleições.

É muito importante para os fiscais eleitorais entenderem este caldo psicossocial que fertiliza o meio-ambiente eleitoral no qual trabalharão. Devem compreender que a fidelidade de muitos eleitores e fiscais brasileiros à Seita do Santo Baite é que levou nosso País ao Zerésimo Mundo, onde garantias virtuais são tidas como reais.

Assim, a primeira lição conceitual que se dá aos fiscais eleitorais que querem aprender a fiscalizar o voto eletrônico é enfrentar sem vergonha e excomungar os mitos da Seita do Santo Baite, despertar o instinto de investigação adormecido e partir em busca de garantias reais, mais precisamente, partir em *busca de garantias que possam compreender como funcionam*.

2.3 Acúmulo de Poderes

Além de compreender os aspectos psicossociais que afetam o seu meio de trabalho, também é muito importante para o fiscal eleitoral conhecer os fatores jurídico-institucionais, que contribuem na modelagem do nosso sistema eleitoral.

O principal destes fatores a ser compreendido é o acúmulo de poderes pela Justiça Eleitoral brasileira.

O estudo nº 143/2000[24], da Consultoria Legislativa do Senado Federal, feito a pedido do então senador Roberto Requião apresenta uma análise comparativa entre a ordenação juridico-institucional

23. Ver em: *http://www.votoseguro.org/textos/brennan1.htm*

24. Este estudo não se encontra disponível para consulta. Para cópias, dirigir-se diretamente à Consultoria Legislativa do Senado Federal.

do processo eleitoral nos seguintes países: Brasil, Estados Unidos, Alemanha, Itália, França, Finlândia, Chile, Uruguai e Argentina.

Muitas são as maneiras de se distribuir os poderes e as funções entre os atores do processo eleitoral. Em alguns países existe a Justiça Eleitoral dentro do Poder Judiciário, em outros não. Nos EUA, o contencioso eleitoral é decidido na Justiça Comum. No Uruguai é decidido por uma corte especial nomeada pelo Poder Legislativo.

A administração do processo eleitoral (Poder Executivo) pode ficar nas mãos do executivo municipal, como na Itália e França, ou do executivo estadual, como nos EUA, ou do executivo federal, como na Alemanha e Finlândia, ou ainda ser independente dos três Poderes tradicionais, como no Chile.

Mas no Brasil, uma única autarquia federal concentra os três poderes republicanos e, apesar de ter a palavra "tribunal" no seu nome (Tribunal Superior Eleitoral) e por isto ser chamada de Justiça Eleitoral, ela exerce também toda administração executiva e a normatização legislativa do processo eleitoral. O Paraguai também adota estrutura similar a brasileira. Lá, o Tribunal Superior de Justiça Eleitoral, TSJE, acumula as funções administrativa e normativa das eleições.

Esta situação, incomum no resto do mundo desenvolvido, foi construída ao longo de nossa história eleitoral.

A criação do TSE em 1932 visava democratizar as eleições brasileiras marcando o fim da época conhecida como a do *Voto à Bico de Pena* e da *Política Café-com-Leite*. Vários conceitos que são essenciais numa democracia moderna, como o voto universal, a inviolabilidade do voto e a transparência do processo, foram aperfeiçoados com o advento do TSE, mas o Princípio de Tripartição do Poderes foi abandonado.

O acúmulo de poderes do TSE está consubstanciado logo no artigo primeiro do nosso Código Eleitoral de 1965:

***"CE, Art. 1º** Este código contém normas destinadas a assegurar a organização e o exercício de direitos políticos, precipuamente os de votar e ser votado.*

***Parágrafo único.** O Tribunal Superior Eleitoral expedirá instruções para sua fiel execução."*

Neste parágrafo único está clara a delegação de poderes legislativos a um tribunal que, por meio das tais instruções, regulamenta como seus membros atuarão na administração das eleições e, numa clara anomalia institucional, regulamenta até os limites de atuação da fiscalização que atuará sobre seus próprios atos administrativos.

Quanto ao voto eletrônico, o Art. 152 e o Art. 173 do Código Eleitoral reforçam ainda mais os poderes do TSE deixando a seu exclusivo critério o uso e regulamentação de máquinas de votar e de apurar.

*"**Art. 152.** Poderão ser utilizadas máquinas de votar,* ***a critério e mediante regulamentação do Tribunal Superior Eleitoral.***

Art. 173. Parágrafo único.** Na apuração, poderá ser utilizado sistema eletrônico,* ***a critério do Tribunal Superior Eleitoral e na forma por ele estabelecida."

O Tribunal Superior Eleitoral é o único órgão integrante da Justiça Brasileira que detém funções administrativa e legislativa que extrapolam seu âmbito jurisdicional. Pode-se contar nos dedos de uma só mão os países onde um só órgão acumula tantos poderes sobre o processo eleitoral como o nosso TSE. O Paraguai é um destes países.

Num equívoco inegável, deixou-se com a Justiça Eleitoral o poder de regulamentar a fiscalização e ainda o controle de todos os recursos orçamentários oficiais em eleições. Toda a verba da União para as eleições, inclusive eventual verba para fiscalização deste processo, é destinada e controlada por este superórgão.

É um caso clássico kafkaniano onde o fiscalizado manda no fiscal.

Como, numa espécie de teorema social, em terreno adubado com o acúmulo de poderes, crescem sempre, como ervas daninhas, o autoritarismo, o corporativismo e a falta de transparência. Nosso processo eleitoral sofre destes males.

Assim, também é importante que o fiscal eleitoral compreenda esta ordenação autoritária e centralizadora sob a qual deverá atuar.

Em processos jurídicos normais perante a Justiça Eleitoral, como em casos relativos à publicidade, pesquisas e abusos de poder econômico, existem os tradicionais pólo ativo (o denun-

ciante) e pólo passivo (o denunciado) que serão julgados por um juiz independente.

Mas na grande maioria dos processos sobre irregularidades detectadas pela fiscalização eleitoral, o pólo passivo é o agente administrativo responsável pelo problema que se questiona, ou seja, *é o próprio juiz eleitoral!*

Assim, não é raro acontecer que um juiz eleitoral julgue causa em que ele próprio é, por extensão de comando, o réu.

Inúmeros são os exemplos deste conflito jurídico, como o já citado Caso Proconsult onde todo o inquérito foi desenvolvido sob ordem dos mesmos juízes responsáveis administrativos pela decisão de usar e pelo uso do sistema burlado. Apesar de terem sido forçados pelas evidências a anular a apuração inicial, recontar os votos e inverter o resultado fraudado[25], concluíram oficialmente que não houve tentativa de fraude[26] e absolutamente ninguém foi responsabilizado ou punido.

Outro exemplo clássico do problema causado por esta mistura de acúmulo de poderes com a tecnofascinação é o Caso de Araçoiaba da Serra[27], pequeno município de São Paulo, que nem foi o caso de fraude, apenas de um erro.

Na eleição municipal de 2000, oficiais do Cartório Eleitoral de responsabilidade administrativa do Juiz da Comarca, esqueceram de incluir o nome de alguns candidatos a vereador no arquivo de dados carregados nas urnas eletrônicas.

Os agentes oficiais e os fiscais eleitorais – crentes do Santo Baite anestesiados pela propaganda oficial da infalibilidade do sistema – não conferiram nem fiscalizaram coisa nenhuma e não detectaram a falta de alguns nomes na extensa lista de candidatos chamada Zerésima.

---

25. Amorim, P.H. e Passos, M.H. – "*Plim-Plim, A Peleja de Brizola Contra a Fraude Eleitoral*" – Conrad Livros, São Paulo. 2005

26. Porto, Walter. C. – "*A Mentirosa Urna*" – Livraria Martins Fontes Editora, São Paulo, 2004

27. Ver em: *http://jus2.uol.com.br/doutrina/texto.asp?id=1553*

No dia da eleição, os candidatos esquecidos não puderam ser votados. A solução óbvia seria o juiz anular a eleição, porque viciada. Mas, para tanto, o juiz teria que reconhecer erro cometido sob sua própria administração e comando.

A soberba e o instinto de autodefesa, uma vez que juízes também são seres humanos sujeitos as nossas mazelas, não lhe permitiram reconhecer o erro. Julgando onde era o réu, indeferiu todos os pedidos de anulação que lhe foram apresentados, inclusive pelo Ministério Público. Na instância estadual prevaleceu o espírito de corpo e todos os recursos também foram negados. Somente na instância superior prevaleceu o bom senso e, 3 anos depois, a eleição foi anulada.

Um erro que poderia ter sido detectado antes da eleição, não fosse a tecnofascinação que cegou os fiscais e os agentes oficiais, ou que poderia ter sido corrigido em 30 dias com uma nova eleição, não fosse o acúmulo de poderes que cegou o juiz eleitoral, só foi corrigido mais de 3 anos depois. Os novos vereadores regularmente eleitos tiveram menos de 12 meses de mandato.

Uma reportagem do Jornal do Brasil[28], de junho de 2006, mostra mais uma conseqüência do acúmulo de poderes dos juízes eleitorais: **o pré-julgamento sem pejo**.

Há um inquérito na Polícia Federal para apurar possíveis fraudes nas eleições do Rio de Janeiro em 2002. Antes mesmo do inquérito se concluir, retardado que foi pela demora de sete meses do TRE-RJ em entregar os cartões de memória das urnas para perícia, o presidente do TRE-RJ, juiz e responsável administrativo direto no processo investigado, já decretou a sentença afirmando, na reportagem: "*a investigação servirá para demonstrar quanto as urnas são seguras*".

Recentes exemplos de abuso de poder sobre a fiscalização, são as decisões do TSE de não respeitar alguns artigos da lei eleitoral 9.504/97 como:

a. o Art. 66: não apresentando aos fiscais dos partidos os programas de computador que utiliza em eleições suplementares;

28. Matéria "*Em xeque, segurança da urna eletrônica*", Jornal do Brasil, 11/06/2006

b. o Art. 68: não entregando cópias dos Boletins de Urnas[29] aos fiscais dos partidos que as solicitarem.

Para não alongar demais esta lista, apenas se faz referência a outros exemplos públicos sobre as dificuldades de fiscalização conseqüentes do acúmulo de poderes da Justiça Eleitoral: a) a impugnação do *software* eleitoral em 2000[30]; b) o Caso de São Domingos[31], GO, em 2000; c) o Caso de Marília[32], SP, em 2004; e d) o impedimento de Testes de Penetração[33].

É importante compreender o papel fundamental da acumulação de poderes do TSE no Brasil e do TSJE no Paraguai no processo que levou estes dois países a ingressarem no Zerésimo Mundo.

Fiéis do Santo Baite existem em todos os países, mas foi nestes, onde a tecnofascinação pôde associar-se ao autoritarismo eleitoral, que primeiro ocorreu a adoção precipitada de Urnas-E Virtuais sem garantias reais.

Na Argentina, por exemplo, onde a Justiça Eleitoral não acumula tantos poderes, juízes eleitorais impediram o uso oficial de Urnas-E Virtuais, oferecidas gratuitamente pelo TSE e OEA ao agente administrador das eleições provinciais em 1999 e 2003.

A solução para esta situação jurídica anômala no Brasil, onde o réu pode ser o próprio juiz, é óbvia, mas não é simples de ser construída.

Dever-se-ia desconcentrar os poderes eleitorais. Criar, no Congresso Nacional, uma comissão de regulamentação da fiscalização eleitoral, tirando este poder do TSE. Criar um órgão executivo eleitoral independente do comando direto dos poderes tradicionais, como no Chile, por exemplo. Criar um órgão fiscalizador composto pelos Partidos, mas com verba oficial própria.

---

29. O Art. 42 da Resolução TSE 22.154 de março de 2006 conflita com a lei, restringindo a entrega de BU aos fiscais e impedindo a defesa contra fraudes na Totalização. Foi questionada a validade deste Art. 42. Mas sua validade será decidia pelos mesmos juízes que, legislando, criaram o artigo questionado.
30. Ver em: *http://www.votoseguro.org/textos/unicamp1.htm*
31. Ver em: *http://www.votoseguro.org/textos/evandro1.htm*
32. Ver em: *http://www.votoseguro.org/arquivos/marilia2004.zip*
33. Ver em: *http://www.votoseguro.org/textos/penetracao1.htm*

Manter no TSE apenas a função judiciária e, preferencialmente, que seus juízes não fossem os mesmos de instâncias superiores, evitando que recursos contra suas decisões voltassem a cair nas suas próprias mãos ou nas mãos de seus pares.

Mas enquanto esta solução ideal não vem – e deve demorar ainda muito a vir porque nossa sociedade nem conscientizada do problema está – **é fortemente recomendado que os advogados de Partido Político que atuarem em processos regulares, de publicidade, pesquisas, etc., NÃO ATUEM também em processos de fiscalização do voto-E**. Pois o advogado que atuar na fiscalização eleitoral terá que ser treinado para **enxergar e tratar o juiz eleitoral como o seu fiscalizado, um funcionário público administrativo passível de sofrer e esconder mazelas**, e não como um ente imparcial e isento de interesses.

2.4 A Gênese das Fraudes

Nos anos 90, grassou o *Mito da Tecnologia Redentora* entre os fiéis do Santo Baite, que acreditavam que recursos da informática, como a criptografia e a assinatura digital, seriam capazes de erradicar qualquer possibilidade de fraudes e golpes em cadastros informatizados, como os de empresas, os de bancos, o da previdência e o eleitoral.

No início de 1994, Bruce Schneier, já citado, autor dos maiores *best-sellers* sobre segurança de dados, escreveu o livro "*Aplied Cryptography*" onde descrevia uma utopia: novas técnicas matemáticas que permitiriam criar em ambientes informatizados, coisas como jogos confiáveis, autenticação não-falsificável, dinheiro virtual anônimo e até eleições seguras.

Logo depois, em dezembro de 1994, imbuído neste mito, o Min. Carlos Velloso na sua posse como presidente do TSE comunicou sua decisão monocrática de imediatamente implantar a "*informatização do voto*", ou seja, as Urnas Eletrônicas, para erradicar as fraudes no processo eleitoral brasileiro. Textualmente o Min. Velloso disse:

"Estamos convencidos que estas fraudes serão banidas do processo eleitoral brasileiro no momento em que eliminarmos as cédulas, as urnas e os mapas de urnas, informatizando o voto".

É ou não é apologia do Mito da Tecnologia Redentora?

Assim, não foi por acaso que no Brasil foi adotada a Urna-E Virtual que não emite o voto impresso conferido pelo eleitor.

Mas a crença de Schneier e do Min. Velloso era ilusão. No nascer do novo milênio ficou claro para a comunidade de segurança que fraudes vêm das pessoas e não das tecnologias.

Logo em 2001, em novo *best-seller* chamado "*Secrets and Lies*"[34], Schneier humildemente reconheceu o seu erro conceitual e declarou que os problemas de segurança em sistemas informatizados não seriam resolvidos pela tecnologia digital.

Já no prefácio de seu novo livro, ele disse:

"Acreditou-se que a criptografia era um tipo de pó mágico da segurança, que poderia ser espalhado pelo software para que se tornasse seguro. Que poderiam invocar palavras mágicas como 'chave de 128 bits' e 'infraestrutura de chaves públicas'.

Segurança é um projeto, e não um produto. Nenhum sistema é perfeito; nenhuma tecnologia é a Resposta.

Se você acredita que a tecnologia pode resolver seus problemas de segurança, ***então você não conhece os problemas e nem a tecnologia.****"*

É ou não é exorcismo do Mito da Tecnologia Redentora?

Só que nossas autoridades eleitorais não tiveram a mesma humildade do criptógrafo americano. As Urnas-E Virtuais criadas sob este mito, estão sendo banidas em todo o mundo desenvolvido, mas continuam sendo usadas no Brasil.

Em qualquer sistema eleitoral, seja manual ou informatizado, para ocorrência de fraudes é essencialmente necessário que três tipos de agentes tenham comportamento comprometedor:

---

34. Schneier, Bruce. *Segurança.com, Segredos e Mentiras sobre a proteção na vida digital*. Editora Campus, Rio de Janeiro, 2001.

1. **Candidatos**: deve haver ao menos um candidato inescrupuloso disposto a burlar a segurança do sistema;
2. **Funcionários** do processo eleitoral: é preciso a participação, ativa ou passiva, de funcionários muito incompetentes ou que cedam à corrupção;
3. **Fiscais** dos Partidos: é necessário erro, omissão ou intimidação dos fiscais dos candidatos honestos.

A primeira condição acima é óbvia. Para que haja fraude é necessário existir alguém disposto a atacar o sistema.

A segunda condição é fundamental, pois nas eleições os funcionários da Justiça Eleitoral dispõem de recursos e poderes para tentarem impedir ataques e fraudes. Somente quando eles cedem à corrupção e aceitam se omitir ou a agir maliciosamente é que fraudes se viabilizam.

A terceira condição também é fundamental.

Por exemplo, no sistema tradicional de voto manual onde tantas fraudes afligiam. O Código Eleitoral concedia acesso aos fiscais dos partidos a todos locais e momentos que eram necessários para detectar e inibir fraudes e, por isto, as fraudes só ocorriam quando, por qualquer motivo, a fiscalização falhava.

Os fiscais podiam:

1. Ter conhecimento prévio do cadastro de eleitores;
2. Ter conhecimento prévio dos mesários indicados;
3. Estar presente na lacração das urnas vazias;
4. Acompanhar a identificação dos eleitores e a votação;
5. Acompanhar o transporte das urnas com votos até o local da apuração;
6. Ficar a um metro de distância dos escrutinadores;
7. Anotar o resultado de cada mapa de urna.

E, apesar disto tudo, ocorriam fraudes em todos estes sete momentos. Eleitores fantasmas eram cadastrados e votavam, mesários ligados a candidatos eram admitidos, urnas eram "*engravidadas*" antes da votação, eleitores regulares eram constrangidos ou induzidos

na hora de votar, mesários introduziam votos extras nas urnas, a urna com votos era trocada durante o transporte, a apuração era fraudada e os resultados nos mapas de urnas eram adulterados.

Na realidade, havia uma verdadeira competição de fraudes onde umas se sobrepunham a outras. E tudo isto acontecia porque os fiscais falhavam em cumprir suas tarefas.

Muitas vezes falhavam porque eram intimidados pelo autoritarismo de funcionários corruptos, que impediam o livre acesso dos fiscais bem no momento onde eles mesmos iriam burlar. O abuso de poder por agentes eleitorais, inclusive por juízes, costuma ser um bom indício de fraudes em andamento.

Em resumo, a gênese das fraudes eleitorais está no comportamento de pessoas. Onde houver candidatos e funcionários desonestos e fiscais incompetentes… tentativas de fraude brotarão.

É muito ingênuo pensar, como pensou o Min. Velloso em 1994, que a informatização do voto sozinha, como um passe de mágica, tivesse o condão de acabar com a ação de candidatos inescrupulosos, funcionários corruptos e fiscais incompetentes.

Com o advento da eletrônica não sumiram estas pessoas. Elas continuam existindo e atuando em eleições. A tecnologia pode adicionar dificuldades e custos às fraudes, mas assim que a "*tecnologia de fraude*" for dominada e os custos compensarem, as fraudes ressurgirão.

Por exemplo, na primeira eleição com urnas eletrônicas em 1996 se dizia que a nova tecnologia não permitia que mesários introduzissem votos extras nas urnas eletrônicas.

Mas logo, nas eleições seguintes, os mesários foram descobrindo como isto era possível e a prática fraudulenta foi crescendo a cada eleição. Em 2005, o ministro Carlos Velloso, novamente ocupando a presidência do TSE, finalmente reconhecendo a gravidade do problema, mas ainda embevecido pelo Mito da Tecnologia Redentora, anunciou que agora iria implantar os modernos recursos de "*biometria*" (impressão digital do eleitor) nas urnas-E para "*acabar com o último reduto da fraude eleitoral*".

Lembre-se de que ele tinha dito exatamente isso em 1994 quando decidiu implantar as Urnas-E Virtuais. Felizmente a implantação da biometria foi suspensa para melhores estudos, depois de denunciada sua ineficácia ao Tribunal de Contas da União pelo PDT.

Assim, a lição deste capítulo é que **só a boa fiscalização pode atenuar as fraudes eleitorais** e não a tecnologia em si como pleiteava o Min. Velloso.

A boa fiscalização pode se valer da boa tecnologia, iniciando por entendê-la, mas repudiar o Mito da Tecnologia Redentora é obrigatório para o bom fiscal eleitoral.

A partir do próximo capítulo, passa-se a explicar: a) como fraudes podem ser introduzidas nas diversas etapas e momentos do processo eleitoral eletrônico como no cadastro, na votação e na apuração; b) como os fiscais devem atuar para tentar impedir estas fraudes; e c) como as tecnologias podem afetar esta relação fraudeXdefesas para um lado ou para o outro.

3. As Fraudes e as Defesas

"No campo do adversário
é bom jogar com muita calma,
esperando pela brecha,
pra pode ganhar."

– Luís Gonzaga Jr.

3.1 Regras Gerais

No atual sistema eleitoral informatizado, com limitações à auditoria plena impostas por regras equivocadas, muitos tipos de fraudes podem acontecer. Certos tipos, principalmente as de baixa tecnologia, viabilizam-se por falta de uma fiscalização atenta e consciente. Se os fiscais atuarem com competência, boa parte destas fraudes poderão ser detectadas a tempo de neutralizá-las.

Existem algumas regras gerais que devem ser sistematicamente seguidas pelos fiscais eleitorais para que possam enfrentar e impedir os ataques ao sistema eleitoral que porventura partirem de candidatos e funcionários eleitorais desonestos.

Planejamento e Controle

O processo de fiscalização de uma eleição não deveria ocorrer somente nos dias próximos da eleição.

A fiscalização do Cadastro de Eleitores nos Cartórios Eleitorais deve ser permanente, mesmo em anos nos quais não haja eleição.

Participar da elaboração das resoluções do TSE que estabelecem as regras de fiscalização, apresentando sugestões que facilitem a vida do fiscal e viabilizem seu trabalho, deve ser desenvolvida já no mês de janeiro do ano de eleições.

A fiscalização dos programas de computador que serão utilizados em eleições em outubro deve ser desenvolvida a partir do mês de abril junto ao TSE em Brasília.

Os programas de computador para análise e apoio à fiscalização devem ser desenvolvidos a partir de maio/junho.

O treinamento dos fiscais que atuarão nas eleições deve começar em agosto/setembro.

E tudo isto deve ser coordenado e planejado por uma equipe eclética, onde elementos especializados em informática e advogados tenham participação igualitária[35].

Treinar e apoiar os Fiscais

A falta de recursos financeiros e físicos nos diretórios municipais dos partidos políticos é uma realidade constante. Como, também, não existe nenhuma verba oficial da União destinada a fiscalização das eleições, dificilmente se consegue montar uma equipe de fiscalização profissional.

Normalmente os fiscais eleitorais são voluntários motivados, mas são, quase sempre, amadores despreparados e sem apoio logístico.

Pior do que não fiscalizar, é fiscalizar equivocadamente deixando passar as fraudes e ainda lhes dando a legitimidade de terem sido "*fiscalizadas*".

O Partido Político, interessado em se defender de fraudes, deve sempre dar algum treinamento aos seus voluntários para que, no mínimo, conheçam a legislação e as peculiaridades do processo, e saibam o que e porque estão fazendo, para evitar serem enganados.

Dar-lhes apoio logístico, como equipamentos, materiais, condução e até alimentação, também é importante.

Por exemplo, é muito comum a fiscalização nos locais de votação começar animada pela manhã do dia de votação, mas no final do dia, sem apoio e alimentação, no momento mais propício para a Fraude de Engravidar Urnas-E[36], estar desatenta, quando não, ausente.

---

35. É exatamente por este motivo que este livro foi escrito em conjunto por um técnico em segurança de dados e uma advogada eleitoral.
36. Descrita no capítulo 3.3.

Sinergia dos Grupos

Uma forma de enfrentar a carência de recursos para a fiscalização é a associação entre partidos afins.

Por exemplo, cada partido pode não conseguir colocar 3 fiscais (número ideal) em cada seção eleitoral e ainda arcar com os custos de treinamento. Coordenando esforços de vários partidos num projeto centralizado, mas dividindo tarefas de forma planejada e disciplinada, pode-se valer da sinergia que faz um grupo funcionar melhor que a soma de cada parte individual.

Aliás, de maneira geral, fiscais eleitorais podem e devem tratar os fiscais dos outros partidos como aliados e não como oponentes. Na maioria dos casos, há muita convergência de interesses entre os fiscais de partidos diferentes.

Apurar o Instinto

São inúteis os fiscais que, entorpecidos pelo Mito da Tecnologia Redentora ou pela propaganda oficial sobre a invulnerabilidade do sistema eleitoral, se tornarem crentes da Seita do Santo Baite e passarem a atuar como se a tecnologia, que não dominam, substituísse seus serviços.

Devem ser afastados do grupo de fiscais, os voluntários de qualquer nível que acreditam no discurso oficial de que tal ou tal tipo de fraude não possa ocorrer, pois pela brecha que eles deixam aberta podem passar muitos votos falsos.

Desconfiar sempre que algo errado possa estar acontecendo é obrigação dos fiscais e para isto eles devem aguçar o seu "*instinto investigativo*" procurando imaginar como se poderia burlar a etapa do processo sob sua fiscalização.

Respeitar todos os agentes

Saber que a ocorrência de fraudes depende da conivência de funcionários eleitorais não os torna todos desonestos. Pelo contrário, a maioria estará agindo corretamente, dentro de suas atribuições.

Por isto, é regra de ouro respeitar todos os agentes públicos tratando-os com a deferência devida. O bom trato abre muitas portas e é disto o que o fiscal mais necessita.

Jamais levantar a voz, ofender ou agredir os representantes oficiais, mesmo quando se desconfia de sua honestidade.

Uma atitude impensada de um fiscal permite que ele venha a ser rotulado de impertinente e acaba por dar mais munição ao inimigo.

Quando se encontrar perante alguém que supostamente esteja participando de um esquema fraudulento, procurar ajuda, procurar testemunhas, ***procurar registrar o fato detalhadamente em atas oficiais***, fotos ou o que for possível, e, em seguida, levar o problema para instâncias superiores.

Enfrentar o Autoritarismo

Respeito não é submissão.

Os fiscais possuem direitos de acesso estabelecidos por leis e resoluções do TSE que regem todo o processo eleitoral e devem exigir seus direitos nos momentos oportunos.

O comportamento autoritário em agentes eleitorais é muito exacerbado por causa do acúmulo de poderes da Justiça Eleitoral. Até simples cidadãos, levados à função de mesários sentem-se "*otoridades*" e abusam disto procurando negar direitos de acesso aos fiscais. Não é raro ameaçá-los de prisão.

Também os juízes eleitorais, humanos que são, freqüentemente cedem à soberba, seduzidos pelos inéditos poderes executivos e legislativos que recebem quando adentram à Justiça Eleitoral.

Lembrar que o **autoritarismo pode ser um forte sinal de fraude em andamento**.

Por isto, o fiscal eleitoral deve compreender que os juízes e os funcionários eleitorais são seus fiscalizados e nunca deve abrir mão de direitos ou aceitar ser afastado de locais em momentos nos quais a lei garante sua presença.

Conhecer toda a Legislação Pertinente

Obviamente, para exigir o respeito a seus direitos de acesso, o fiscal deve conhecê-los todos e muito bem.

Assim, no treinamento prévio dos fiscais deve-se, necessariamente, incluir aulas da legislação que digam respeito à fiscalização eleitoral e também sobre a ordenação jurídica de todo o processo.

O fiscal deve entender claramente quais são os níveis hierárquicos na Justiça Eleitoral e quais são as relações e as diferentes atribuições dos Tribunais, dos Cartórios, das Juntas e das Seções eleitorais.

Também é importante que conheça, em detalhes, seus direitos de acesso, seu direito absoluto de peticionar perante órgãos públicos, a proibição de ser detido por motivo de fiscalização e as penas que recaem sobre quem o impedir.

É conveniente, inclusive, que os fiscais sejam munidos de um "*Kit de Direitos*", que contenha cópias das leis e das resoluções do TSE pertinentes, para lançarem mão quando envolvidos numa situação em que uma atitude autoritária possa cerceá-los.

Isto aumenta muito a autoconfiança do fiscal e pode inibir atos autoritários que estejam encobrindo fraudes.

Entender a Lógica do Processo

Fiscais que não entenderem muito bem o funcionamento do processo fiscalizado, nem como este se encaixa em todo o resto do processo eleitoral, serão constantemente enganados pelo interessado em burlar.

Por exemplo, os fiscais devem entender claramente que, para impedir a Clonagem de Urnas-E[37] ou as fraudes de totalização[38], a coleta do BU impresso deve ser feita no exato momento de sua emissão pelas urnas eletrônicas na Seção Eleitoral. Coletá-lo

37. Descrita no capítulo 3.3.
38. Descrita no capítulo 3.5.

posteriormente, no Cartório Eleitoral, é inútil, pois já pode ter chegado lá trocado.

Porém são muito freqüentes casos em que juízes provocam a quebra da segurança na totalização porque estimulam os partidos a obter suas cópias dos BU somente com o Comitê Interpartidário no Cartório Eleitoral, com argumentos de invulnerabilidade (impossibilidade da troca) e da diminuição de custos para todos.

Há casos até de Desembargadores de Tribunais Regionais que patrocinaram acordos formais entre os representantes dos partidos em que estes, não entendendo a engrenagem da fiscalização, abriram voluntariamente mão do direito de ter acesso ao BU no momento de sua emissão. Neste caso, estavam abrindo mão de poder fiscalizar com efetividade a totalização dos votos em troca de absolutamente nada.

Se o fiscal não entender um mínimo de informática, será invariavelmente enganado por ineficazes rituais de fiscalização, verdadeiros shows de ilusionismo, como a emissão da Zerésima, as votações simuladas e as verificações de assinatura digital mostradas na tela da própria máquina sob análise.

Ter Muita Calma

O fiscal eleitoral vai ter que atuar num ambiente em que os fiscalizados mandam.

Naturalmente isto pode criar dificuldades e não se pode desistir ou perder a paciência por isto.

Como disse o Gonzaginha*: "No campo do adversário é bom jogar com muita calma, esperando pela brecha, pra pode ganhar*".

3.2 Fraudes no Cadastro Eleitoral

O Eleitor Fantasma

Incluir nomes de eleitores inexistentes no Cadastro Nacional de Eleitores, ou manter como ativos eleitores já falecidos, para que de alguma forma alguém, de carne-e-osso, vote no lugar deles, é uma modalidade de fraude que persistiu mesmo depois do advento da eletrônica no processo eleitoral.

Alias, piorou muito com a informatização do Cadastro de Eleitores em 1986, pois na sua regulamentação, pela Lei 7.444/85, eliminou-se a foto do Título de Eleitor, erro tático que facilitou tremendamente a votação em nome dos Eleitores Fantasmas.

A adoção das urnas eletrônicas em 1996 não dificultou em nada a vida dos "*gasparzinhos*".

Trata-se uma modalidade de fraude onde é necessária a participação de funcionários dos cartórios eleitorais e de juízes, desatentos ou venais, pois são estes que têm que assinar os títulos falsos.

Normalmente são estes mesmos agentes públicos desonestos que ficam de posse dos títulos falsos para "*venderem votos*" durante as eleições.

Os autores deste livro, em suas andanças por cartórios eleitorais em todo Brasil, tiveram oportunidade de várias vezes verem, guardados em gavetas ou caixotes, títulos eleitorais em branco já assinados pelos juízes "*para descomplicar a emissão dos títulos de novos eleitores*". É uma situação onde só falta um passo para a fraude acontecer.

Os que pensam que eleitores fantasmas só existem em pequenos e afastados rincões, se enganam. A partir de 1998, graças a um fabuloso trabalho de coleta de provas por Douglas Rocha e José Roberto Rocha, então membros do PPS de Camaçari na Bahia, ficou comprovado que milhares de eleitores fantasmas haviam votado em eleições naquela cidade, que é um município bem grandinho, pólo industrial bem próximo da Capital e segundo maior orçamento municipal da Bahia.

Nos grossos volumes de provas colhidas tinha até fotos de lápides em cemitérios gravadas com os nomes de eleitores que votaram anos após sua própria morte!

Para se limpar este cadastro fictício de eleitores, foram necessários três recadastramentos, pois até estes eram fraudados[39] pelos mesmos agentes internos corruptos que controlavam o Cartório Eleitoral.

As urnas eletrônicas, utilizadas excepcionalmente como máquinas de recadastramento naquela ocasião, facilitaram enormemente o repique da fraude. Chegou-se a encontrar dezenas de casos de eleitores fantasmas recadastrados em ordem alfabética à taxa de cinco a seis por minuto[40].

Num dia em que compareceram pouco mais de 100 eleitores para o recadastramento, mais de 700 foram recadastrados fraudulentamente. Durante a correição promovida pelo TSE em 2002, chegou-se a encontrar 1.300 eleitores fantasmas como moradores em um único endereço de uma casa.

Colocar a foto nos Títulos de Eleitor em muito ajudaria a dificultar esta fraude, pois o eleitor, que fosse apresentar o título ao mesário e ao fiscal, teria ao menos que ter alguma semelhança com a foto.

Mas, para isto, é necessário mudar a Lei 7.444/85 que explicitamente desobriga o eleitor de fornecer sua foto ao cadastro eleitoral. Com a quase completa paralisia, que já dura anos, do Congresso Nacional pelo trancamento de pauta por medidas provisórias do Poder Executivo, *não se deve esperar a volta da foto do eleitor para breve.*

Outra tentativa de solução idealizada pelo TSE, anunciada em abril de 2005, era acoplar recursos de biometria às urnas eletrônicas. O projeto inicial era recolher as impressões digitais de 120 milhões de eleitores e colocar leitores de impressão digital em 400 mil urnas eletrônicas. Pareceu bom para muitos fiéis do Santo Baite que ainda esperam tecnologias mágicas para resolver problemas de segurança.

Mas uma análise mais detalhada do processo revelou que era apenas mais uma forma de gastar muito dinheiro e continuar com o problema de segurança inicial quase intacto.

Pessoas poderiam ter até 10 títulos diferentes, um para cada dedo da mão, e ainda poderiam ter títulos extras, com nenhum dedo

39. Ver detalhes em: *http://www.votoseguro.org/textos/camacari1.htm*
40. Ver em: *http://www.votoseguro.org/textos/camacari1.htm#4a*

registrado, bastando apresentarem-se como "*sem-digitais*" (mãos enfaixadas, por exemplo) no cadastramento.

A defesa verdadeira contra Eleitores Fantasmas, como sempre, é a boa fiscalização. Mas neste caso tem eficiência variável dependendo muito da persistência dos fiscais eleitorais que devem atuar em dois momentos: a) no cadastramento, para impedir a inclusão dos fantasmas; e b) na votação, para impedir que os fantasmas votem.

É necessário credenciar fiscais permanentes, mesmo fora de período eleitoral, junto aos Cartórios Eleitorais para, valendo-se dos direitos de fiscalização determinados pelos artigos 27 e 28 da Resolução TSE 21.538/03, acompanharem e examinarem os documentos relativos aos pedidos de alistamento, transferência, revisão, segunda via e revisão de eleitorado.

Como se trata de ato de fiscalização continua junto ao Cartório Eleitoral, é muito importante que se procure desenvolver relação de convivência amistosa, mas não de confiança cega, com o juiz eleitoral. Procurar estabelecer regras claras e transparentes para o acesso à documentação e aos relatórios informatizados do cadastro, inclusive verificando se o número de novos eleitores confere com o de pedidos e de documentação pessoal apresentada.

A atuação persistente nos Cartórios, para impedir que os fantasmas surjam, é importante porque, na outra ponta da fraude, para se impedir que os fantasmas votem, pode ser complicado.

Normalmente, as pessoas portando títulos de eleitores fantasmas votam dez, vinte vezes a cada eleição, mas apenas uma vez em cada Seção Eleitoral, de forma que os fiscais nas seções, em virtude dos títulos sem foto, ficam sem elementos para desconfiar de determinado eleitor.

3.3 Fraudes na Votação

Clonagem de Urnas-E

Clonagem de urnas talvez não seja um termo preciso para designar esta fraude, mas tem apelo e por isto pegou.

A fraude consiste em trocar as urnas eletrônicas verdadeiras, preparadas com o programa original e oficialmente registradas nas Tabelas de Correspondências Esperadas por outras urnas, também verdadeiras e também preparadas com o programa original, mas não registradas nas Tabelas de Correspondência.

A preparação das Urnas-E não registradas é possível a partir de cópias idênticas – daí o nome clonagem – dos *Flashs de Carga*[41], que são tiradas em qualquer computador equipado com leitor de cartões tipo *flash-card*.

As Urnas-E não registradas serão levadas às Seções Eleitorais para receberem os votos dos eleitores verdadeiros.

As Urnas-E registradas oficiais são levadas a um outro local onde, no momento oportuno, são carregadas com votos falsos, gerando uma documentação oficial (Zerésima, Boletins de Urna e Disquete) que serão aceitos sem problemas pelo Sistema de Totalização, burlando todos os seus bloqueios lógicos e criptográficos.

O último passo da fraude é trocar a documentação produzida nas Seções Eleitorais pela documentação falsa produzida com as urnas registradas.

Esta Fraude de Clonagem de Urnas-E que, como todas as demais fraudes contam com a omissão dos fiscais, é perfeitamente possível, mas necessita da participação ativa dos funcionários do Cartório Eleitoral que controlam a logística de distribuição das Urnas-E e a coleta da documentação na totalização.

A história de fraudes anteriores ao voto eletrônico comprova que existiam elementos corrompidos dentro dos Cartórios Eleitorais que

41. Flash de Carga é o nome de cartões de memória, tipo flash-cards, usados para a carga dos programas oficiais nas urnas eletrônicas.

viabilizavam a troca de urnas e o mapismo[42]. É difícil crer que tais elementos deixaram de existir agora só porque o voto foi informatizado.

Existem duas variações nas escolhas das urnas que substituirão as registradas.

Pode-se usar a mesma Urna-E duas vezes:

1. Carregam-se Urnas-E sem a presença de fiscais;
2. Registra-se esta carga nas Tabelas de Correspondência;
3. Adianta-se a data das urnas para iniciar a votação;
4. Introduzem-se os votos desejados para gerar a documentação falsa;
5. Só então, convocam-se os fiscais para assistirem a uma nova carga de urnas feitas com *flash de carga* clonados. Estas urnas serão levadas às Seções Eleitorais, mas terão seus resultados verdadeiros trocados pelos falsos.
6. Se quiser sofisticar e limpar vestígios, o fraudador apaga dos arquivos de eventos[43] as referências a eventos que possam indicar a fraude como a carga não registrada, o reajuste da hora para votação antecipada, etc.;

Outra alternativa é usar Urnas-E diferentes quando há quantidade disponível[44]. Algumas urnas-E são carregadas na frente dos fiscais sem se registrar suas correspondências e serão levadas às Seções. Outras são carregadas à parte, para serem registradas como as válidas e para produzirem a documentação falsa a ser trocada.

---

42. Mapismo era uma modalidade de fraude muito praticada em eleições com apuração manual dos votos. Consistia em modificar os Mapas de Urna onde eram registrados os resultados da apuração.

43. Arquivo de eventos, ou arquivo de log, é o nome de arquivos digitais onde são registrados a data e hora de eventos controlados de um sistema. No sistema eleitoral há os arquivos de log das Urnas-E, os do Sistema de Geração de Mídias e os de Totalização.

44. As urnas-e são distribuídas em função da quantidade de seções eleitorais de cada local. Depois, seções com poucos eleitores são agrupadas, sobrando urnas-e. Outro exemplo: na eleição renovada em Campos de Goytacases, RJ, em março de 2006, havia 1300 urnas-e disponíveis no Pólo de Carga, mas apenas 780 seções eleitorais.

A única defesa eficiente contra esta fraude é a coleta dos Boletins de Urna (BU) **no momento em que são impressos nas Seções Eleitorais**. De nada adianta receber cópia do BU entregue ao Comitê Interpartidário no Cartório Eleitoral, pois, apesar das negativas da propaganda oficial, este já poderá vir trocado.

Por isto, deve ser repelida qualquer tentativa de Juízes Eleitorais que, alegando economia de papel ou de trabalho, sugiram entregar cópia do BU apenas no Cartório.

É tão importante ter acesso ao BU nas Seções Eleitorais que é bastante recomendado, inclusive, tomar medidas preventivas para garantir o seu recolhimento, como enviar previamente ofício aos Juízes das Zonas Eleitorais, comunicado que o Partido irá recolher os Boletins de Urna diretamente nas Seções Eleitorais de acordo do Art. 68 da Lei. 9.504/97.

Para as eleições de 2006 surgiu mais um forte empecilho para os partidos poderem se defender da Clonagem de Urnas-E.

Em mais um evidente exemplo de abuso de poderes, onde o fiscalizado manda no fiscal, o TSE em decisão unilateral emitiu em março de 2006 a Resolução 22.154/06 em cujo artigo 42 restringe a entrega de cópias de BU impressos aos fiscais dos partidos nas Seções Eleitorais.

Em 2004, os fiscais de partido tinham disponíveis 9 cópias do BU para compartilharem. Agora, pela nova norma de 2006, os presidentes da mesa só entregarão *uma única via* do BU impresso a um representante do Comitê Interpartidário e mais nenhuma aos fiscais de cada partido.

O problema não é falta de papel para imprimir BU, porque o TSE decidiu ainda que representantes da imprensa tenham disponíveis até 4 vias do BU para retirarem nas seções eleitorais se quiserem. Enfim, não se consegue vislumbrar nenhum outro objetivo desta nova norma do TSE além de se querer dificultar a fiscalização dos partidos.

Como este Art. 42 da Res. TSE 22.154/06 conflita diretamente com o Art. 68 da Lei 9.504/97, um partido político, o PDT, iniciou contatos com o TSE visando reverter a restrição à distribuição de cópias de BU impresso.

Não se sabe se até as eleições este quadro, tenebroso para a fiscalização, será corrigido. Se não for, restará aos fiscais dos partidos apresentarem-se como jornalistas para tentar obter uma das cópias do BU destinadas a estes.

É humilhante e indigno este comportamento a que o fiscal eleitoral terá que se submeter para defender a sociedade de fraudes eleitorais, mas será o necessário em vista da situação criada por causa do acúmulo de poderes da Justiça Eleitoral.

Como o recolhimento de BU pode falhar, por restrição oficial, por falta de fiscais ou por intimidação destes pelos mesários, pode-se tentar detectar a Clonagem de Urnas nos registros do sistema onde provas poderão aparecer, como:

a. a data e hora da carga da Urna-E registrada na Tabela de Correspondência Esperada que não será a mesma da carga feita na frente dos fiscais[45];
b. o arquivo de eventos (log) da urna carregada duas vezes, acusará este fato[46].

Mas 99.999…% dos fiscais dos partidos ignoram totalmente a existência destes recursos de auditoria que muitas vezes podem indicar fraudes. Raríssimas vezes comparecem à Cerimônia de Geração das Mídias, que nem sabem para o que serve, ou à Cerimônia de Carga e Lacração das Urnas, e quando comparecem nem percebem o risco do monte de cartões *flash-cards* que entram e saem dos bolsos de funcionários temporários que não conhecem.

Praticamente nunca solicitam, no momento correto, os dados de controle do sistema. Por exemplo, de nada adianta receber cópias das Tabelas de Correspondência Esperadas depois das eleições totalizadas, pois, se tiver ocorrido a Fraude de Clonagem de Urnas, estas tabelas também poderão ser adulteradas, depois da totalização, para esconder a fraude.

---

45. A não ser que, numa sofisticação incomum, a carga extra das urnas seja feita simultaneamente em outro local.
46. A menos que, num cuidado extra, o fraudador apagar, dos Flash Cards Internos das Urnas-E, o arquivo de eventos com a carga falsa registrada.

Um exemplo desta situação é o Caso Guarulhos, um grande município do Estado de São Paulo. Nas eleições de 2004, os Boletins de Urna não foram recolhidos como deviam. Depois das eleições, diante de resultado que contrariava as pesquisas, iniciou-se a garimparem dos arquivos do sistema. Na realidade houve, primeiro, que se dispender um bom tempo para treinar os fiscais sobre o que poderia ser procurado.

O resultado da procura foi apresentado num relatório[47] que aponta inúmeras inconsistências nos arquivos de eventos analisados, como *a carga de urnas-e diferentes com o mesmo cartão flash-de-carga no mesmo instante*. Esta situação é fisicamente impossível e só se explica pela duplicação dos *flash-de-carga*, primeiro passo para a clonagem de urnas.

Voto de Cabresto Pós-Moderno

O voto de cabresto é uma modalidade de fraude eleitoral de natureza psicológica, onde alguém procura coagir eleitores desprotegidos a votar em determinado candidato, sob o argumento de que quebrará o sigilo do voto podendo identificar em quem o eleitor votou.

No sistema de votação tradicional existia uma forma muito difundida de se conseguir quebrar o sigilo do voto de eleitores intimidados. Era chamado de voto-carreirinha e se valia do fato do eleitor depositar seu voto em papel nas urnas.

Consistia em fazer que cada eleitor levasse consigo uma cédula oficial já preenchida quando entrasse para votar, a depositasse na urna e trouxesse sua cédula vazia para fora da seção eleitoral. A primeira cédula para dar partida no processo era obtida com um mesário conivente.

A técnica para impedir esta fraude era numerar as cédulas externamente, de 1 a 5 por exemplo, dá-las em seqüência aos eleitores e verificar se este depositava a mesma cédula que recebeu. Mas não era uma prática que a Justiça Eleitoral impunha aos mesários

47. Ver em: *http://www.votoseguro.org/textos/guarulhos04.pdf*

de forma que a fraude persistiu até que, com a adoção das urnas eletrônicas, o eleitor deixou de depositar o voto em urnas de lona, desarticulando o esquema.

Esta qualidade das urnas eletrônicas foi muito utilizada na sua propaganda: ela teria acabado com o voto de cabresto.

Também foi utilizado como argumento pelo TSE para pressionar os senadores a modificar um projeto de lei que tornava obrigatório o uso de Urnas-E Reais no Brasil. Dizia-se que, com o voto impresso nas mãos dos eleitores, voltaria a possibilidade do voto-carreirinha.

A solução dada pelo Sen. Romeu Tuma, relator do projeto de lei, para impedir o voto-carreirinha em Urnas-E Reais, foi a de que o voto impresso seria mostrado ao eleitor através de um visor transparente e, depois de confirmado pelo eleitor, seria depositado automaticamente numa sacola acoplada à Urna-E, sem que o eleitor pudesse manuseá-lo.

Mas, será que a Urna-E Virtual brasileira acabou mesmo com o voto de cabresto?

Não acabou, pois o agente coator não precisa de fato conseguir quebrar a sigilo do voto do eleitor coagido, basta que consiga convencê-lo de que conseguiria, daí a natureza psicológica desta fraude.

E, neste aspecto, o método de liberação do voto nas nossas urnas eletrônicas, que consiste em **se digitar o número do Título do Eleitor na mesma máquina e no mesmo momento em que o eleitor digita o seu voto**, ajuda muito a se difundir a idéia de que o voto poderá ser identificado posteriormente.

Já na segunda eleição com urnas eletrônicas, em 1998, surgiu forte boato entre os funcionários de empresas estatais do Rio Grande do Sul de que a digitação do número do título simultânea à digitação do voto seria usada para identificar os funcionários públicos que não votassem na chapa da situação.

Era uma modalidade nova de golpe eleitoral que chegou com a urna eletrônica: o voto de cabresto em massa.

Tão grave chegou a ser a situação antes das eleições que o TRE-RS teve que apresentar repetidos esclarecimentos pela imprensa[48], tentando desconvencer os eleitores intimidados pelo boato.

Não se sabe avaliar como o conflito psicológico interno, entre o boato e o contra-boato, se resolveu nas mentes dos eleitores.

Mas a situação do voto de cabresto pós-moderno piorou muito em 2003 com a aprovação ligeira e ilegítima da Lei 10.740/03, a Lei do Voto Virtual às Cegas[49], sob o rolo compressor da Justiça Eleitoral que conseguiu impedir seu debate ou emenda.

A lei acabava com a auditoria automática da apuração dos votos nas urnas eletrônicas a ser efetuada a partir das eleições de 2004 por meio do voto impresso conferido pelo eleitor.

Não tendo absolutamente nada a oferecer em troca do fim da auditoria da apuração, o TSE procurou seduzir os parlamentares com a invenção do *Registro Digital do Voto,* inútil para a fiscalização, que permitiria aos políticos desenvolverem ***estudos de correlação***, para determinar como os eleitores combinaram os seus votos nos diversos cargos, se as coligações foram respeitadas pelo eleitor, etc.

O Registro Digital do Voto nada mais é que o conjunto dos votos de cada eleitor escrito numa linha de um arquivo digital que é gravado em 3 vias nas memórias da Urna-E.

Assim que a lei foi aprovada, Jorge Stolfi, Professor Titular do Instituto de Computação da UNICAMP, anunciou como a possibilidade dos tais "*estudos de correlação*" também viabilizava a identificação do voto de eleitores coagidos. Era, exatamente, uma versão informatizada do voto de cabresto, que ressurgia com a nova lei.

Nesta próxima eleição de 2006, o Voto de Cabresto Pós-Moderno pode ser aplicado, por exemplo, por um candidato a deputado federal que queira garantir os votos de eleitores sobre os quais tenha poder de pressão psicológica, com os seguintes procedimentos:

---

48. Reportagem *"Justiça Eleitoral Garante Sigilo do Voto"*, Jornal ZeroHora, 23/10/1998 - pág. 20.

49. Ver mais em: *http://www.votoseguro.org/textos/PLazeredo.htm*

1. O agente coator escolhe candidatos inexpressivos, que terão poucos votos, para presidente, para governador, para senador e para deputado estadual. É sempre possível se conseguir um punhado de candidatos a deputado que com certeza não terão votos em determinada região;
2. Com estes nomes, monta combinações incomuns de votos, todas diferentes entre si. Isto é possível com uma boa escolha de deputados sem voto;
3. Copia, em duas vias, estas combinações diferentes e inclui o seu próprio nome no cargo ao qual concorre;
4. Entrega uma via com uma relação diferente para cada eleitor coagido. Como o TSE estimula o uso de "*colas*", nada chamará atenção dos fiscais. Na segunda via da cola, anota o nome do eleitor e guarda;
5. Após a eleição, basta obter acesso ao arquivo com os Registros Digitais dos Votos, que estarão gravados em inúmeros locais, como nos cartões de memória interno e externo das urnas eletrônicas, nos disquetes que ficam nos cartórios e nos computadores da rede. Este arquivo também poderá ser impresso pela própria Urna-E com o uso de um disquete especial chamado SIBVD[50].
6. No arquivo, os conjuntos com os votos de cada eleitor estarão em linhas embaralhadas, mas poderão ser localizados pelas combinações incomuns, pois dificilmente haverá outra combinação igual no mesmo arquivo;
7. Se alguma combinação esperada, faltar, pune-se o respectivo eleitor.

---

50. SIBVD – significa *Sistema de Impressão do Boletim do Voto Digital*. É um programa disparado por um disquete especial que imprime a relação de todos os votos dados naquela urna. A inutilidade deste disquete SIBVD para qualquer outra função além de facilitar o voto de cabresto pós-moderno, levou o PDT a peticionar a sua exclusão do rol de programas instalados nas Urnas-e. A exclusão será decidida pelos mesmos que idealizaram o programa questionado.

Depois que o prof. Stolfi anunciou este roteiro que explora falha de segurança criada pela Lei do Voto Virtual, o TSE tentou contornar o problema que criou e, pela Resolução 21.744/04, decidiu dificultar os "*estudos de correlação*" que prometera aos parlamentares, decidindo manter secretos todos os arquivos de votos digitais (uns 2 milhões de arquivos) espalhados pelo Brasil. Se vai conseguir mantê-los todos secretos, sem vazamentos, não se sabe.

E, para que criar zilhões de cópias de arquivos perigosos, que podem permitir a violação de votos, só para mantê-las obrigatoriamente secretas, também não se sabe.

Mesmo que o coator não consiga acesso ao arquivo de votos, ainda assim poderá coagir se convencer os eleitores de que obterá o acesso.

Uma outra conseqüência perversa do Voto de Cabresto Pós Moderno é que candidatos de votação antes inexpressiva começarão a ganhar vários votos inesperados em locais em que nem são conhecidos, distorcendo a Verdade Eleitoral. Quando a incidência desta fraude aumentar, e sob a vigência da Lei do Voto Virtual é inevitável que aumente, alguns candidatos até poderão vir a ser eleitos com os votos recebidos em locais inesperados.

Não existem defesas eficazes contra esta fraude, tamanho foi o estrago na fiscalização eleitoral causado pela Lei do Voto Virtual, cujo autor oficial, Sen. Eduardo Azeredo, cumpriu rigorosamente a vontade dos autores verdadeiros, funcionários do TSE. Em pronunciamento no plenário em 22 de julho de 2003, o Sen. Azeredo revelou desconhecer a finalidade do próprio projeto de lei que, ainda assim, foi aprovado sem debates públicos ou emendas, sob forte pressão dos ministros do TSE.

Os fiscais terão que tentar convencer eleitores coagidos a denunciar o esquema. Mas tudo ficará num bate-boca inócuo.

Compra de Votos

Compra de Votos é o nome genérico dado a muitos esquemas, nem sempre iguais, que visam pagar eleitores para que votem em determinados candidatos.

É pratica coibida por lei que pode resultar, se comprovada, na cassação e perda de direitos políticos do eleito.

A compra simples e direta do voto, dando dinheiro a um eleitor que promete votar, é muito arriscada. O eleitor pode receber o dinheiro e não votar no candidato combinado.

Assim, alguns esquemas mais complexos acabam sendo elaborados.

Um deles é uma variante do voto de cabresto pós-moderno, no qual após identificar o voto do eleitor no candidato determinado, se paga a quantia combinada. As pequenas dificuldades deste esquema são: a) obter acesso ao arquivo dos votos digitais depois da eleição; e b) encontrar eleitores que aceitem só receber o seu dinheiro depois das eleições, pois em geral o nível de credibilidade destes candidatos é baixo.

O esquema mais freqüente parece ser o da compra ou aluguel de títulos do eleitor, que se vale do fato dos títulos não possuírem foto do eleitor, conseqüência da Lei 7.444/85 que instituiu a informatização do cadastro eleitoral.

Consiste em pagar para um eleitor entregar o seu título. No dia da votação se envia alguém de confiança para votar no lugar do eleitor comprado. Eleitores maliciosos podem até tirar segunda via do título para vendê-lo mais de uma vez.

O que se faz com o título depois da eleição é variável. Alguns devolvem para recomprar nas próximas eleições. Outros tentam reter os títulos indefinidamente para voltar a utilizá-los.

Para se defender deste esquema de compra de votos é necessário que o Juiz Eleitoral decrete a obrigação de apresentação de documento com foto pelo eleitor para poder votar. Mas esta é uma decisão radical, que cria dificuldades ao eleitor comum e, por isto, encontra bastante resistência entre os juízes.

Engravidar Urnas-E

Muito se propagandeou que, com as urnas eletrônicas, os mesários não poderiam mais colocar votos nas urnas, mesmo quando os fiscais estivessem ausentes, pois a urnas só aceitariam um voto por cada eleitor autorizado e presente.

Este argumento está totalmente equivocado, pois colocar um voto em nome de um eleitor ausente é perfeitamente possível, o que torna viável ao mesário colocar muitos votos nas Urnas-E em nome de muitos eleitores ausentes.

Em média, há 15% a 20 % de abstenção de eleitores, em nome dos quais se pode introduzir votos que "*engravidam a urna*".

A fraude pode ser feita da seguinte forma:

1. Mesários desonestos agindo em conluio;
2. Momento em que não há eleitores votando, muito comum no final de tarde, antes das 17 h;
3. Fiscais desatentos ou ausentes (sempre contribui a falha do fiscal);
4. Um conhecido dos mesários, ou mesmo um deles, fica em frente à Urna-E;
5. Outro mesário vai digitando no seu microterminal os números dos eleitores que ainda não vieram votar, para liberar a urna para receber mais um voto. Os números válidos são obtidos na Folha de Votação impressa que, por lei, o mesário possui;
6. Aquele que está defronte à urna digita o voto para os candidatos desejados, completa a votação e aguarda a nova liberação;
7. Na eventualidade de aparecer um eleitor em nome do qual já foi depositado um voto, basta ao mesário digitar o número do eleitor seguinte na Folha de Votação que o eleitor poderá votar sem maiores problemas.

Este tipo de fraude, de baixa tecnologia, é sucessora de fraude similar no sistema de voto manual e tem pequeno alcance, pois só afeta os votos de uma seção eleitoral. Mas já é de conhecimento de muitos mesários que normalmente são chamados a trabalhar em seguidas eleições e vão descobrindo como burlar a segurança.

Uma curiosidade é que até mesmo mesários simpáticos a candidatos diferentes de partidos concorrentes podem vir a estabelecer o conluio, aceitando colocar um voto de cada vez para cada candidato. Os demais candidatos é que serão prejudicados.

Isto tudo traz duas conseqüências negativas: 1) a quantidade de fraude aumenta a cada eleição; e 2) o número oficial de abstenções é falsamente diminuído.

Dificilmente um presidente ou governador será eleito por Urnas-E emprenhadas desta forma, mas, em determinadas situações, vereadores e deputados podem conseguir ser eleitos.

Ao final do livro *Plim-Plim*[51], o jornalista Paulo Henrique Amorim cita o Caso de Caruaru, Pernambuco, em 2004, onde mais de 50% dos mesários foram substituídos nas vésperas da eleição e houve inversão dos resultados em seções onde a taxa de abstenção foi abaixo da média, sugerindo que urnas foram engravidadas.

A má vontade da Justiça Eleitoral em apurar as irregularidades ocorridas em suas próprias entranhas, conseqüência natural do acúmulo de seus poderes, fez com que na primeira e segunda instância fossem rejeitados pedidos de conferência das assinaturas dos eleitores nas Folhas de Votação. Passado um ano, o caso subiu ao TSE.

Mas que solução este poderia dar?

Se analisarem os arquivos de eventos (*log*) das Urnas-E, periciarem as assinaturas nas Folhas de Votação e confirmarem que eleitores fantasmas emprenharam as urnas, como anular seus votos sem anular também uma quantidade maior de votos válidos de eleitores legítimos?

As urnas eletrônicas introduziram algumas dificuldades para esta fraude, como o tempo para inserir um voto falso que é um pouco maior (10 a 15 segundos) e ainda tocam um sonoro "*pililim*" quando o voto é completado, podendo acordar um fiscal que porventura esteja dormindo de tédio, mas nada que impossibilite a fraude.

---

51. Amorim, P.H. e Passos, M.H. – "*Plim-Plim, A Peleja de Brizola Contra a Fraude Eleitoral*" – Conrad Livros, São Paulo. 2005.

Analisar os arquivos de eventos das urnas eletrônicas, dos quais os fiscais podem solicitar cópias depois das eleições, pode indicar a ocorrência desta fraude, já que registram o instante em que cada voto é confirmado.

Um programa de análise de freqüência do voto pode rapidamente indicar em que seções houve uma mudança de freqüência (votos muito rápidos) fora do padrão. Mas esta análise não serve de prova definitiva da fraude. No município de Marília no Estado de São Paulo, em 2004, a análise apresentada em um recurso[52] foi simplesmente ignorada pelo juiz eleitoral que acatou a falaciosa explicação de técnicos do TRE-SP de que a votação anormalmente rápida também ocorrera em outros municípios!

Acoplar a leitura da impressão digital do eleitor às Urnas-E também não resolve. Como a leitura de impressão digital pode falhar por dezenas de motivos e como não se pode impedir eleitores legítimos de votar, ter-se-ia que fornecer ao mesário uma forma de liberar a urna para o voto, retornando ao problema inicial que é causado pelo mesário desonesto que libera a urna indevidamente.

Assim, a melhor e bastante eficaz defesa contra Urnas-E grávidas é ter fiscais alertas, treinados e descansados em todas as seções eleitorais, durante todo o período de votação das 08 h às 17 h, principalmente depois das 15 horas quando começa a rarear o número de eleitores. Não precisa de alta tecnologia, mas é o que funciona.

O Eleitor Anulado

Outra fraude de mesários, que surgiu com o advento das urnas eletrônicas, é a *possibilidade de anularem os votos de eleitores demorados.*

Este problema *não existia no sistema manual de votação*, quando um eleitor lento poderia ficar quanto tempo quisesse preparando o seu voto sem atrapalhar os demais, que continuavam votando em paralelo.

52. Ver mais em: *http://www.votoseguro.org/arquivos/marilia2004.zip*

Mas as Urnas-E, equipamento caro se considerar que se precisa de mais de 400 mil, só permitem que um eleitor vote de cada vez. Um eleitor lento segura toda a fila de eleitores.

Um projeto para adoção de uma segunda Urna-E nas seções eleitorais chegou a ser iniciado no TSE, mas acabou abandonado devido a dificuldades de sincronizar a relação de eleitores que votaram, para evitar que um eleitor conseguisse votar nas duas urnas, e também ao alto custo da votação eletrônica que quase dobraria.

Então, para contornar este problema dos eleitores lentos, o TSE adotou o critério de dar um pouco mais de um minuto para o eleitor completar o seu voto a todos os cargos. São cinco os votos que cada eleitor terá que dar nesta eleição de 2006.

Caso o eleitor não consiga completar todos os seus votos neste prazo, *o mesário pode*, através da digitação de uma senha em seu terminal, *anular os votos que faltarem do eleitor demorado*, encerrando a votação daquele eleitor para desobstruir a fila. Os votos nos cargos que já tiverem sido confirmados pelo eleitor não serão anulados.

Como o critério de anular ou não os votos restantes de um eleitor lento é de exclusiva decisão do presidente da mesa depois de constatada a demora, este pode anular votos de eleitores que achar que irão votar contra seu candidato majoritário preferido.

É uma fraude de baixo alcance, normalmente de iniciativa do próprio mesário, mas é possível e, sem dúvida, ocorre. Se muitos mesários forem simpáticos ou cooptados pelos partidários de um mesmo candidato, seus concorrentes poderão ser prejudicados.

A defesa é a mesma do caso anterior: fiscais atentos nas seções eleitorais.

Mas a eficácia da defesa é menor neste caso. Como o critério para anular o voto é pessoal do presidente da mesa, fica difícil impedi-lo. Uma vez que ele tenha anulado os votos restantes de um eleitor, não se poderá voltar atrás e o eleitor não poderá mais completar o voto.

O Golpe do Candidato Nulo

É um golpe barato e escandaloso, que pode ser revertido por medidas judiciais, mas como a burocracia, os atos procrastinatórios e a conhecida lentidão dos processos jurídicos podem retardar muito a reversão, os seus beneficiários podem acabar ficando no poder por muito tempo antes de o devolverem a quem de direito.

Consiste em apenas convencer o técnico responsável por editar o arquivo de candidatos, a "*esquecer*" de incluir o nome e número de um dado candidato e, passar a contar com a absoluta omissão dos fiscais concorrentes para não perceberem o truque armado.

Para candidatos em eleições proporcionais, é uma fraude que pode passar despercebida facilmente até o dia da eleição, como aconteceu no citado Caso de Araçoiaba da Serra[53]. Os beneficiários do erro exerceram o mandato de vereador por mais 3 anos até serem destituídos sem nenhuma outra pena adicional.

Para candidatos de eleições majoritárias é mais difícil de não ser percebida a tempo de ser revertida, como ocorreu recentemente nas eleições renovadas na cidade de Campos de Goytacases, RJ.

Nova eleição para prefeito ocorreu em Campos, em 12 de março de 2006, em virtude da anulação da eleição de 2004. A propaganda política corria solta com cinco candidatos. Para o candidato que estava em primeiro lugar nas pesquisas podia interessar transformar votos válidos em votos nulos, o que diminuiria a quantidade de votos de que precisaria para se eleger no 1º Turno.

Os autores deste livro, chamados para treinar a fiscalização do candidato que estava em segundo lugar nas pesquisas, mobilizaram os demais candidatos, que nem tinham idéia do que seria fiscalizar voto eletrônico, e juntos compareceram à cerimônia de carga das urnas, ocorrida cinco dias antes da eleição, para fazer o que não havia sido feito no Caso de Araçoiaba: conferir a lista de candidatos nas urnas-e. Constatou-se que o candidato que estava em terceiro lugar

53. Ver mais em: *http://www.jus.com.br/doutrina/urnael19.html*

nas pesquisas, com 15% das expectativas de voto, não tinha seu nome entre os candidatos na Zerésima.

Se o erro não tivesse sido detectado, como não seria se os fiscais não estivessem lá, os votos que eleitores tentassem dar ao candidato ausente seriam anulados pela própria urna eletrônica, aumentando muito a possibilidade de eleição do primeiro candidato já no 1º Turno.

Curiosamente o erro persistiu ainda numa segunda cerimônia de carga, no dia seguinte, quando o nome do vice de um candidato apareceu trocado, o que ensejaria novas anulações. Somente uma terceira carga das urnas, na antevéspera da eleição regularizou tudo.

Houve segundo turno.

Assim, a defesa 100% eficaz contra o Golpe do Candidato Nulo, é comparecer às cerimônias de carga das urnas eletrônicas que, pela regulamentação, são públicas e obrigatórias.

Neste caso surge a real utilidade da Zerésima. Ela não serve, de forma nenhuma, como garantia de que não há votos escondidos nas urnas-e como se verá na Fraude de Adulteração dos Programas, mas serve como prova de que os nomes de todos os candidatos estão regularmente carregados. Ela deveria ser chamada apenas de Lista de Candidatos e não de Zerésima, porque induz a erro de compreensão de sua função.

Olhar a Zerésima e ver apenas o que de fato ela é, uma lista de candidatos com o número zero impresso ao lado, é um exercício psicológico que os fiscais eleitorais precisam praticar. Só assim se escapa da ilusão criada pela mistificação dos fiéis da Seita do Santo Baite que costumam endeusar a Zerésima apresentando-a como se fosse uma prova cabalística da confiabilidade do sistema.

O Candidato de Protesto

O voto de protesto é uma expressão popular. Existe.

Nas antigas eleições manuais, o voto de protesto se dava pela descarga de votos num ***alvo peculiar***, como o rinoceronte Cacareco em São Paulo ou o macaco Tião no Rio de Janeiro. O protesto do

eleitor podia também ser expresso por meio de palavras ofensivas escritas nas cédulas eleitorais.

Todos estes votos eram anulados pelos juízes eleitorais e o efeito do voto de protesto no resultado eleitoral era apenas o de aumentar a quantidade porcentual de votos nulos.

As Urnas-E utilizadas no Brasil foram projetadas de forma muito rígida quanto às possibilidades de interação com o eleitor. Um limitado teclado, de apenas 10 teclas numéricas e outras 3 teclas específicas, é deixado para o eleitor se manifestar.

Por isto, houve dificuldade para muitos eleitores no Referendo de 2005. Simplesmente não havia teclas SIM e NÃO para o eleitor responder à pergunta apresentada no visor.

Urnas-E mais modernas, como as usadas nos EUA, no Canadá e na Venezuela, com o sistema *touch-screen* de teclado variável, dão mais flexibilidade para a expressão do eleitor.

Esta limitada interação das Urnas-E brasileiras com o eleitor, que não consegue mais escrever um palavrão ou votar no Cacareco e não se satisfaz em digitar ZERO-ZERO e CONFIRMA, levou-os a conceber uma nova forma de expressar seu voto de protesto: votar em ***Candidatos Peculiares*** que de alguma forma simbolizem sua angústia.

O exemplo inegável deste novo fenômeno cultural-eleitoral é a enorme votação do candidato Enéas para deputado federal no Estado de São Paulo, em 2002. Sua figura marcante, seu tom agressivo ao falar e sua propaganda peculiar[54] atraíram o voto de eleitores descontentes, que em outras eras recorriam ao voto de protesto.

O Dep. Enéas obteve a maior votação de um deputado federal de todos os tempos no Brasil. Quase 1,6 milhões de votos, o quádruplo do segundo colocado, 8% dos votos do maior Estado do Brasil.

---

54. A propaganda do candidato Enéas sempre se caracterizou pela frase: "*Meu nome é Enéas*", dita de forma incisiva e repetida com insistência no minúsculo tempo de TV de que dispunha.

Reconhece-se a legitimidade na eleição deste candidato que soube atrair votos, mas os votos de protesto que lhe foram dados elegeram muito mais do que um deputado.

Como o coeficiente eleitoral[55] foi de aproximadamente 280 mil votos, 1,3 milhão dos votos restantes do Dr. Enéas foram transferidos para outros cinco candidatos de seu partido, PRONA. Todos com votação individual inexpressiva. Três deputados federais eleitos na carona do Dr. Enéas obtiveram menos de 500 votos diretos cada um!

Tantos foram os votos de protesto atraídos pelo Enéas que se na lista de candidatos do PRONA houvesse mais um candidato inscrito *este seria eleito mesmo que não tivesse voto nenhum*.

O Dep. Enéas sempre esteve na oposição parlamentar, fiel ao seu estilo e ao seu eleitor de protesto. Mas é tão baixo o compromisso com o eleitor dos outros deputados, eleitos na sua carona, que em poucos meses, bem no meio do troca-troca partidário alimentado pelo mensalão[56], 4 dos 5 caronistas do protesto ingênuo traíram seus eleitores e pularam para partidos da base de apoio ao governo.

Outra conseqüência desta atração de votos por candidatos de protesto é que diminui artificialmente a quantidade de votos nulos e brancos. Os 8% dos votos obtidos pelo Dep. Enéas em 2002 somados aos nulos e brancos resultam em 17,1%, muito próximo dos 19,7% de votos brancos e nulos na eleição com urnas-E anterior em 1998 quando nenhum candidato peculiar atraiu o voto de protesto.

Enfim, o voto de protesto, que antes das nossas sisudas Urnas-E apenas aumentava a quantidade de votos nulos, agora pode até eleger uma boa bancada de candidatos nulos.

Mas nada do que foi dito até aqui caracteriza fraude eleitoral.

Esta vai surgir quando, compreendendo que nossas urnas eletrônicas favorecem a concentração de votos em candidatos peculiares que atraiam o voto de protesto, um partido pressionado pela cláusula

55. É a quantidade de votos necessária para um candidato a deputado se eleger.
56. Esquema de financiamento de candidaturas, com recursos não declarados, para montar a base de apoio ao governo na Câmara Federal. Popularmente chamado de compra de votos com caixa 2.

de barreira lançar candidato deste tipo, **o Candidato de Protesto**, mesmo que seja uma pessoa absolutamente irresponsável, apenas para angariar os votos de protesto ingênuo.

E fiscalização que defenda contra este oportunismo, não há.

Está aí uma perversão inesperada trazida ao processo eleitoral pela moderna tecnologia.

Uma possível solução seria alterar o Código Eleitoral e criar a figura do *Coeficiente Eleitoral Mínino*, abaixo do qual nenhum candidato seria considerado eleito.

Ou, talvez, a solução fosse adotar a proposta do humorista Millor Fernandes e incluir nas urnas eletrônicas uma quarta tecla "***Vá a M....***" que capture a expressão de quem queira protestar, evitando-se assim que se elejam deputados e vereadores oportunistas.

3.4 Fraudes na Apuração

Adulteração dos Programas das Urnas-E

Ao contrário de Urnas-E Reais, nas quais uma auditoria estatística posterior por recontagem dos votos impressos permite se determinar tecnicamente a integridade do *software* de apuração com a margem de confiança desejada, as **Urnas-E Virtuais** usadas no Brasil, não permitem que se possa fazer auditoria da contagem dos votos. Por isto, **são extremamente dependentes da confiabilidade dos seus programas de computador** para que haja alguma garantia ao eleitor de uma justa apuração e de que não haverá violação sistemática do voto.

Mas garantir que um *software* eleitoral seja 100% confiável e, além disso, garantir que este *software* confiável é o que de fato estará carregado nas 400 mil urnas, não é tarefa trivial que possa ser efetuada apenas se assistindo a alguns espetáculos ilusionistas de emissão de Zerésima ou de autovalidação das urnas eletrônicas.

A segunda parte do Relatório Hursti[57] e o Vídeo do Paraguai[58] comprovaram, por meio de Testes de Penetração, que é possível a adulteração dos programas das Urnas-E Virtuais americanas e brasileiras, respectivamente, burlando suas defesas lógicas. Quebrou-se a esperança de fieis do Santo Baite que ainda achavam que Urnas-E Virtuais pudessem ser garantidas apenas por técnicas de assinatura digital e outras similares.

Mesmo inexistindo no Brasil relatório que seja similar aos Relatórios Hursti, porque o TSE rejeita permissão[59] para que Testes de Penetração sejam efetuados, ainda é possível descobrir as fragilidades das urnas-e brasileiras pela análise de documentos oficiais públicos, como as especificações técnicas incluídas nos editais de concorrência e laudos de perícias técnicas ocorridas dentro de processos judiciais.

Desta forma, pode-se afirmar que são muito similares as falhas de segurança das urnas eletrônicas brasileiras quando comparadas com as falhas apontadas no Relatório Hursti.

Recorrendo-se brevemente ao informatiquês, as urnas eletrônicas brasileiras:

1. Possuem *chip BIOS* (com programa inicializador) preso em soquete e regravável por *software*, como especificado nos editais de concorrência;
2. Possuem *extensão de BIOS* habilitada por "*jumper*" na placa-mãe, conforme descrito nos capítulos 3.1.1 e 4.2 do Relatório Unicamp[60], que permite a inicialização a partir do soquete externo para cartão de memória *flash-card*;
3. Possibilitam a execução de "*software batch file*" gravado em disquete conforme descrito no capítulo 4.10 do Relatório Unicamp;

57. Ver a partir de: *http://www.votoseguro.org/textos/relatoriohursti1.htm*
58. Ver em: *http://www.votoseguro.org/textos/penetracao2.htm*
59. Ver em: *http://www.votoseguro.org/textos/penetracao1.htm#5a*
60. Ver a partir de: *http://www.votoseguro.org/textos/relfuncamp1.htm*

4. Permitem a violação da verificação de integridade interna do sistema como revelado em análise do Prof. Pedro Rezende[61];
5. Possuem sistema de lacres e de fechamento do gabinete simples e permitem acesso ao soquete do cartão de memória interno, conforme descrito no laudo da perícia no município de Santo Estevão[62], BA;

Traduzindo rapidamente este conjunto de palavras estranhas do informatiquês, as urnas brasileiras são tão passíveis de fraudes por adulteração do seu programa quanto suas similares vendidas no Canadá e EUA.

Valendo-se destas fragilidades um programador capaz, que obtenha acesso físico às urnas eletrônicas nos Cartórios Eleitorais, tem muitas alternativas para adulterar seu *software* de forma que o resultado da apuração seja modificado ou que o voto seja regularmente violado numa eleição comum *mas que nada seja detectado pelos esquemas de testes utilizados*.

Por exemplo, aproveitando a possibilidade de executar programas gravados em disquetes revelada no relatório Unicamp, os funcionários temporários encarregados de efetuarem a carga das urnas podem colocar nelas um disquete previamente preparado que, logo que a urna é ligada para o teste de carga, contamine o programa básico das memórias internas e se apague imediatamente do próprio disquete. Todos os testes de integridade feitos a partir daí, como impressão das assinaturas *hashs* e votações simuladas, poderão ser burlados.

Uma outra alternativa de ataque é quando o programa adulterado só praticar a fraude de desvio de votos, se encontrar determinado *"gatilho"*, como, por exemplo, um sinal determinado incluído na foto do candidato, uma seqüência de teclas digitada por um eleitor, etc.

No caso de fraude disparada por seqüências de teclas, o programa adulterado estará automaticamente vacinado contra o teste oficial de Votação Paralela. Passará por este teste sem ser detectado.

---

61. Em: *http://www.cic.unb.br/docentes/pedro/trabs/analise_setup.html*
62. Ver em: *http://www.votoseguro.org/textos/stoestevao1.htm*

Comumente as adulterações não substituem o *software* oficial de votação atacado por outro, mas modificam o ambiente operacional interno de forma que as defesas e *verificações de integridade dos programas originais sejam burladas* sem que se de conta, como foi feito no caso do teste no Paraguai.

Por exemplo:

1. Para burlar as verificações internas de integridade dos programas instalados, pode-se reescrever a BIOS, desabilitando temporariamente os seus *jumpers* de proteção, para sempre iniciar o sistema por um programa malicioso específico que controlará o ambiente interno mantendo-se invisível às verificações de integridade e apagando as pistas imediatamente antes de encerrar a apuração. Funcionando numa espécie de *Matrix*, os programas oficiais de verificação de integridade sempre estarão rodando sob um ambiente falso, enxergando uma imagem construída para iludi-lo e nunca se aperceberão disso. *Burlam-se, assim, todas as conferências oficiais de assinaturas digitais permitidas, inclusive as feitas com os programas de verificação dos Partidos Políticos, da OAB e do Ministério Público;*
2. Para violar o sigilo dos votos, no mesmo princípio de funcionamento dos vírus de computador chamados *sniffers* que assumem o controle do teclado e roubam senhas secretas, o ambiente adulterado pode gravar todas as teclas digitadas na urna e no microterminal do mesário. Depois se pode reconstruir o voto de cada eleitor juntamente com o número de seu título de eleitor, violando sistematicamente todos os votos;
3. Para desviar votos, utilizando a mesma técnica de *envelopamento* que se valem os vírus de computador, pode-se interferir na comunicação entre o programa oficial de votação, o vídeo e o teclado do eleitor, de forma a mostrar ao eleitor o que ele espera ver (a foto do seu candidato) mas enviar ao programa apurador o número de outro candidato. No caso do teste de penetração do Paraguai, um *sniffer* foi utiliza-

do para trocar uma seqüência teclas digitada pelo eleitor[63], por exemplo, <8, CONFIRMA> por outra seqüência <8, CANCELA, 2, CONFIRMA> mas deixou-se a tela apresentar a troca para torná-la propositadamente bem visível, devido a natureza didática do vídeo;

4. Para burlar a emissão da Zerésima basta deixar o programa oficial rodar normalmente no início e somente depois iniciar o desvio de votos, como no caso paraguaio;
5. Para burlar o Teste de Votação Paralela basta não desviar voto que demorou mais de 2 minutos para ser confirmado ou só iniciar o desvio de votos a partir do 200º voto, pois, devido ao complexo rito deste teste, nunca um voto é confirmado em menos de 2 minutos e jamais se chega a simular 200 votos.

Esta lista não esgota as possibilidades do programador malicioso. O *Flash de Carga* também pode ser adulterado para inserir os programas adulterados num grupo de urnas-e em vez de se trocar os programas uma a uma.

Todas estas técnicas de adulteração de programas exigem acesso físico às Urnas-E nos Cartórios Eleitorais e programadores experientes em programação básica, linguagem Assembly, depuração de *software*, etc.

É uma fraude de alta tecnologia, de médio ou alto alcance e, se for bem feita, pode esconder pistas.

Os porta-vozes da Justiça Eleitoral insistem que nada disso é possível. Mas é muito fácil falar que o sistema é invulnerável e ao mesmo tempo impedir que seja testado.

Enquanto o TSE continuar impedindo que Testes Livres de Penetração sejam efetuados, seus membros não obtêm credibilidade moral para declarar a invulnerabilidade do sistema.

---

63. Explicação mais detalhada sobre o funcionamento da troca do voto, no teste de penetração do Paraguai, pode ser vista em: *http://www.votoseguro.org/textos/penetracao2.htm#2b*

A mais eficaz defesa contra a Adulteração de Programas em Urnas-E Virtuais seria transformá-las em Urnas-E Reais. Nestas, pela recontagem dos votos impressos conferidos pelo eleitor, se pode determinar, numa auditoria estatística, se o programa de apuração desviou ou não os votos.

Enquanto no Brasil não se adota urnas-E Reais, as defesas contra a adulteração de programas das Urnas-E necessitam de equipe de fiscais muito bem preparados, no nível técnico, e ainda assim são apenas parcialmente eficazes, podendo ser burladas por atacantes mais sofisticados. Estas defesas consistem em:

1. Acompanhar todas as cerimônias públicas oficiais de Geração de Mídias, de Carga e Lacração das Urnas, e de Oficialização do Totalizador. São em torno de 20 mil cerimônias em todo o Brasil que ocorrem num intervalo de uma semana aproximadamente;
2. Fazer a verificação das assinaturas digitais (*hashs*) permitidas nestas cerimônias, preferencialmente com o uso do Programa Verificador antecipadamente homologado pelo próprio partido junto ao TSE. Em Campos do Goytacazes, por exemplo, foi encontrado um programa diferente do oficial no computador de totalização. O sistema teve que ser reinstalado;
3. Ficar atento a qualquer sinal de comportamento inesperado dos programas testados, como telas ligeiramente diferentes, reinícios não programados, demora incomum na inicialização, "*bips*" não esperados, etc.
4. Analisar todos os arquivos disponíveis como: Tabelas de Correspondências, Arquivos de Eventos (log) e Resultados por Seção Eleitoral. São em torno de 1 milhão de arquivos em todo o Brasil que devem ser analisados em até 72 duas horas após a publicação do resultado oficial.

Deve-se ainda ter em mente que, atualmente, as verificações de assinaturas digitais, permitidas pela Justiça Eleitoral ao Ministério Público, à OAB e aos Partidos Políticos, não têm valor absoluto porque são baseadas em metodologia equivocada.

São as próprias urnas eletrônicas e computadores de totalização, nos quais se quer determinar sua integridade, que rodam os Programas Verificadores de Assinaturas Digitais e assim, se contaminados por programas maliciosos, podem simplesmente apresentar na sua tela uma simulação do teste real. Por isto, os fiscais devem procurar conhecer com minúcias as telas apresentadas pelo seu próprio Programa Verificador e procurar detectar qualquer pequena diferença que apareça na tela apresentada.

Apesar de todos estes números e condições desanimadores, enquanto não houver o voto impresso conferido pelo eleitor que permita uma auditoria da apuração mais simples e barata, deve-se fazer estas verificações de integridade que podem detectar adulterações mal feitas que tenham sido inseridas nos Cartórios Eleitorais.

Programas Descontrolados

A verificação de assinaturas dos programas das Urnas-E Virtuais, para tentar evitar que sejam adulterados nos Cartórios Eleitorais, é o segundo passo da defesa contra *software* malicioso.

Um passo anterior consiste em verificar se o conjunto dos programas foi desenvolvido corretamente sem que algum código malicioso tenha sido introduzido já na sua produção.

A inserção de código fraudulento, que desvie ou identifique votos, já na produção do conjunto de programas do sistema eleitoral, é uma fraude de alta tecnologia das mais perigosas e de largo alcance, pois:

1. Pode ser disparada por diversos gatilhos inseridos posteriormente, como as fotos dos candidatos, seqüências de teclas, disquetes preparados, etc.;
2. Pode eleger candidatos a qualquer cargo;
3. Pode se esconder das verificações de integridade e das simulações de voto;
4. Pode apagar todas as pistas digitais para não ser detectada depois das eleições.

Se aplicada com sucesso em eleições proporcionais (de vereadores e deputados) será praticamente imperceptível em análises estatísticas, podendo montar bancadas legislativas inteiras.

Em eleições majoritárias deve ser aplicada com parcimônia, pois não pode se desviar muito além das margens de segurança das pesquisas, que costumam ficar em torno de 3% para cima e para baixo.

Acompanhar a produção de todo *software* desenvolvido para o sistema eleitoral para garantir sua integridade é tarefa hercúlea e nada trivial, como foi descrito no Relatório da Sociedade Brasileira de Computação[64] quando se referiu ao acompanhamento do desenvolvimento do *software* eleitoral do ano 2002:

"Em essência, não foi possível verificar a corretude dos programas-fonte e a versão compilada produzida pelo TSE, apesar de termos acompanhado o trabalho dos técnicos do TSE, solicitado explicações, visto os códigos-fonte, etc.

... Na hipótese de que alguém tivesse colocado algo suspeito, a probabilidade de um terceiro descobrir isto durante nossas sessões no TSE é quase zero. A segurança e corretude dos programas usados na urna baseiam-se em confiar na boa fé dos técnicos do TSE."

Sem dúvida, este ataque é mais facilmente implantado por programadores internos desonestos que, tendo acesso privilegiado, incluam os programas viciados sem que os auditores externos percebam.

Mas também agentes externos podem tentar este tipo de ataque, pois criatividade aos *hackers* não falta. Um exemplo de ataque externo bastante sofisticado:

a. Pode-se desenvolver vírus de computador inoculados em páginas virtuais de interesse de funcionários da Justiça Eleitoral, que fiquem adormecidos em computadores comuns, mas que se ativam ao detectarem estar em computadores da Justiça Eleitoral que farão a compilação[65] dos programas da eleição;

64. Ver em: *http://www.votoseguro.org/textos/relatoriosbc1.htm*

65. Transformação do código-fonte para código executável que é entendida pelos microprocessadores dos computadores.

b. Uma vez ativados, podem adulterar os programas compiladores[66], deixando os códigos-fontes[67] originais intactos, de maneira a infectar as programas finais compilados.

Tudo isto pode passar despercebido pelos auditores externos e também pelos próprios funcionários da Justiça Eleitoral.

O acompanhamento do desenvolvimento do *software* eleitoral se inicia no mês de abril. A apresentação dos programas verificadores do próprio partido ocorre em junho. Em agosto ou setembro é feita a compilação, a assinatura digital e lacração final.

Infelizmente, a fiscalização eleitoral na grande maioria dos Partidos Políticos é gerida por fiéis do Santo Baite desatentos que acreditaram na propaganda da invulnerabilidade do sistema e, adormecidos, ignoram a necessidade do acompanhamento do desenvolvimento do *software*.

Simplesmente não comparecem ao TSE para saber o que tem dentro dos programas que serão usados nas eleições.

Neste ano de 2006 apenas o PT, o PDT e o PV estão se preparando para cumprir estas tarefas. Os demais vinte e tantos partidos terão os seus fiscais nos Cartórios Eleitorais totalmente despreparados, quer dizer, sem a mínima condição de fazer alguma fiscalização consciente e racional.

De que adianta algum fiscal verificar assinaturas *hash* nos cartórios se não sabe o que isto significa e nem tem idéia de onde veio aquela verdadeira sopa de letrinhas?

Uma vez que usamos Urnas-E Virtuais, que não permitem auditoria da apuração, os partidos que queiram garantias de uma justa apuração eletrônica terão que arcar com o custo de manter uma equipe altamente especializada em Brasília por seis meses.

Esta equipe terá que:

---

66. Um artigo clássico na comunidade de segurança, mostra como é possível se introduzir código malicioso em programas prontos sem adulterar seus códigos-fonte. Ver em: *http://www.acm.org/classics/sep95/*

67. Código-fonte: versão dos programas de computador em forma de texto que pode ser lida e entendida pelos especialistas.

1. Desenvolver uma análise exaustiva do código-fonte dos programas eleitorais escritos em diversos níveis como Assembler, C, Delphy, SQL Oracle, etc. São mais de 50 mil arquivos de código-fonte;
2. Acompanhar a montagem de um ambiente seguro de compilação e da própria compilação de todos os sistemas que dura pelo menos uma semana de trabalho muito especializado e minucioso;
3. Apor a sua assinatura digital nos programas compilados. (esta é a parte fácil);
4. Enviar fiscais aos locais de carga das urnas para conferirem a assinatura digital. São em torno de 10 mil locais de carga que devem ser fiscalizados dentro do prazo de uma semana.

E ainda se deve ter consciência de que todo este trabalho tem eficiência relativa, pois como disseram os professores que escreveram o Relatório SBC:

"Na hipótese de que alguém tivesse colocado algo suspeito (no meio daqueles 50 mil arquivos), a probabilidade de um terceiro descobrir isto durante nossas sessões no TSE é quase zero".

Este é o custo de fiscalização imposto pelas Urnas-E Virtuais: Programas Descontrolados e Fiscalização da Apuração cara e pouco eficiente.

Houvesse o voto impresso conferido pelo eleitor, como nas Urnas-E Reais, poder-se-ia fazer uma auditoria estatística da apuração, bem mais simples de se entender, bem mais barata e, por tudo isto, mais viável e mais segura. Todo o ritual de acompanhamento do desenvolvimento do programas ao longo de seis meses por equipes especializadas, seria até dispensável, como foi dispensado das sugestões apresentadas no Relatório Brennan[68].

68. Ver em: *http://www.votoseguro.org/textos/brennan1.htm#3a*

3.5 Fraudes na Totalização

O Voto Cantado

A Clonagem de Urnas, já apresentada, é uma técnica de gerar documentação com resultados falsos, mas que será aceita pelo sistema de totalização, burlando suas defesas.

Há, no entanto, outra forma de se gerar resultados falsos e introduzi-los no sistema de totalização. Consiste em se utilizar o Sistema de Voto Cantado que está disponível em qualquer urna eletrônica.

Este sistema foi desenvolvido com recursos flexíveis para propiciar solução para vários problemas que podem ocorrer durante a totalização dos votos.

Problemas como urnas que deram defeito e não emitiram os disquetes com seus resultados, seções eleitorais que por falta de urnas substitutas passaram para o voto manual, disquetes que perderam seus dados (por desmagnetização), etc. são resolvidos com os recursos do Sistema de Voto Cantado.

Este sistema permite gerar um disquete com resultados da votação de qualquer seção eleitoral bastando que se introduzam os votos individuais ou em bloco em qualquer urna eletrônica que estiver disponível.

A introdução de votos individualmente é feita segundo um rito em que cada voto é cantado em voz alta para ser ouvido pelo digitador e pelos fiscais, daí o nome do sistema.

Ao final da introdução dos votos, o resultado é gravado num disquete para ser levado para o sistema de totalização, no qual gerará um aviso de pendência que precisa de uma liberação por senha determinada para sua aceitação.

No relatório do resultado geral da eleição devem constar todas as pendências geradas pelo totalizador indicando as seções que passaram pelo voto cantado.

Estes recursos disponíveis no Sistema de Voto Cantado permitem, também, sua má utilização para fraudar a totalização. Consiste em gerar disquetes com resultados falsos para substituir os verdadeiros que vierem das seções eleitorais.

É uma fraude de médio alcance, podendo afetar os resultados de uma Zona Eleitoral, e que deixa muitas pistas registradas nos arquivos de eventos, nas tabelas de correspondências e até no relatório final.

Mas todas estas pistas podem vir a ser apagadas pelos fraudadores, que provavelmente serão funcionários dos Cartórios Eleitorais com acesso suficiente para cantar escondidos votos em uma urna de reserva, trocar os disquetes na totalização e liberar as pendências no totalizador utilizando as senhas que os juízes normalmente lhes fornecem.

Em eleição estadual, como será a eleição de 2006, fica difícil apagar pista do relatório final que é produzido no TRE na Capital, mas pode-se contar com a falta de fiscalização dos partidos que raramente conferem se as pendências citadas no relatório foram legítimas ou fraudadas.

A defesa mais eficiente contra a fraude do Voto (maldosamente) Cantado, como no caso da Clonagem de Urnas, é o recolhimento dos boletins de urna nas seções eleitorais, mas aqui há um agravante.

Como esta fraude normalmente é operacionalizada depois de encerrada a votação, ao contrário da clonagem que tem que ser preparada antes, os fraudadores podem ter acesso às atas das seções eleitorais e descobrir em quais não houve retirada de BU pelos fiscais, e só adulterar os resultados destas seções dificultando sua descoberta.

Assim, recomenda-se recolher o máximo possível de BU impressos nas seções eleitorais (nunca nos cartórios) para evitar esta fraude.

O Ataque Final

A "*Mãe de Todas as Fraudes*", aquela que se acontecer pode reverter o resultado de qualquer outra fraude que porventura tiver ocorrido, consiste em se obter acesso direto ao banco de dados onde são registrados os votos de cada candidato por seção eleitoral.

Os bancos de dados com os resultados eleitorais ficam instalados em computadores protegidos, mas que necessariamente estão ligados a toda a rede de computadores da Justiça Eleitoral que, por sua vez, se interconecta em todos os Estados por canais externos.

Existe todo um sistema de proteção e de controle de acesso tanto na rede quanto no banco de dados, mas todos sabem que não exis-

te sistema de controle de acesso 100% invulnerável, principalmente contra ataques internos.

Muitos funcionários da Justiça Eleitoral ou de empresas contratadas têm autorização para acessar o banco de dados durante a totalização, seja para sua operação normal ou para sua manutenção de emergência.

Seria ingenuidade imaginar que é impossível alguns deles adulterarem os dados de votação, podendo ainda apagar pistas parcialmente. A experiência mundial confirma que o ataque aos bancos de dados por agentes internos é a maior origem de fraudes informatizadas como exemplificam o Caso do Painel do Senado[69] e o Caso da Quebra do Sigilo do Fracenildo[70].

O caso ocorrido na eleição de 2002 no Rio de Janeiro[71], quando totalizações parciais indicavam mais votos para alguns candidatos que o resultado final, sugere a manipulação dos resultados diretamente no banco de dados. Este caso se encontra sob investigação policial segundo reportagem no Jornal do Brasil[72].

Alguns candidatos a deputado estadual foram dormir no dia da eleição com uma votação parcial publicada e quando acordaram no dia seguinte tinham menos votos.

Como não conseguiram juntar os boletins de urna impressos das seções eleitorais das cidades onde a estranha queda de votos ocorreu, pois seus partidos nem de longe imaginavam que isto era necessário, não têm como provar se houve fraude.

Qualquer outro método de análise para encontrar provas é demorado e ineficiente.

---

69. Quebra do sigilo do voto de senadores ocorrido em 2000. A segurança do banco de dados do Senado foi violada por funcionários graduados, com credencial de acesso, atendendo pedido do Presidente do Senado que renunciou depois do caso se tornar público.

70. Quebra do sigilo bancário de testemunha chave na CPI dos Bingos ocorrida em 2006. A segurança do banco de dados da Caixa Econômica foi violada por funcionários graduados, com credencial de acesso, atendendo pedido do Ministro da Fazenda que pediu afastamento depois do caso se tornar público.

71. Ver mais em: *http://www.votoseguro.com/fraudenuncamais*

72. Matéria de Capa "*Polícia Federal Investiga Fraude na Urna Eletrônica*", Jornal do Brasil, 11/06/2006.

A Polícia Federal, que investiga o Caso Rio 2002, por não ter os BU impressos colhidos pelos fiscais, solicitou ao TRE-RJ os cartões de memórias das urnas para desenvolver perícias. Este órgão, que ao mesmo tempo é o investigado e é o guardião das provas, demorou 7 meses para entregar os cartões, comprometendo-os como valor de prova.

Praticamente esgotado o tempo do mandato disputado, ainda não se concluíram as investigações e os candidatos que viram seus votos diminuírem nos telões da Justiça Eleitoral ficam sem nenhuma explicação convincente a não ser fraude acobertada.

Assim, a defesa mais eficiente contra o Ataque Final é a coleta dos Boletins de Urna nas Seções Eleitorais, mas numa eleição estadual pode ficar bem difícil se o Partido não se organizar direito para coletar os Boletins de Urna em todas as cidades e, de alguma forma, deixá-los acessíveis a todos os seus candidatos.

De nada adianta fazer a coleta de BU impresso numa cidade e abandonar a coleta em outra. Se o Ataque Final ocorrer na cidade não fiscalizada, será difícil se provar a fraude.

4. Adendos

4.1 Manifesto sobre o Sistema Eleitoral Brasileiro

Em 1º de outubro de 2003, sob regime de urgência urgentíssima forçado por pressão da Justiça Eleitoral, a Câmara Federal aprovou a **Lei do Voto Virtual**[73]**,** sancionada minutos depois pelo Presidente da República.

Esta Lei 10.740/03, aprovada às pressas e sem debate no Congresso, eliminou os meios de fiscalização externa do processo eleitoral eletrônico brasileiro, tornando nossas eleições impossíveis de serem conferidas com eficiência.

Antes da aprovação da lei, membros da comunidade acadêmica brasileira, com o apoio de centenas de cidadãos preocupados com a lisura das eleições, publicaram um alerta, o qual não foi considerado pelos parlamentares pressionados. Este alerta, abaixo transcrito, permanece válido e conta hoje (junho de 2006) com o apoio de mais de 2.400 eleitores, entre eles renomados juristas, titulares das maiores universidades brasileiras e profissionais da área.

Os especialistas em Informática, que sabem que um sistema computacional sem controle é altamente inseguro, têm o dever de alertar a população, maravilhada com os dispositivos eletrônicos e sem conhecimento dos riscos que está correndo.

Não podemos deixar para as próximas gerações um sistema eleitoral sujeito a erros e fraudes eletrônicas difíceis de descobrir. Lutamos por um estudo técnico independente sobre a segurança desse sistema, que proponha meios de fiscalização dos resultados. Sem isto, não existirá democracia.

Apóie-nos em: *http://www.votoseguro.com/alertaprofessores*

A nação agradece.

---

73. Ver mais em: *http://www.votseguro.org/textos/PLazeredo.htm*

Alerta Contra a Insegurança do Sistema Eleitoral Informatizado

Somos favoráveis ao uso da Informática no Sistema Eleitoral, mas não à custa da transparência do processo e sem possibilidade de conferência dos resultados.

Cidadão brasileiro,

Nosso regime democrático está seriamente ameaçado por um projeto de lei em tramitação no Congresso Nacional, o Projeto do Voto Virtual, PL 1503/03. Este projeto, sob a máscara da modernidade, acaba com as alternativas de auditoria eficiente do nosso Sistema Eleitoral Informatizado, pois: (1) elimina o registro impresso do voto conferido pelo eleitor, substituindo-o por um "*voto virtual cego*", cujo conteúdo o eleitor não tem como verificar; (2) revoga a obrigatoriedade da Justiça Eleitoral efetuar uma auditoria aberta no seu sistema informatizado antes da publicação dos resultados finais; (3) permite que o Sistema Eleitoral Informatizado contenha programas de computador fechados, ou seja, secretos.

O Projeto de Lei do Voto Virtual nasceu por sugestão de ministros do Supremo Tribunal Federal e do Tribunal Superior Eleitoral (TSE), ao Senador Eduardo Azeredo, e sua tramitação tem sido célere, empurrado pela interferência direta desses ministros sobre os legisladores, como declarado por estes durante a votação no Senado.

As Comissões de Constituição e Justiça das duas casas legislativas analisaram a juridicidade do projeto mas, apesar dos constantes alertas de membros da comunidade acadêmica para seus riscos sem rigorosos procedimentos de auditoria e controle, nenhuma audiência pública com especialistas em Informática e Segurança de Dados foi realizada.

Essa lei, se aprovada, trará como resultado a instituição de um sistema eleitoral no qual não se poderá exercer uma auditoria externa eficaz, pondo em cheque até os fundamentos do projeto democrático brasileiro. Aceitando essa interferência e implantando um sistema eleitoral obscuro, corremos o risco de virmos a ser governados por

uma dinastia, com os controladores do sistema eleitoral podendo eleger seus sucessores, mesmo sem ter os votos necessários.

A nação, anestesiada pela propaganda oficial, lamentavelmente desconhece o perigo que corre. Os meios de comunicação, com honrosas exceções, omitem-se inexplicavelmente, como se o assunto não fosse merecedor de nossa preocupação.

A finalidade deste alerta é a denúncia da falta de confiabilidade de um sistema eleitoral informatizado que: utiliza programas de computador fechados, baseia-se em urnas eletrônicas sem materialização do voto, não propicia meios eficazes de fiscalização e auditoria pelos partidos políticos, e identifica o eleitor por meio da digitação do número de seu título eleitoral na mesma máquina em que vota. Assim, o princípio da inviolabilidade do voto, essencial numa democracia, será respeitado apenas na medida em que os controladores do sistema eleitoral o permitirem, transformando-se o voto secreto em mera concessão.

Uma verdadeira caixa-preta a desafiar nossa fé, este sistema é inauditável, inconfiável e suscetível de fraudes informatizadas de difícil detecção. Como está, ele seria rejeitado na mais simples bateria de testes de confiabilidade de sistemas, pois em Informática, "Sistema sem fiscalização é sistema inseguro". Muitas das fraudes que ocorriam quando o voto era manual, foram eliminadas, mas o cidadão brasileiro não foi alertado de que, com a informatização, introduziu-se a possibilidade de fraudes eletrônicas mais sofisticadas, mais amplas e mais difíceis de serem descobertas.

Enquanto os países adiantados caminham no sentido de exigir que sistemas eleitorais informatizados possuam o registro material do voto, procedam auditoria automática do sistema e só utilizem programas de computador abertos, com esse Projeto de Lei do Voto Virtual, o Brasil vai na contramão da história.

De que adianta rapidez na publicação dos resultados, se não respeitarmos o direito do cidadão de verificar que seu voto foi corretamente computado? Segurança de dados é assunto técnico especializado e assusta-nos a falta de seriedade com que nossa votação eletrônica tem sido tratada, nos três Poderes, por leigos na matéria. Os

rituais promovidos pelo TSE, como a apresentação dos programas, a carga das urnas e os testes de simulação são apenas espetáculos formais, de pouca significância em relação à eficiência da fiscalização.

Surpreende-nos, sem desmerecer suas competências na área jurídica, que autoridades respeitáveis da Justiça Eleitoral possam anunciar, com toda a convicção, que o sistema eleitoral informatizado é "100% seguro" e "orgulho da engenharia nacional", externando inverdades em áreas que não dominam, alheias ao seu campo de conhecimento específico.

Para o eleitor, a urna é 100% insegura, pois pode ser programada para "eleger" desde vereadores até o próprio presidente. O único e mais simples antídoto para esta insegurança é a participação individual do eleitor na fiscalização do registro do seu próprio voto, pois ele é o único capaz de fazer isto adequadamente.

O TSE sempre evitou debater tecnicamente a segurança da urna, ignorando todas as objeções técnicas em contrário. Nenhum estudo isento e independente foi feito até hoje sobre a alegada confiabilidade da urna sem o voto impresso. O estudo de um grupo da Unicamp (pago pelo TSE), parcial e pleno de ressalvas, recomendou vários procedimentos como condição para garantir o nível de segurança necessário ao sistema. Essas ressalvas, infelizmente, foram omitidas na propaganda sobre as maravilhas da urna.

A confiabilidade de sistemas informatizados reside nas pessoas e nas práticas seguras. Palavras mágicas como assinatura digital, criptografia assimétrica, embaralhamento pseudo-aleatório e outras panacéias de nada valem se não forem acompanhadas de rigorosos procedimentos de verificação, fiscalização e auditoria externas. Se esta urna algum dia cair sob o controle de pessoas desonestas, elas poderão eleger quem desejarem. De modo algum podemos confiar apenas nas pesquisas eleitorais como modo de validar os resultados das urnas eletrônicas, especialmente se as diferenças entre os candidatos forem pequenas.

Nenhum sistema informatizado é imune à fraude, especialmente a ataques internos, como sucedeu em julho de 2000 com o Painel Eletrônico do Senado, fato que levou à renúncia de dois senadores.

A única proteção possível é um projeto cuidadoso que atenda aos requisitos de segurança, e à possibilidade de auditorias dos programas, dos procedimentos e dos resultados.

Basta de obscurantismo no sistema eleitoral. Enfatizamos a necessidade de serem realizados debates técnicos públicos e independentes sobre a segurança do sistema e de seus defeitos serem corrigidos, antes da aprovação de leis que comprometam a transparência do processo.

A democracia brasileira exige respeito ao Princípio da Transparência e ao Princípio da Tripartição de Poderes no processo eleitoral.

Instamos todos os eleitores preocupados com a confiabilidade de nosso sistema eleitoral a transmitirem suas preocupações, por todos os meios possíveis, a seus representantes no Congresso e aos meios de comunicação.

Brasil, setembro de 2003.

Walter Del Picchia – Professor Titular, Escola Politécnica da Universidade de São Paulo – USP.

Jorge Stolfi – Professor Titular, Inst. de Computação da Univ. Estadual de Campinas – UNICAMP.

Michael Stanton – Professor Titular, Depto. de Ciência da Comput. da Univ Federal Fluminense – UFF.

Routo Terada – Professor Titular, Depto. de Ciências da Comput. do Inst.de Matemática e Estat.- USP.

Edison Bittencourt – Professor Titular, Fac. de Eng. Química da Univ. de Campinas – UNICAMP.

Pedro Dourado Rezende – Professor do Depto. de Ciência da Comput. da Univ. de Brasília – UNB – Representante da Socied. Civil no Comitê Gestor da Infra-estrutura de Chaves Públicas ICP-Brasil.

Paulo Mora de Freitas – Chefe Informática do Lab. Leprince-Ringuet da Ecole Polytechnique, França.

José Figueiredo – Professor Dr. do Depto.de Energia da Fac. de Eng. Mecânica da UNICAMP.

ALGUNS APOIOS IMPORTANTES

(entre mais de 2.400 apoios)

Roberto Romano – Professor Titular de Ética e Filosofia Política e ex-presidente da Comissão de Perícias da UNICAMP – Campinas, SP.

Celso Antônio Bandeira de Mello – Professor Titular de Direito Administrativo da Faculdade de Direito da PUCSP – São Paulo, SP

Sérgio Ferraz – Conselheiro Federal da OAB (Decano), Professor Titular de Direito Administrativo da Faculdade de Direito da PUCRJ – São Paulo, SP.

Fábio Konder Comparato – Professor Titular da Faculdade de Direito da USP, Doutor em Direito da Universidade de Paris, Doutor Honoris Causa da Universidade de Coimbra – São Paulo, SP.

Plínio de Arruda Sampaio – Promotor de Justiça, ex-deputado Federal Constituinte, Professor, Bacharel em Ciências Jurídicas (USP), Mestre em Desenvolvim.Internacional (EUA) – São Paulo, SP.

Sérgio Sérvulo da Cunha – Advogado, jurista, ex-Chefe de Gabinete do Minist.da Justiça – Santos, SP.

Américo Lourenço Masset Lacombe – Advogado, Presidente do Instituto de Defesa das Instituições Democráticas – Caieiras, SP.

Antonio Carlos Mendes – Advogado, Prof.de Direito Constituc.-Faculd.de Direito – PUCSP-S Paulo, SP.

João Roberto Egydio Piza Fontes – Advogado, ex-presidente da Seccional da OAB-SP –S. Paulo, SP.

Claudio Zamitti Mammana – Professor Livre Docente do Institutode Física da USP, ex-presidente da SBC e da ABICOMP, ex-secret.adjunto da Secretaria de Ciência e Tecnol. do Estado de São Paulo, SP.

João Antonio Zuffo – Professor Titular da Escola Politécnica da USP – Alphaville, SP.

Imre Simon – Professor Titular Aposentado do Instituto de Matemát. e Estatíst. da USP-São Paulo, SP.

Valdemar Setzer – Professor Titular do Depto de Ciência da Computação do Inst. de Matemática da USP, SP.

Plínio Benedicto de Lauro Castrucci – Professor Titular da Escola Politécnica da USP – S.Paulo, SP.

Giorgio Gambirasio – Professor Titular da Escola Politécnica da USP – Sao Paulo, SP.

Dimetri Ivanoff – Professor Titular da Escola Politécnica da USP – Sao Paulo, SP.

André Fabio Kohn – Professor Titular da Escola Politécnica da USP – São Paulo, SP.

Alessandro La Neve – Prof.Titular e Secr.Geral do Centro Univ.da FEI-Faculd.de Eng.Ind.-S.Paulo, SP.

Carlos Alberto Maziero – Prof.titular, pesquisador em segurança de sistemas – PUC Paraná-Curitiba, PR.

Claudio Thomás Bornstein – Professor Titular, COPPE/UFRJ – Rio de Janeiro, RJ.

Wilhelmus Van Noije – Professor Titular da Escola Politécnica da USP – S. Paulo, SP.

Yuda Dawid Goldman Vel Lejbman – Professor Titular do Instituto de Física da USP – S. Paulo, SP.

José Roberto Camacho – Doutor e Prof.Titular – Faculd.de Eng. Elétrica-Univers.Fed.de Uberlândia –MG.

Sonia Fleury – Prof.Titular da Escola Brasil.de Admin.Públ. e Empresas da Fund.Getúlio Vargas – RJ.

Guido Rummler – Professor Titular, Universidade Estadual de Feira de Santana – Salvador, BA.

Horácio Ortiz – Engenheiro e ex-Deputado Federal – São Paulo, SP.

Jose Roberto Faria Lima – Ex-Deputado Federal, Coordenador da implantação do PRODASEN, Ex-Presidente da PRODAM – São Paulo, SP.

Leik K. Sarev – PHD em Física Nuclear, MIT – Framingham, Boston, USA.

4.2 Resumo e Propostas do Fórum do Voto-E

Texto produzido em conjunto pelos assinantes do Fórum do Voto-E sob coordenação do Prof. Dr. Walter Del Picchia:

Principais Defeitos do Atual Sistema Eleitoral Informatizado Brasileiro

Falta transparência ao sistema eleitoral brasileiro pois:

1. As urnas eletrônicas não permitem recontagem nem qualquer conferência dos resultados.
2. Elas podem ser fraudadas por meio de programação e apresentar resultados diferentes dos votos colhidos.
3. No prazo concedido aos partidos políticos é impossível fazer uma avaliação efetiva dos programas da urna-e. Além disso, o TSE mantém em sigilo uma parte dos programas das urnas (o sistema operacional).
4. A digitação do número do Título Eleitoral na urna possibilita a identificação do voto por programas maliciosos (violação do voto secreto).
5. O prazo exíguo concedido pelo TSE e a falta de condições técnicas adequadas tornam impossível aos partidos fazer a conferência da totalização dos votos (totalização paralela).
6. O Teste de Votação Paralela, da forma como foi realizado, é inútil, pois simula uma votação com no máximo 180 votos, muito inferior à votação normal. Deste modo o programa da urna pode detectar que está sob teste e abortar a fraude.
7. O TSE desinforma a sociedade com a prática de manter secretos relatórios técnicos que apresentem criticas a confiabilidade do seu sistema.

Soluções Propostas para Minimizar os Riscos

Criar condições para a efetividade da auditoria externa do processo eleitoral através de:

1. Impressão paralela do voto pela própria urna, conferido pelo eleitor e recolhido automaticamente para contraprova, sem qualquer contato manual.
2. Recontagem dos votos impressos em 2% das urnas, escolhidas depois de encerrada a votação e emitidos os boletins de urna.
3. Abertura completa dos programas e sistemas da urna, antes das eleições, e meios efetivos de auditoria das urnas, antes e depois da votação.
4. Desvinculação entre a identificação do eleitor e a votação, eliminando qualquer digitação que identifique o eleitor na própria urna.
5. Apresentação dos Boletins de Urna das seções eleitorais na Internet, de forma a permitir uma eficiente conferência da totalização dos votos.
6. Correção dos procedimentos do teste de votação paralela para torná-lo eficaz, isto é, o mais próximo possível da situação real.

Observações

1. Os painéis do Senado e da Câmara sofrem das mesmas fragilidades das urnas eletrônicas.
2. Corremos o risco da criação de uma dinastia de governantes fraudadores, sem meios legais para contestá-los.
3. O TSE resiste aos aperfeiçoamentos no sistema de votação, quando é ele quem tem, além da atribuição, o dever de proporcionar um sistema eleitoral o mais possível imune a fraudes.

4.3 Pensamentos recolhidos pelo Fórum do Voto-E

Ignorância e Poder

Nós criamos uma civilização global em que elementos cruciais – como as comunicações, o comércio, a educação e até ***a instituição democrática do voto*** *– dependem profundamente da ciência e da tecnologia.*

Também criamos uma ordem em que quase ninguém compreende a ciência e a tecnologia. ***É uma receita para o desastre****. Podemos escapar ilesos por algum tempo, porém mais cedo ou mais tarde* ***essa mistura inflamável de ignorância e poder vai explodir na nossa cara****.*

– Carl Sagan
cientista, escritor e divulgador científico
Sagan, Carl – *O Mundo Assombrado pelos Demônios*
Cia das Letras, 1997, São Paulo – Cap. 2

Segurança de Dados

Se você acredita que a tecnologia pode resolver seus problemas de segurança, ***então você não conhece os problemas e nem a tecnologia****.*

– Bruce Schneier
criptógrafo, moderador do Crypto-Gram Newsletter
Schneier, Bruce – *Segurança.com (secrets and lies)*,
Ed. Campus, 2001, Rio de Janeiro – prefácio

Transparência Eleitoral

É até irônico que estas máquinas de votar, que supostamente deveriam resolver os problemas causados pelo sistemas eleitorais antiquados, estão simplesmente tornando os problemas invisíveis para o eleitor.

– Penny M. Venetis
Professora de Direito na Rutgers University, NJ, USA

O que é mais importante?

Se você não puder confiar na maneira como os votos são contados pouca coisa mais importa na política.

– Marian Beddill, Eng.
Mantenedora da página No Leaky Buckets

Pensando melhor...

Se você pensa no voto informatizado por cinco minutos, você pensa: 'Por que não?'. ***Mas se você pensa por algumas horas, descobre uma porção de razões do por que não.***

– Kim Alexander
presidente da California Voter Association

Além do Estado da Arte

O Brasil informatizou o voto em todas as etapas de uma eleição mas isto não indica que estamos na linha de frente no domínio desta tecnologia e sim que ***ultrapassamos esta linha de forma imprudente e precipitada****.*

É chegada a hora da sociedade civil brasileira entrar neste debate, ***sob pena de deixarmos para nossos filhos um arremedo de democracia onde*** *a Inviolabilidade do Voto não é garantida, o eleitor não pode verificar para quem foi dado o seu voto, não se permite fiscalizar a apuração...* ***como já está ocorrendo agora****!*

– Amílcar Brunazo Filho
moderador do Fórum do Voto Eletrônico

Jogando Palitinho por Telefone

Votar na urna eletrônica brasileira é mais ou menos como jogar palitinho por telefone.

– Paulo Mora de Freitas, Fis.
Chefe de Informática do Laboratório Leprince-Ringuet
da Ecole Polytechnique, França

Votar em Caça-níqueis

O voto eletrônico é só uma idéia extravagante. Para o resultado do escrutínio é como jogar numa máquina caça-níqueis

– Manuel Blanco
Juiz Eleitoral de La Plata, Argentina
referindo-se às urnas eletrônicas brasileiras da Diebold
oferecidas para as eleições de 1999 na província de Buenos Aires
Jornal O Clarín, de Buenos Aires, em 24/09/1999

Só Eles Sabem

Eu sei em quem votei,
Eles também,
Mas só eles sabem quem recebeu meu voto.

– Walter Del Picchia, eng.
Professor Titular da Escola Politécnica da USP

Voto X Dinheiro Eletrônico

Eu fui vítima de um desses programas de computador, espalhados pela Internet, com os quais até uma criança consegue gerar números válidos de cartão de crédito e apareceram compras no valor de 1.500 dólares na minha fatura.

Bastou um telefonema e uma carta de próprio punho à administradora do cartão para que todas essas compras fossem estornadas.

A questão do voto é bem diferente, pois ninguém vai "estornar" voto roubado.

– Jussara Simões
eleitora brasileira

Lema escolhido pelo Fórum do Voto-E

Se a urna não imprimir, seu voto pode sumir!

– Benjamin Azevedo, eng.
Membro do Fórum do Voto Eletrônico

ALL PRINT
EDITORA
www.allprinteditora.com.br
info@allprinteditora.com.br
Fone: (11) 5574-5322