COMITÊ MULTIDISCIPLINAR INDEPENDENTE

Relatório sobre o

Sistema Brasileiro de Votação Eletrônica

O TSE pode fazer mais.
Além da apuração rápida, que já nos oferece,
deveria propiciar uma apuração conferível pela sociedade civil

Comitê Multidisciplinar Independente

Sérgio Sérvulo da Cunha

Augusto Tavares Rosa Marcacini

Maria Aparecida Cortiz

Clovis Torres Fernandes

Jorge Stolfi

Pedro Antonio Dourado de Rezende

Amilcar Brunazo Filho

Frank Varela de Moura

Marco Antônio Machado de Carvalho

Márcio Coelho Teixeira

1ª edição
Edição dos Autores
Brasília
Março de 2010

Direitos do Autor – Copyleft

Para demais usos, contate os autores do CMind, em:

Sérgio Sérvulo da Cunha <sergioservulo@uol.com.br>

Augusto Tavares Rosa Marcacini <amarcacini@adv.oabsp.org.br>

Maria Aparecida Cortiz <maria.cortiz@uol.com.br>

Clovis Torres Fernandes <clovistf@uol.com.br>

Jorge Stolfi <stolfi@ic.unicamp.br>

Pedro Antonio Dourado de Rezende <prezende@unb.br>

Amilcar Brunazo Filho <amilcar@brunazo.eng.br>

Frank Varela de Moura <frank.varela@camara.gov.br>

Marco Antônio Machado de Carvalho <gersisbr@yahoo.com.br>

Márcio Coelho Teixeira <mlista@tasco.com.br>

CMind – telefone 4004 0435 ramal 5030 – (ligação local no Brasil; falar com Amílcar)

Dados Internacionais de Catalogação
Sistema de Bibliotecas da Universidade Católica de Santos – *SibiU*

R382 2010

Relatório sobre o sistema brasileiro de votação eletrônica / Sérgio Sérvulo da Cunha...[et al.].-- Brasília : Edição dos Autores, 2010.
105 p.; 29 cm

Inclui bibliografia

1. Fraude eleitoral - Brasil. 2. Justiça eleitoral - Brasil. 3. Voto eletrônico - Brasil. 4. Separação de poderes - Brasil. 5. Equilíbrio de poderes. 6. Sigilo do voto. I. Cunha, Sérgio Sérvulo da. II. Marcacini, Augusto Tavares Rosa. III. Cortiz, Maria Aparecida Silva da Rocha. IV. Fernandes, Clovis Torres. V. Stolfi, Jorge. VI. Rezende, Pedro Antonio Dourado de. VII. Brunazo Filho, Amílcar. VIII. Moura, Frank Varela de. IX. Carvalho, Marco Antonio Machado de. X. Teixeira, Márcio Coelho. XI. Comitê Multidisciplinar Independente. XII. Título

CDU 324 – 1997

SUMÁRIO

continua

1 INTRODUÇÃO

Este relatório foi escrito por advogados e especialistas em tecnologia da informação com experiência no processo eleitoral brasileiro, reunidos sob a denominação de ***Comitê Multisciplinar Independente***, e apresenta uma avaliação sobre o Sistema Brasileiro de Votação Eletrônica.

Este documento **também constitui uma réplica** ao relatório elaborado pelo *Comitê Multidisciplinar do TSE*, criado em março de 2009 para avaliação de propostas apresentadas pela Subcomissão Especial de Segurança do Voto Eletrônico da Comissão de Constituição e Justiça e Cidadania da Câmara dos Deputados (CCJC).

O presente Relatório e Réplica se destina a subsidiar os deputados da CCJC da Câmara Federal na elaboração de legislação destinada a elevar o nível de confiança e de segurança do sistema de votação eletrônica do Brasil.

Ainda, pretende reforçar e ampliar as justificativas às propostas encaminhadas pela CCJC ao TSE, no que possam ter sido mal interpretadas, distorcidas ou desconsideradas no relatório do *Comitê Multidisciplinar do TSE* (CMTSE).

Tem por objetivo mostrar as inconsistências e problemas do *Relatório do CMTSE*, além de enfatizar o que precisa ser aperfeiçoado no sistema eletrônico de votação brasileiro, de modo a garantir a integridade e o bom funcionamento do software que controla a urna eletrônica brasileira, em consonância com as propostas apresentadas pela Subcomissão Especial de Segurança do Voto Eletrônico da CCJC.

Na Seção 1.1, apresenta-se um histórico dos passos que levaram à escrita deste relatório e réplica. Na Seção 1.2, apresenta-se a composição do *Comitê Multidisciplinar Independente*. Na seção 1.3, apresenta-se a estrutura deste documento. Na Seção 1.4, apresenta-se um resumo das conclusões deste relatório. Na Seção 1.5, apresenta-se a terminologia empregada neste documento.

1.1 HISTÓRICO

Após audiência pública em 29 de março de 2007 na Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados, foi criada a **Subcomissão Especial de Segurança do Voto Eletrônico**, presidida pelo dep. Geraldo Magela (PT-DF), para avaliar projetos de lei relativos ao sistema de votação informatizada em uso no Brasil.

Ao longo de 2007 e 2008, a subcomissão promoveu 7 audiências públicas, tendo ouvido 11 especialistas no processo eletrônico de votação e em segurança de dados, incluindo-se nesse rol tanto o Diretor Geral quanto o Secretário de Tecnologia da Informação do TSE, e elaborou dois relatórios aprovados posteriormente no plenário da CCJC.

O primeiro destes teve como relator o dep. Vital do Rêgo (PMDB-PB) e foi aprovado em novembro de 2007. O segundo, relatado pelo dep. Gerson Peres (PP-PA), foi aprovado em fevereiro de 2009.

Para referência no presente trabalho, esses relatórios serão denominados respectivamente por *Relatório CCJC 2007* [1] e *Relatório CCJC 2008* [2].

Ambos apresentam propostas para incremento da confiabilidade do sistema eletrônico de votação e foram entregues em mãos ao Presidente do TSE, Min. Ayres Britto, em audiências em 18 de fevereiro de 2009 e em 03 de março de 2009.

As propostas nos dois relatórios da CCJC divergem bastante, havendo em comum apenas o seguinte item:

> *"Criar Auditoria Independente do Software das urnas eletrônicas, por meio da recontagem automática dos Votos Materializados Conferíveis pelo Eleitor."*

No dia 20 de março de 2009, por meio da Portaria TSE 192/2009, foi criado o ***Comitê "Multidisciplinar" do TSE***, doravante designado como CMTSE, indicado e coordenado pelo seu Secretário de Tecnologia da Informação, com o seguinte objetivo, assinalado em seu art. 1º:

> "*analisar as sugestões apresentadas no Relatório da Subcomissão Especial do Voto Eletrônico da CCJC da Câmara dos Deputados*"

Obs.: o motivo do termo "Multidisciplinar" aparecer entre aspas, quando se refere ao CMTSE, será explicado na Seção 2.1 do Capítulo 2 desta Réplica.

Em 26 de maio de 2009, o CMTSE apresentou[3] o seu relatório[4] onde, por iniciativa própria, informou o seguinte:

> "*... não se limitou aos temas abordados pela subcomissão da CCJC mas, em função do rico debate e apresentação de ideias, ampliou seu escopo*".

Em julho de 2009, com o intuito de prosseguir esse rico debate, alguns dos especialistas ouvidos pela CCJC, professores universitários e técnicos em informática especializados em urna eletrônica, juntaram-se a juristas e advogados eleitorais bem como com os representantes técnicos de Partidos Políticos e da OAB que acompanharam o desenvolvimento dos sistemas eleitorais, compondo-se o ***Comitê Multidisciplinar Independente***, doravante designado como **CMind**, para elaborar este relatório e réplica ao *Relatório do Comitê "Multidisciplinar" do TSE,* aqui denominado, por simplicidade, apenas por Réplica.

---

1 Texto disponível em: *http://www.votoseguro.org/textos/sve2007-relatorio.pdf*

2 Texto disponível em: *http://www.votoseguro.org/textos/sve2008-relatorio.pdf*

3 Notícia do TSE: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1187457*

4 *Relatório do Comitê Multidisciplinar nomeado pela Portaria TSE 192* . Brasília: TSE, 26/05/2009 - *http://www.votoseguro.org/textos/comiteTSE-1.pdf*

1.2 Sobre a Composição do Comitê Multidisciplinar Independente

O CMind é composto por dez membros, sendo três professores universitários de ciência da computação, um jurista, autor de livro sobre Direito Eleitoral, um advogado especializado em informática jurídica que já acompanhou o desenvolvimento dos sistemas no TSE, uma advogada eleitoral com larga experiência na fiscalização do voto eletrônico no Brasil e quatro técnicos em informática com experiência junto ao sistema de votação eletrônica brasileiro.

Seis membros do CMind possuem experiência pessoal própria como agentes credenciados para acompanhar o desenvolvimento dos sistemas eleitorais junto ao TSE, conforme §§ 1º ao 4º do Art. 66 da Lei 9.504/97, na qualidade de representantes de Partidos Políticos ou da OAB , e, neste sentido, **CONSTITUEM A TOTALIDADE dos representantes de ENTIDADES EXTERNAS que de fato acompanharam a apresentação e o desenvolvimento dos sistemas do TSE desde 2004**.

Isso carateriza e ilustra o aspecto multidisciplinar do CMind, uma vez que seus integrantes têm formação apropriada, **capacitações diferentes mas correlatas, complementares e condizentes com o objetivo do comitê**.

Com relação à área de informática, registra-se que os especialistas têm conhecimento teórico e prático qualificado em sistemas de segurança informacional, em engenharia de software, em criptografia, em projeto de circuitos, em programação geral e em linguagem de máquina.

Além disso, todos eles possuem conhecimento expressivo de aspectos relevantes do sistema eleitoral brasileiro, seja por seu histórico de trabalhos em sistemas que exigem alto grau de segurança, seja por trabalhos realizados junto ao próprio sistema eleitoral brasileiro.

Quanto ao aspecto de independência, em especial do TSE, cumpre assinalar que a reunião dos autores ocorreu de forma espontânea e pessoal. Nesse sentido, **os autores membros do CMind declaram o seguinte**:

- **Não receberam nenhuma orientação, ajuda ou apoio financeiro** de nenhuma entidade pública, privada, acadêmica ou partidária para elaborar o presente trabalho.
- Nunca prestaram nenhum serviço remunerado ao TSE.
- **Não existe hierarquização dentro do CMind**, inexistindo a figura de coordenador. Todos os membros participam das decisões do grupo com igual direito à palavra e ao voto.
- Este Relatório reflete a opinião conjunta dos autores e **não deve ser creditada a terceiros**, sejam pessoas ou entidades.
- Finalmente, **nenhum dos autores fala em nome da entidade em que trabalha ou presta serviços**.

A seguir, apresenta-se um resumo das qualificações profissionais e da atuação no tema do relatório de cada um dos membros do *Comitê Multidisciplinar Independente*, dentro de uma categorização pela atuação principal do membro:

Juristas e Advogados:

- **Adv. Sérgio Sérvulo da Cunha**, 74, jurista, foi presidente da Subsecção de Santos da OAB (1981/83); coordenou o Bureau de Acompanhamento da Constituinte, do Conselho Federal da OAB; Assessor da Presidência do Conselho Federal da OAB; Membro da Comissão Permanente de Direito Constitucional do Instituto dos Advogados Brasileiros; Chefe de Gabinete do Ministro da Justiça, Dr. Márcio Thomás Bastos (2003/04); autor de inúmeros textos publicados inclusive o "*Manual das Eleições*" [5], em coautoria com o Prof. Roberto Amaral.

- **Adv. Augusto Tavares Rosa Marcacini**, 45, advogado em São Paulo. Bacharel, Mestre e Doutor em Direito pela Faculdade de Direito da USP. Presidente da Comissão de Informática Jurídica da OAB-SP, nos triênios 2004/2006 e 2007/2009. Membro da Comissão de Tecnologia da Informação do Conselho Federal da OAB, no triênio 2004/2006, e indicado como **representante da OAB junto ao TSE para a fiscalização dos sistemas eletrônicos de votação, em 2004**. Professor de Direito Processual Civil e Direito da Informática em cursos de Graduação e Pós-Graduação. Autor de "*Direito e Informática: uma abordagem jurídica sobre a criptografia*" [6], dentre outros livros e artigos jurídicos publicados.

- **Adv. Maria Aparecida da Rocha Cortiz**, 49, advogada em São Paulo. Bacharel com curso de extensão em direito administrativo pela PUC-SP, credenciada como representante de partidos políticos e especializada em fiscalização eleitoral. Acompanha o desenvolvimento dos sistemas eleitorais junto ao TSE desde 2002. Coautora do primeiro relatório[7] de análise dos arquivos digitais de auditoria de Alagoas em 2006, e do livro "Fraudes e Defesas no Voto Eletrônico" [8], além de outros artigos publicados.

Professores Universitários na área de Ciência da Computação:

- **Prof. Dr. Jorge Stolfi** [9], 59, Ph.D pela Stanford University em 1988 é **Professor Titular do Instituto de Computação da UNICAMP**. Apresentou-se em audiências públicas, para discorrer sobre a segurança das urnas eletrônicas, no dia 04 de dezembro de 2008 perante a CCJC da Câmara Federal e no dia 20 de agosto de 2009 perante as comissões CCJ e CCT do Senado Federal.

- **Prof. Dr. Clovis Torres Fernandes** [10], 56, **Professor Associado da Divisão de Ciência da Computação do ITA**, especializado em **Engenharia de Software**. Organizador do SSI - Simpósio sobre Segurança em Informática, realizado no ITA de 1999 a 2006, onde teve início o debate acadêmico sobre voto eletrônico no Brasil. Autor do segundo e principal relatório[11] sobre as urnas eletrônicas usadas na eleição em Alagoas 2006. Apresentou-se perante a CCJC da Câmara dos Deputados em 29 de março de 2007[12].

---

5 **Amaral, R. e Sérvulo da Cunha, S.** - *Manual das Eleições, 3ª edição* - São Paulo: Editora Saraiva, 2006 - *http://www.livrocamp.com.br/produtos_descricao.asp?lang=pt_BR&codigo_produto=1801*

6 **Marcacini, A.T.R** - *Direito e Informática: uma abordagem jurídica sobre a criptografia* – São Paulo: Ed. Forense, 2002

7 **Brunazo F., A. , Cortiz, M.A.R. e Carvalho, M.A.M.** - *Laudo de Avaliação dos Dados Oficiais da Eleição de Alagoas 2006* . Alagoas: outubro de 2006 – *http://www.votoseguro.org/arquivos/AL06-laudoBCC.zip*

8 **Brunazo F., A. e Cortiz, M.A.R.** - *Fraudes e Defesas no Voto Eletrônico*. São Paulo: All Print Editora, 2006 – *http://www.brunazo.eng.br/voto-e/livros/F&D-texto.pdf*

9 Mais informações a partir de: *http://en.wikipedia.org/wiki/Jorge_Stolfi* , e em: *http://www.ic.unicamp.br/~stolfi/*

10 Currículo Lattes em: *http://lattes.cnpq.br/6635354260645535*

11 **Fernandes, C. T**. - *Radiografia das Urnas Eleitorais.* S. J. dos Campos: ITA, dezembro de 2006 - *http://www.votoseguro.org/arquivos/AL06-laudoFerITA.zip*

obs.: no início deste relatório, o autor explicita que fala em nome próprio e não da instituição que trabalha.

12 Áudio da palestra em: *http://www.votoseguro.org/arquivos/CCJaudio1Clovis.mp3*

- **Prof. Pedro Antônio Dourado de Rezende** [13], 57, **matemático e criptógrafo**, Professor de Criptografia e Ciência da Computação da **Universidade de Brasília, UnB**, ex-representante da Sociedade Civil na Infra-Estrutura de Chaves Públicas Brasileira (ICP-BR) e membro do Conselho Consultivo do Instituto Brasileiro de Direito e Política de Informática. Participou do *I Seminário do Voto Eletrônico* ocorrido no Centro Cultural da Câmara dos Deputados em 25 de maio de 2002 e apresentou-se perante a CCJC da Câmara dos Deputados em 25 de novembro de 2008.

Técnicos em informática com experiência no sistema eleitoral brasileiro:

- **Eng. Márcio Coelho Teixeira**, 46, engenheiro e programador em linguagem de máquina. Projetista do protótipo de urna eletrônica apresentado pelo TRE-MG em 1995, que foi considerada a melhor proposta pela Comissão de Informatização do Voto do TSE. **Acompanhou a apresentação dos sistemas eleitorais do TSE em 2000**. Em 2001 foi nomeado assistente técnico pela Subcomissão do Voto Eletrônico da CCJ do Senado, para acompanhar a auditoria da UNICAMP.

- **Eng. Amilcar Brunazo Filho**, 60, engenheiro pela Poli-USP e representante técnico de partido político para **acompanhamento do desenvolvimento dos sistemas eleitorais desde 2000**. Assistente Técnico de diversos partidos políticos em perícias eleitorais. Coautor do livro *"Fraudes e Defesas no Voto* Eletrônico" e do primeiro relatório de análise dos dados eleitorais de Alagoas em 2006. Apresentou-se perante a CCJC da Câmara Federal em 29 de março de 2007[14] e em 04 de junho de 2007 e perante as comissões CCJ e CCT do Senado Federal no dia 20 de agosto de 2009. Em 2001 foi nomeado assistente técnico pela Subcomissão do Voto Eletrônico da CCJ do Senado, para acompanhar a auditoria da UNICAMP.

- **Frank Varela de Moura**, 38, analista de sistemas e pós-graduando em Ciência da Computação na área de *"Desenvolvimento de Sistemas Distribuídos com orientação a objetos"* pela UnB/FINATEC. **Acompanha o desenvolvimento dos sistemas eleitorais do TSE desde 2004**. Ministrou cursos de fiscalização eletrônica e é autor de manuais de fiscalização eleitoral [15] nas últimas três eleições, em conjunto com a Dra. Stella Bruna Santo e com a Sra. Gisa Guimarães. Palestrante no Carter Center[16], em Atlanta, GA/USA, sobre o tema *"Eleições Eletrônicas no Brasil"*, como representante da delegação enviada pela Câmara dos Deputados para observação das eleições nos EUA em 2004.

- **Marco Antônio Machado de Carvalho**, 44, analista de sistemas e programador de computadores, representante técnico de partido político para **acompanhamento do desenvolvimento dos sistemas eleitorais em 2008** e especializado em recuperação profissional de dados digitais[17], civil e forense. É coautor do primeiro relatório de análise dos arquivos digitais de auditoria de Alagoas em 2006.

13 Ver produção acadêmica em: *http://www.cic.unb.br/~pedro/sd.htm*

14 Áudio da palestra em: *http://www.votoseguro.org/arquivos/CCJaudio2Brunazo.mp3*

15 Manual 2008 de fiscalização eleitoral geral em: *http://www.assessoriadopt.org/manualfiscaliza.pdf*
Manual 2008 de fiscalização da carga das urnas em: *http://www.assessoriadopt.org/manualcarga.pdf*

16 Carter Center - instituição criada e presidida pelo ex-presidente americano Jimmy Carter

17 Ver em: *http://www.sosdados.com.br/*

1.3 Sobre este Documento

No Capítulo 2 deste documento são analisados alguns aspectos formais preliminares relativos ao *Relatório do CMTSE*.

No Capítulo 3, como *Informações Preliminares,* são apresentados casos concretos que revelam as dificuldades na fiscalização do voto eletrônico pelos Partidos Políticos (Seção 3.1) e pela OAB (Seção 3.2).

Ao final desse capítulo, é introduzido o conceito de ***Independência do Software,*** que vem sendo adotado nas normas técnicas internacionais sobre equipamentos de votação e que será usado como paradigma na avaliação de mérito desenvolvida no capítulo seguinte.

No Capítulo 4, que contém a avaliação de mérito, apresenta-se inicialmente uma descrição dos temas citados nos *Relatórios da CCJC* mas que foram omitidos ou desconsiderados no *Relatório da CMTSE*. Em seguida, apresenta-se uma avaliação crítica e a réplica aos argumentos técnicos centrais do CMTSE.

No Capítulo 5 apresentam-se as conclusões e recomendações do CMind para o sistema eleitoral brasileiro .

Como Anexos, foram incluídos documentos de difícil acesso por outros meios e informações complementares relevantes para a análise e conclusões apresentadas.

Nas referências bibliográficas, procurou-se, sempre que conhecido, indicar um endereço na Internet onde seja possível encontrá-la de forma rápida. Todos esses endereços foram conferidos quanto à disponibilidade no dia 25 de março de 2010.

Todas as inclusões de textos de terceiros foram marcadas em azul, mas eventuais destaques dentro delas, em negrito ou sublinhado, são dos autores deste relatório.

1.4 Resumo das Conclusões e Sugestões

A conclusão final do CMind é que o TSE pode e deveria fazer mais.

Além do sistema de **apuração rápida**, que já nos oferece, o TSE deveria propiciar uma sistema eleitoral de **apuração conferível** pela sociedade civil.

Concluiu-se, ainda, que há exagerada concentração de poderes no processo eleitoral brasileiro, resultando em **comprometimento do Princípio da Publicidade e da soberania do eleitor** em poder conhecer e avaliar, *motu próprio*, o destino do seu voto.

Como consequência disso, constata-se que no atual sistema eleitoral brasileiro **É IMPOSSÍVEL para os representantes da sociedade conferir e auditar o resultado da apuração eletrônica dos votos**. Em outras palavras, desde 1996 a sociedade civil brasileira não tem como conferir e confirmar o resultado publicado pela autoridade eleitoral.

Esta impossibilidade de auditoria independente do resultado eleitoral é que levou à **rejeição de nossas urnas eletrônicas em todos os mais de 50 países** que aqui vieram avaliá-la.

Com relação ao *Relatório do CMTSE* verificou-se que **consiste basicamente numa reprodução fiel dos argumentos apresentados anteriormente por seu coordenador** - o Secretário de TI do TSE, Sr. Guiseppe Dutra Janino - em audiências públicas perante a Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados.

Em seu relatório, **o CMTSE foi a extremos**, chegando a **CITAR COM EXPLÍCITA INVERSÃO DE MÉRITO**, trabalhos técnicos de terceiros para emprestar crédito a seus argumentos, conforme pode-se constatar na Seção 4.4 do Capítulo 4 e no Anexo 4 desta Réplica.

A análise dos argumentos técnicos defendidos no *Relatório do CMTSE* mostrou que ele se encontra eivado de **OMISSÕES**, **PARCIALIDADE** e **SUPERFICIALIDADE**, como exaustivamente demonstrado nos Capítulos 3 e 4 desta Réplica e registrado nas conclusões finais da mesma, no Capítulo 5.

Diante dessas condições, conclui-se que **o *Relatório do Comitê "Multidisciplinar" do TSE* não construiu a credibilidade necessária para o fim que se propôs**, devendo ser desconsiderado em qualquer análise séria com o fim de aperfeiçoar o nível de confiança e de segurança do sistema de votação eletrônica brasileiro.

As principais recomendações do CMind são as seguintes:

1. Propiciar **separação mais clara de responsabilidades nas tarefas de normatizar, administrar e auditar o processo eleitoral brasileiro**, deixando à Justiça Eleitoral apenas a tarefa de julgar o contencioso.

2. Possibilitar uma **auditoria dos resultados eleitorais de forma totalmente independente das pessoas envolvidas** na sua administração.

3. **Regulamentar mais detalhadamente o Princípio de Independência do Software em Sistemas Eleitorais**, expresso no Art. 5 da Lei 12.034/09, definindo claramente as regras de auditoria com o Voto Impresso Conferível pelo Eleitor.

1.5 Terminologia Adotada

Apuração e Totalização – São processos separados que ocorrem em momentos e locais diferentes. A *Apuração* ocorre primeiro e consiste na soma dos votos colhidos por uma máquina de votar que resulta no *Boletim de Urna*, expresso em forma digital e impressa. Já a *Totalização* ocorre depois, nos computadores dos Tribunais Eleitorais, e consiste na soma dos Boletins de Urna para se gerar o resultado final da eleição.

Arquivos Digitais de Auditoria – É um conjunto de arquivos digitais gerados numa máquina de votar, destinados a uso na auditoria do seu funcionamento, que inclui a preparação, a coleta de votos e a apuração. No caso das urnas brasileiras, os principais, mas não únicos, arquivos digitais de auditoria são, a saber: BU, LOG e RDV, também descritos nesta seção.

Arquivo BU (de Boletim de Urna) - Arquivo digital da urna eletrônica brasileira onde é gravado o resultado da *apuração*.

Arquivo LOG – Arquivo digital da urna eletrônica brasileira onde são registrados a data e hora de eventos importantes ocorridos durante determinado processo.

Arquivo RDV (de Registro Digital do Voto) – Arquivo digital da urna eletrônica brasileira onde fica gravado o conjunto de todos os votos confirmados pelos eleitores.

Auditoria Independente do Software – Procedimento de conferência da apuração eletrônica de votos de forma que não depende, para tanto, da integridade ou do bom funcionamento do software da máquina de votação e apuração.

Boletim de Urna: Resultado da apuração em cada máquina de votar e que pode ter a forma de arquivo digital ou ser impresso em papel logo que calculado.

CMind - **Comitê Multidisciplinar Independente** – Conjunto dos dez autores desta Réplica.

CMTSE - **Comitê "Multidisciplinar" do TSE** – Comitê de cinco integrantes nomeados pela *Portaria TSE 192/2009* de 20/03/2009.

Independência do Software em Máquinas de Votar – Conceito **necessário** para permitir a *Auditoria Independente do Software*. Foi proposto[18] em 2006 por um dos inventores da técnica de assinatura digital, depois de concluir que essas técnicas criptográficas não são suficientes para oferecer garantia de integridade lógica do software das máquinas de votar eletrônicas **durante a votação**.

Máquinas DRE (de *Direct Recording Electronic Voting Machines)* - Tipo de equipamento eletrônico de votação que grava os votos em *Arquivos RDV* para posterior apuração. **As urnas eletrônicas brasileiras são do tipo DRE**.

Registro Digital do Voto – O mesmo que *Arquivo RDV* ou, simplesmente, *RDV*.

Registro Independente do Voto Conferível pelo Eleitor (RICE) – Qualquer forma de registro do voto cuja exatidão possa ser conferida pelo eleitor assim que gerado e de uma maneira que não dependa do software da máquina de votar. Os RICE são necessários para viabilizar a *Auditoria Independente do Software*.

Voto Impresso Conferível pelo Eleitor (VICE) – É o meio pelo qual se pode obter *RICE* em *máquinas DRE*, através da impressão do voto e da sua apresentação para confirmação pelo eleitor **antes da gravação do voto** no *Arquivo RDV*. Assim, podem existir *Máquina DRE com VICE* e *Máquina DRE sem VICE.*

Voto Materializado Conferível pelo Eleitor – É um sinônimo de RICE usado tanto no *Relatório CCJC 2007* quanto no *Relatório CCJC 2008*.

18 **Rivest R.R. , Wack, J.P.** - *On the notion of "software independence" in voting systems* : USA, NIST, 28/07/2006 - *http://vote.nist.gov/SI-in-voting.pdf*

2 ANÁLISE DE ASPECTOS FORMAIS DO RELATÓRIO CMTSE

Antes da apresentação da análise dos argumentos técnicos desenvolvidos no *Relatório CMTSE*, discutem-se alguns aspectos formais preliminares, relativos à composição do CMTSE, à escolha da sua assessoria e sobre as referências bibliográficas citadas.

2.1 Sobre a Composição do Comitê "Multidisciplinar" do TSE

Nesta seção, discutem-se os aspectos de imparcialidade, de independência e de multidisciplinaridade dos componentes do CMTSE.

O CMTSE teve seus membros indicados e foi coordenado pelo **Secretário de Tecnologia da Informação** (STI/TSE), Sr. Giuseppe Dutra Janino, que possui longa experiência com as urnas eletrônicas brasileiras. Como funcionário da STI/TSE, o Sr. Janino acompanhou o desenvolvimento desse equipamento desde o início e seu posicionamento a favor de máquinas de votar puramente digitais, sem registro independente do voto (*máquinas DRE sem VICE*), é público e notório:

- O Sr. **Giuseppe Dutra Janino** apresentou-se perante a CCJC da Câmara dos Deputados em 23 de maio de 2007 e em 04 de dezembro de 2008 quando descreveu o sistema eletrônico de votação criado pelo TSE, citando com detalhes suas salvaguardas e justificando a opção do TSE de adotar *máquinas DRE sem VICE*.

Na escolha dos demais membros do CMTSE, o Coordenador do CMTSE procurou evitar o contraditório, indicando exclusivamente especialistas na área de informática alinhados com sua posição contrária à impressão do voto, não abrindo espaço para especialista de outras áreas, ou com opiniões divergentes ou favoráveis à impressão do voto.

Além disso, o Coordenador do CMTSE priorizou escolher, dentre os técnicos de TI alinhados à sua posição, os que já tivessem prestado serviços remunerados à sua secretaria, sempre que possível.

Apenas um dos membros indicados não havia prestado serviço ao TSE antes de participar desse comitê, mas foi chamado posteriormente para prestar novos serviços.

A seguir, apresentam-se os componentes do CMTSE, onde se procura evidenciar a falta de imparcialidade e independência de todos eles em relação ao TSE, em especial das teses do Coordenador do CMTSE.

Pesquisador Antônio Montes Filho[19]

Pesquisador Amândio Ferreira Balcão Filho[20]

- São pesquisadores do Centro de Tecnologia da Informação Renato Archer do Ministério da Ciência e Tecnologia (CTI/MCT – antigo CenPRA), atuando na área de segurança de informática.
- Foram consultores do TSE sob o *Contrato TSE 032/2008* de maio de 2008, para elaborar análises quanto a segurança do sistema eletrônico de votação.
- Na cláusula 4.3 do contrato com o TSE é estabelecida a participação e **remuneração de técnicos do CTI/CenPRA.**
- No item 1.1 do *Relatório do CMTSE* os pesquisadores são apresentados como *"**autores de relatórios** de análise da segurança do sistema eletrônico de votação, o que ocorreu a partir de um **detalhado estudo** e acompanhamento de todas as etapas de preparação e execução das eleições 2008".*
- No entanto, **tais relatórios não estão disponíveis para conhecimento ou avaliação por terceiros** visto terem sido **declarados secretos** pelo coordenador do CMTSE, através da *Informação nº 002/2008-STI-TSE* de 12/11/2008 (vide Anexo 1).
- Não é prática comum citar, como referência curricular, trabalhos secretos que não possam ser acessados ou consultados por terceiros e, talvez por isso, nos seus próprios currículos Lattes e do CNPq não se encontre nenhuma referência a trabalhos sobre o sistema eletrônico de votação para o TSE.

Professor Ricardo Dahab

- É professor da área de Ciência da Computação do Instituto de Computação da UNICAMP, atuando em criptografia.
- Trabalhou para o TSE sob o *Contrato TSE 054/2001* de novembro de 2001, produzindo em 2002, em coautoria com outros professores da UNICAMP, o polêmico relatório *"Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica)"* [21].
- Esse relatório foi alvo de severas críticas no meio jurídico e no meio acadêmico, de autores como: Marco Aurélio Aydos [22] (Procurador da República), Roberto Romano [23] (ex-Presidente da Comissão de Perícias da UNICAMP), Jorge Stolfi [24] (Diretor do Instituto de Computação da UNICAMP), Jeroen Van der Graaf (UFMG) e Ricardo Felipe Custódio [25] (UFSC) e de Pedro Antônio Dourado Rezende [26] (UnB).

---

19 Currículo Lattes em: *http://buscatextual.cnpq.br/buscatextual/visualizacv.jsp?id=E51301*
Currículo CNPq em: *http://dgp.cnpq.br/buscaoperacional/detalhepesq.jsp?pesq=9186593293344088*

20 Currículo Lattes em: *http://buscatextual.cnpq.br/buscatextual/visualizacv.jsp?id=P074182*
Currículo CNPq em: *http://dgp.cnpq.br/buscaoperacional/detalhepesq.jsp?pesq=5891652594120801*

21 **Tozzi, C.L. et al.** - *Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica). Campinas:* TSE, maio de 2002 - *http://www.tse.gov.br/internet/eleicoes/relatorio_unicamp/rel_final.pdf*

22 **Aydos, M.A.** - *A Mulher de César.* Observatório de Imprensa, junho de 2002 – ver Seção II *http://www.observatoriodaimprensa.com.br/artigos/mid100720025.htm*

23 **Romano, R.** - *Urnas Eletrônicas, ABIN e UNICAMP*. São Paulo: Folha de São Paulo, 11/06/2002 - *http://www.votoseguro.org/noticias/folha14.htm*

24 **Stolfi, J.** - *Sobre o Relatório TSE-FUNCAMP.* Fórum do Voto Eletrônico, 22/10/2002 - *http://www.votoseguro.org/textos/stolfi1.htm e http://www.ic.unicamp.br/~stolfi/urna/04-carta-jornais.html*

25 **Graaf, J.V. e Custódio, R.F.** - *Tecnologia Eleitoral e a Urna Eletrônica.* Sociedade Brasileira de Computação, 2002 – ver item 1.4 - *http://www.sbc.org.br/index.php?language=1&content=downloads&id=281*

26 **Rezende, P.D.** - *Análise do Relatório 'da Unicamp'.* Instituto Alberto Pasqualini, 2002 - *http://www.cic.unb.br/docentes/pedro/trabs/relunicamp.htm*

- Essas críticas ressaltam, de forma unânime, a interferência e uso político desse relatório pelo TSE, a exclusão dos assistentes técnicos do Senado[27] e a omissão em responder seus quesitos e, ainda, à ambiguidade de algumas conclusões e propostas oferecidas.
- Como consequência direta do **uso impróprio e abusivo do nome da instituição pelo TSE**, que sempre o designa esse texto incorretamente como "*Relatório da UNICAMP"*, a *Câmara de Administração do Conselho Universitário da UNICAMP* baixou, em 13 de junho de 2003, a **deliberação CAD-A-4** [28], esclarecendo que **professores dos quadros da universidade, mesmo quando autorizados pelo reitor a realizar trabalhos externos, não estariam autorizados a falar deles em nome da UNICAMP** e que deveriam fazer constar ressalva neste sentido na folha de rosto do relatório produzido.
- Ignorando essa deliberação, não consta tal ressalva no *Relatório CMTSE* e, na Seção 2.1.3, os autores, incluindo o próprio prof. Dahab, voltam a explorar indevidamente a imagem da instituição universitária, citando o relatório escrito em 2002 como se representasse a palavra oficial da UNICAMP.

Em consideração à deliberação CAD-A-4 do Conselho Universitário da UNICAMP, nesta Réplica designaremos o relatório supracitado como *o chamado Relatório "Unicamp"*, com aspas, para caraterizar que não expressa a opinião da instituição.

Professor Mamede Lima-Marques

- É Professor Titular da UnB, atuando em arquitetura de informação, com nenhum trabalho anterior ou artigo publicado na área de votação eletrônica.
- É o único membro do CMTSE que não havia trabalhado anteriormente para o TSE.
- Apresentou-se perante a CCJC da Câmara de Deputados, em 30 de maio de 2007, junto com os professores Ricardo Puttini e André Tofanello, onde **manifestaram-se a favor de controles puramente digitais** em *máquinas DRE*. Na ocasião, ofereceram serviços para desenvolvimento de protocolos de segurança para o sistema eleitoral brasileiro.

Caracterizando e confirmando que a natureza da relação profissional que os componentes do CMTSE mantêm com o TSE é de assistentes técnicos e não de auditores independentes, os membros do CMTSE foram chamados para prestar novos serviços ao TSE, sendo nomeados pela Portaria TSE 648 [29] e Portaria TSE 649 [30], de 09 de setembro de 2009, para comporem as comissões deliberativas e administrativas dos Testes de Segurança, conforme descrito na Seção 4.1.1 do Capítulo 4 deste relatório.

O fato de todos os indicados para compor o CMTSE tenham antes se declarado alinhados com as teses do seu coordenador indica que a fuga ao contraditório tenha sido um dos critérios para sua escolha.

---

27 Os assistentes técnicos do Senado para acompanhar a elaboração desse relatório, que também são membros do CMind, apresentaram quesitos que foram encaminhados, na ocasião, ao Reitor da UNICAMP. Mas os autores do relatório não permitiram o acompanhamento do estudo e nem responderam aos quesitos.

Ver mais detalhes em: *http://www.votoseguro.org/textos/relfuncamp1.htm*

Ofício do Senado à Unicamp em: *http://www.votoseguro.org/textos/oficiosve.htm*

28 Ver a desautorização do Conselho Universitário da UNICAMP para uso do nome da instituição por seus servidores, em: *http://www.pg.unicamp.br/delicad/2003/CAD04A03.htm*

29 Ver em: *http://www.tse.gov.br/internet/eleicoes/arquivos/portaria_comissao_avaliadora_assinado.pdf*

30 Ver em: *http://www.tse.gov.br/internet/eleicoes/arquivos/portaria_comissao_disciplinadora_assinado.pdf*

Sob esses critérios de seleção, **a imparcialidade e a "multidisciplinaridade" do CMTSE restaram prejudicadas** pela similaridade da formação, de experiência, de relação profissional e de predisposição de seus membros quanto ao objeto de análise.

Não há, entre eles, representantes da área do Direito. Isso reduziu a abrangência da análise que o CMTSE pôde produzir, levando à **omissão** em importantes questões, citadas nos *Relatórios CCJC,* que sobrepujam sua área tecnológica estrita, como, por exemplo, o comprometimento do **Princípio da Tripartição de Poderes** e do **Princípio da Publicidade** com a informatização do processo eleitoral brasileiro.

Também, é marcante, no CMTSE, a ausência de fiscais externos ao TSE - representantes dos partidos políticos, da OAB ou do Ministério Público – com experiência direta que pudesse contribuir com uma visão externa sobre as dificuldades que as entidades fiscais do sistema eleitoral encontram para exercer, na prática, essa função.

Essa ausência de fiscais externos com experiência prática constituiu uma lacuna marcante, que levou o CMTSE a conhecer apenas a visão teórica das salvaguardas criadas pelo administrador eleitoral, deixando de consultar aqueles que poderiam apresentar informações sobre a efetividade, a eficácia e a viabilidade econômica das formas de auditoria permitidas.

Por isso, **o uso de aspas** ao citar-se o *Comitê "Multidisciplinar" do TSE* nesta Réplica, já que todos seus componentes são técnicos da área de Tecnologia da Informação, descaracterizando a ideia de grupo multidisciplinar real, que, por definição, consiste em reunir membros com atuação em disciplinas e pesquisas em diversas áreas do saber, o que não ocorre no caso do CMTSE.

Ademais, a relação pessoal e profissional dos membros do CMTSE com a administração eleitoral os qualifica, do ponto de vista estritamente legal, como **assistentes técnicos do TSE** e, portanto, **sem isenção formal para a função de auditores independentes e imparciais** neste caso em que o fruto do trabalho administrativo do seu contratante é o alvo do questionamento externo a ser avaliado.

Enfim, considerando que o *Relatório CCJC 2007* e o *Relatório CCJC 2008* apresentam algumas críticas ao produto da administração eleitoral e que o CMTSE deveria avaliar essas críticas, com a composição escolhida, **o CMTSE foi montado para evitar conhecer o contraditório e, sob a óptica jurídica estrita, não parece estar qualificado para exercer essa avaliação de forma imparcial**.

O que faz lembrar a máxima de Upton Sinclair:

> *"It is difficult to get a man to understand something when his salary depends upon his not understanding it"*
>
> *"É dificil fazer um homem entender alguma coisa quando seu salário depende dele não entendê-la"*
>
> ***Upton Sinclair** (1878 - 1968) escritor e ativista político norte-americano, vencedor do Premio Pulitzer em 1943*

2.2 Sobre a Escolha dos Assessores do CMTSE

A dependência do CMTSE ao administrador eleitoral foi reforçada pela escolha dos seus consultores e assessores. Na Seção 1.1 do seu relatório informa-se que "*o Comitê foi assessorado por membros da equipe técnica do TSE diretamente ligados ao desenvolvimento da urna eletrônica e do sistema eletrônico de votação brasileiro*".

Essa assessoria foi dada exclusivamente por funcionários do TSE. **Nenhuma pessoa independente ao corpo técnico do administrador eleitoral foi ouvida pelo CMTSE** para apresentar contestações ou alternativas ao discurso oficial.

É natural esperar que os técnicos diretamente envolvidos no desenvolvimento das urnas eletrônicas, o objeto final sob avaliação do comitê, filtrassem as informações apresentadas, omitindo aquelas que, por qualquer motivo, pudessem macular o ideal concebido por eles próprios.

Por exemplo, ao avaliar as salvaguardas do sistema, o CMTSE, descreveu nas Subseções 2.1.1 e 2.1.2 do seu relatório, a **concepção ideal** da apresentação dos sistemas aos representantes dos partidos, da OAB e do MP durante 180 dias anteriores à eleição, sugerindo que o procedimento é efetivo e satisfatório para a transparência do processo.

Porém, por não ter sido ouvido nenhum dos representantes dessas entidades fiscalizadoras, que realmente acompanharam a apresentação dos sistemas desde 2004 - **e que são todos membros deste CMind** -, no relato do CMTSE não são citados os seguintes fatos observados diretamente pelos fiscais externos em 2008:

- **Dados Secretos** – foram mantidos secretos e longe do conhecimento dos fiscais, segundo a *Informação nº 002/2008-STI/TSE* do coordenador do CMTSE (vide Anexo 1 desta Réplica), os relatórios parciais desenvolvidos pelas entidades FACTI e CenPRA (atual CTI/MCT), que induziram centenas de alterações nos programas das urnas, algumas delas **introduzidas até nos últimos minutos antes da compilação final.**

- No dia da compilação e lacração dos sistemas, foram descobertas **diferenças entre os programas-fonte que eram apresentados para análise** dos fiscais externos **e os programas-fonte que estavam sendo compilados de fato.** Em ato autoritário, este fato foi omitido na ata da cerimônia, e petição para incluí-lo foi ignorada (vide detalhes na Subseção 3.1.10 desta Réplica).

- Ao contrário do citado na Subseção 2.1.2 do *Relatório CMTSE*, uma parte dos arquivos fixos das urnas eletrônicas não teve seus **resumos criptográficos** calculados ao final da cerimônia oficial em 15/09/2008. Contrariando a lei, **esse cálculo foi feito no dia 25/09/2008, 10 dias depois de terminada a cerimônia, sem a presença dos representantes externos** (vide data no documento oficial no Anexo 2.2).

- Apesar de ser dito na Subseção 2.1.1 do *Relatório CMTSE* que "*não é possível modificar ou executar qualquer trecho de código neste ambiente de acompanhamento externo*", alguns **programas,** contendo roteiros de compilação (*scripts),* **foram alterados de última hora naquele ambiente para corrigir erros** que impediam a compilação correta.

- A maior parte da **documentação** descritiva do sistema **só ficou pronta DEPOIS** do encerramento do prazo da apresentação.

Esses fatos comprometem totalmente a finalidade da alegada salvaguarda, pois não adianta projetar uma apresentação ideal dos sistemas eleitorais para conhecimento e fiscalização externa se, na prática, as **regras estabelecidas para segurança não são cumpridas**, se os **sistemas apresentados têm diferenças em relação aos que serão usados** nas eleições e se valores essenciais para a verificação de integridade dos sistemas (resumos e assinaturas digitais) não são calculados na presença dos fiscais.

Todas essas informações, acima referidas, seriam significativas para a análise do CMTSE, mas **acabaram ignoradas** em seu relatório por serem embaraçosas para os assessores escolhidos porque, a rigor, **foram consequências de erro, de falta de planejamento ou de autoritarismo dos próprios assessores do CMTSE**.

Lembre-se, ainda, que esses problemas na apresentação dos sistemas **são apenas um exemplo** de como as diferenças entre o ideal descrito pelos assessores do CMTSE e a realidade prática observada pelos fiscais externos pode apontar para conclusões muito diferentes sobre a eficácia das salvaguardas descritas.

Outros exemplos, de outras áreas, outros atores e em outros momentos, serão detalhados ao longo dos Capítulos 3 e 4 desta Réplica.

2.3 Sobre as Referências Bibliográficas

São escassas as citações e referências bibliográficas no *Relatório do CMTSE*, a começar pela **completa omissão** relativa à especificação dos *Relatórios da CCJC*, objetos da análise. **Não é dito qual dos dois foi analisado ou se foram ambos**.

As citações e referências que aparecem no corpo do relatório do CMTSE são genéricas, nunca especificando de forma objetiva o capítulo ou ponto referido na obra citada.

Ao longo do texto, são apresentadas apenas duas referências bibliográficas formais. Somente uma delas permite a identificação do objeto apontado. A outra é ambígua e não remete a um documento único.

Há, também, caso de texto citado sem a devida referência bibliográfica correta e explícita, como o relatório "*Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica)*", indevidamente [31] chamado como "*Relatório da UNICAMP"* na Seção 2.1.3 do *Relatório CMTSE*.

Há, ainda, erros de forma até em referência interna do *Relatório CMTSE*. O "*Anexo I*", ao final do documento, é referido como "*Anexo A*" na Seção 2.4, revelando descompromisso e desatenção na revisão final do texto.

As duas mais graves dessas impropriedades formais, que comprometem a qualidade formal do *Relatório CMTSE*, são descritas, a seguir, nas Subseções 2.3.1 e 2.3.2 desta Réplica.

31 Ver a desautorização do Conselho Universitário da UNICAMP para uso do nome da instituição por seus servidores, em: *http://www.pg.unicamp.br/delicad/2003/CAD04A03.htm*

2.3.1 Os Relatórios da CCJC da Câmara dos Deputados

A CCJC da Câmara dos Deputados produziu dois relatórios sobre a questão do voto eletrônico, referenciados como *Relatório CCJC 2007* e *Relatório CCJC 2008*.

O *Relatório CCJC 2007* foi elaborado após as audiências públicas de 2007, com a presença do Dr. Mamede Lima-Marques e do Sr. Giuseppe Janino, membros do CMTSE, e do Dr. Clovis Fernandes e do Eng. Amílcar Brunazo Filho, membros do CMind. O relatório foi entregue ao presidente do TSE no dia 03 de março de 2009 [32].

O *Relatório CCJC 2008* foi elaborado após as audiências de 2008, novamente com a presença do Sr. Giuseppe Janino, Coordenador do CMTSE, e do Dr. Jorge Stolfi e do Prof. Pedro Antônio Dourado Rezende, membros deste CMind. Foi entregue ao presidente do TSE pelo seu autor, o Deputado Gerson Peres, no dia 18 de fevereiro de 2009 [33].

O *Relatório CCJC 2007* recebeu o título "***Relatório da Subcomissão Especial do Voto Eletrônico da CCJC da Câmara dos Deputados***" e tem escopo mais abrangente – multidisciplinar -, abordando temas técnicos, econômicos e jurídicos como os seguintes:

- Consequências da concentração de poderes no processo eleitoral brasileiro.
- Falta de verba oficial para as entidades encarregadas da fiscalização eleitoral.
- *Auditoria Independente do Software* sobre a *Apuração*, por recontagem de 2% dos *votos impressos conferíveis pelo eleitor* (VICE).
- Uso de software de código aberto nas urnas eletrônicas.
- Permissão do voto em trânsito.

Ao final do *Relatório CCJC 2007,* referente a face legislativa da questão, são propostos quatro Projetos de Lei sobre esses temas.

Destaque-se, no entanto, que no *Relatório CCJC 2007* nada é proposto a respeito da separação física e lógica entre a máquina de identificar o eleitor e a máquina de votar.

Já o *Relatório CCJC 2008* tem escopo mais restrito, ficando centrado em duas questões tecnológicas e apresentando os seguintes itens como necessários:

- Separação entre a máquina de identificar o eleitor e a máquina de votar.
- *Registro independente do voto* (RICE), impresso ou escaneado, para permitir *Auditoria Independente do Software* sobre a *Apuração*.

A Presidência do TSE formalizou a criação do seu Comitê "Multidisciplinar" através da *Portaria TSE 192/2009* com o explicito objetivo de:

> "*... analisar as sugestões apresentadas no* ***Relatório da Subcomissão Especial do Voto Eletrônico da CCJC da Câmara dos Deputados***"

Como a portaria que criou o CMTSE cita literalmente o título do *Relatório CCJC 2007* e denomina o comitê como multidisciplinar, aponta que esse seria o seu relatório-alvo.

---

32 Ver notícia do TSE em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1170472*

33 Ver noticia do TSE em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1156471*

No entanto, no Capítulo 3 do *Relatório CMTSE*, ao citar o relatório da CCJC analisado, reduz a descrição do seu conteúdo apenas ao seguinte:

> *"3 ANÁLISE DAS PROPOSTAS DA SUBCOMISSÃO DA CCJC*
> *A subcomissão da CCJC propôs que fossem introduzidas as seguintes modificações no sistema eletrônico de votação:*
> 1. *a identificação do eleitor deve ser feita em dispositivo separado da máquina que registra o voto, como garantia do sigilo do voto;*
> 2. *impressão do voto como evidência de sua correta contabilização."*

Essa descrição é mais condizente com o *Relatório CCJC 2008*, a saber:

1. A separação das máquinas, que aparece citada no item 1 do Capítulo 3 do *Relatório CMTSE,* não foi abordada no *Relatório CCJC 2007*.
2. Outros temas abordados no *Relatório CCJC 2007* não estão citados, como o acúmulo de poderes, a falta de verba para a fiscalização, a adoção de software de código aberto e do voto em trânsito.
3. Não há referência, no *Relatório CMTSE*, aos quatro Projetos de Lei eleitorais presentes no *Relatório CCJC 2007*.

Desta forma, por não reconhecer a existência de dois relatórios e **ao citar o título de um e o conteúdo do outro**, o ***Relatório CMTSE* não deixa claro e explícito qual dos relatórios da CCJC é o objeto de sua avaliação**.

Trata-se de um **evidente erro de forma** na especificação do seu objeto - item preliminar essencial - **que descredencia do nível acadêmico**, implícito na escolha dos autores indicados, o *Relatório CMTSE*.

Nesta Réplica, para contornar os efeitos desse crasso erro sobre formalidade essencial, consideramos a existência dos dois relatórios da CCJC na análise dos argumentos oferecidos pelo *Relatório CMTSE*.

2.3.2 O Relatório Brennan e as Diretrizes VVSG

O *Relatório CMTSE* apresenta, **por duas vezes**, a seguinte referência bibliográfica:

> ***Brennan**; Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission AUGUST 31, 2007).*

Na Seção 3.2 do *Relatório CMTSE*, essa referência está associada à expressão "*relevantes estudos [que justificariam a adoção de máquinas de votar DRE sem VICE]*".

Na Subseção 4.1.3 do *Relatório CMTSE*, a mesma referência aparece associada à expressão: *"há estudos que comprovam ineficácias em todos os sistemas, com e sem impressão do voto. Esses mesmos estudos fazem recomendações caso se adote cada um dos tipos de sistemas*".

Porém, **a referência, como citada, é ambígua**.

A palavra "*Brennan*", destacada em negrito como se fosse nome do autor, no mundo do voto eletrônico remete ao *Brennan Center for Justice* da *New York University School of Law* que, em junho de 2006, publicou um importante estudo[34], denominado *"The Machinery of Democracy: protecting elections in an electronic world",* o qual passa aqui a ser referido como ***Relatório Brennan***.

Já o restante da referência bibliográfica citada pelo CMTSE, remete diretamente às *Voluntary Voting System Guidelines* (VVSG)[35], preparadas pela agência federal norte-americana *U.S. Election Assistance Commission* (US-EAC) com a colaboração do *National Institute of Standards and Technology* (NIST) em agosto de 2007, as quais passam a ser aqui referidas como ***Diretrizes VVSG***.

Tanto o *Relatório Brennan* quanto as *Diretrizes VVSG* fazem jus ao epíteto de relevantes estudos. São trabalhos desenvolvidos por grande equipes de especialistas, com composição verdadeiramente multidisciplinar, que analisaram todos os tipos de equipamentos eletrônicos de votação conhecidos, a saber, *máquinas DRE sem VICE*, *máquinas DRE com VICE* e máquinas digitalizadoras do voto, estendendo o estudo até sistemas ainda em desenvolvimento teórico, referenciados na categoria *Innovation Class* ou formas alternativas de *RICE* .

O *Relatório Brennan* apresentou o primeiro estudo acadêmico de **avaliação de riscos** de sistemas eleitorais eletrônicos. Descreveu 128 possíveis tipos de fraude eleitoral e propôs um método de cálculo de riscos e danos potenciais, que inclui a medida da quantidade de participantes ativos necessários para mudar indevidamente o resultado de uma eleição majoritária.

---

34 **Norden L.D. et al.** - *The Machinery of Democracy: protecting elections in an electronic world.* New York: Brennan Center of Justice, NYU, 27/06/2006 -
relatório completo em: *http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf*
sumário executivo em: *http://organikrecords.com/corporatenewslies/BrennanCenter_ExecutiveSummary.pdf*
sumário em português: *http://www.votoseguro.org/textos/brennan-pt.pdf*

35 *Voluntary Voting System Guidelines.* USA: U.S. Election Assistance Commission, 31/08/2007 -
página virtual em: http://www.eac.gov/vvsg
relatório completo em: http://www.eac.gov/files/vvsg/Final-TGDC-VVSG-08312007.pdf

Deste estudo, sua principal conclusão é que **a fraude "*menos difícil*"**, ou seja, a de melhor relação custo-benefício para o fraudador, **é a adulteração do software em máquinas DRE sem VICE** - como as urnas eletrônicas brasileiras.

Já as *Diretrizes VVSG,* na prática, constituem a norma técnica norte-americana sobre equipamentos de votação. Foram elaboradas em conjunto com o *National Institute of Standards and Technology* (NIST), contando com quase 600 páginas.

Apresentam detalhada lista de normas e recomendações de segurança para todos os sistemas eleitorais eletrônicos conhecidos e, desde a última versão de 2007, passou a exigir a *Independência do Software*[36] nas máquinas de votar eletrônicas, o que levou ao **descredenciamento sumário das *máquinas DRE sem VICE***.

Nestas condições, por apresentar por duas vezes a mesma referência bibliográfica incompleta e ambígua, sem identificar o trecho referenciado na obra citada, o ***Relatório CMTSE* dificulta a localização do texto que estaria indicando para sustentar a sua tese, impedindo o leitor de avaliar e confirmar como essa referência corroboraria seu argumento.**

Trata-se de **mais um erro evidente de forma**, e que, neste caso, aparece duas vezes no *Relatório CMTSE.*

Esse erro formal repetido, **é ainda agravado** com a constatação, descrita na Seção 4.4 desta Réplica, de que consultadas as fontes ambiguamente apontadas, encontra-se, em ambas, **asserção que diz exatamente o contrário do contexto da citação no *Relatório CMTSE***.

A **associação de três erros formais distintos** – incompletude, ambiguidade e inversão de mérito -, a princípio independentes mas repetidos em dois pontos do relatório, estimula a hipótese de não ter sido simples erro de revisão.

Para sustentar esta Réplica, consideraremos tanto a existência do *Relatório Brennan* quanto das *Diretrizes VVSG* na análise dos argumentos da CMTSE.

36 Ver a Seção: *Introduction: 2.4 das Diretrizes VVSG ;* e a Seção 3.3 deste relatório.

3 INFORMAÇÕES PRELIMINARES

Apresenta-se, neste capítulo, uma série de informações preliminares que ajudarão a ilustrar e esclarecer a análise que será desenvolvida no Capítulo 4 seguinte.

De início, são descrições de alguns casos concretos relacionados às **dificuldades de fiscalização do processo eleitoral eletrônico pelos Partidos Políticos**, apresentando situações vividas pelos fiscais desde a apresentação dos sistemas no TSE até casos ocorridos nos cartórios eleitorais de cidades espalhadas pelo país.

A seguir é descrita a **experiência de fiscalização pela OAB**, destacando-se suas dificuldades em 2004 e o abandono da fiscalização em 2006 e 2008.

Ao final deste capítulo, introduz-se o conceito de ***Independência do Software em Sistemas Eleitorais,*** que vem ganhando cada vez mais espaço e tem sido adotado como referência técnica em muitos países que passaram a dar maior atenção às questões de transparência e confiabilidade geral de sistemas eletrônicos de votação.

3.1 Dificuldades de Fiscalização pelos Partidos - Descrição de Casos Concretos

A cada nova eleição, crescem muito as denúncias de problemas nas urnas eletrônicas, como foto trocada do candidato, votação encerrada antes da confirmação do eleitor, eleitor impedido de votar, etc.

Devido à carga emocional do evento, frequentemente esses casos vêm acompanhados de acusações de fraudes e repercutem na imprensa.

Na Seção 2.4 do *Relatório CMTSE*, se generaliza uma explicação simplória de que *"muitos desses relatos não são apresentados à imprensa por má fé, mas por falta de conhecimento do processo eletrônico de votação".* No Anexo A do *Relatório CMTSE* é apresentada explicação para 3 casos que repercutiram na mídia televisada.

No entanto, existem muitos **casos bem documentados** de problemas no processo eleitoral eletrônico, que **tornam ineficaz a fiscalização pelos partidos políticos** e **que nunca receberam explicação convincente** do administrador eleitoral e também não foram explicados pelo CMTSE, em que pese sua opção espontânea de "*ampliar o escopo deste rico debate*".

Os casos documentados aqui descritos não se ajustam aos rótulos de "*denunciantes desinformados*" ou de "*choro de perdedor*" - há até dois casos em que o denunciante ganhou a eleição - e ainda servem de exemplo de **como está desequilibrado o jogo de poder entre fiscais e fiscalizados no processo eleitoral brasileiro**, com flagrante desvantagem dos fiscais.

3.1.1 Coação em Massa de Eleitores - 1998 e 2008

A opção do administrador eleitoral por identificar o eleitor usando a própria urna eletrônica, seja pelo número do título ou pela biometria, **é um reforço muito forte** à ideia de que o voto poderá ser identificado posteriormente.

Em função desta peculiaridade de nosso sistema, a cada eleição crescem as denúncias de coação de eleitores sob a alegação de que o voto será identificado nas urnas eletrônicas. É uma modalidade nova de golpe eleitoral que chegou com nossa urna eletrônica e tem sido denominada como ***Voto-de-Cabresto-em-Massa***.

Esse problema já havia sido detectado em 1998, na segunda eleição com urnas eletrônicas, quando 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.

O TRE-RS teve que apresentar repetidos esclarecimentos pela grande imprensa[37], tentando desconvencer os eleitores intimidados pelo boato.

Dez anos depois, notícia[38] divulgada pelo TSE pouco antes da eleição de 2008, comprova a persistência do problema. Revela os esforços do TRE-RJ por meio de campanha publicitária pela TV para:

> "... ***esclarecer o eleitores quanto à inviolabilidade do voto****, em resposta à ação de grupos criminosos que atuam em comunidades carentes do Rio de Janeiro que estariam* **coagindo os eleitores** *dessas comunidades, afirmando ser possível identificar aqueles que não votassem nos candidatos impostos pelos criminosos*"

Para viabilizar o voto-de-cabresto-em-massa não é necessário que o agente coator consiga quebrar, de fato, o sigilo do voto do eleitor coagido. **Basta convencê-lo de que conseguiria** e, para isso, **a identificação do eleitor na própria máquina de votar ajuda muito ao infrator**.

Não se sabe avaliar como o conflito psicológico, entre o boato e o contra-boato, se resolve nas mentes dos eleitores: eles acreditarão na propaganda corretiva do administrador eleitoral ou preferirão, por via das dúvidas, submeter-se ao voto-de-cabresto por medo do poder do coator?

O fato é que **o Voto-de-Cabresto-em-Massa** sobrevive e cresce a cada eleição, explorando a equivocada forma de identificar os eleitores na mesma máquina de votar que a autoridade eleitoral escolheu adotar.

A projetada adoção de **identificação biométrica** do eleitor na própria máquina de votar, que tem recebido ampla divulgação publicitária pelo TSE, vai reforçar, no imaginário popular, a ideia de que é possível identificar o voto nas urnas eletrônicas e, com boa certeza, **vai servir de estímulo para o crescimento desta modalidade de fraude**.

---

37 Ver a reportagem "*Justiça Eleitoral Garante Sigilo do Voto*", Jornal ZeroHora, 23/10/1998 - pág. 20

38 Ver em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1037407*

3.1.2 Programas Modificados - 2000

Nas eleições de 2000, o TSE deixou de cumprir vários mandamentos da lei eleitoral relativos a procedimentos de segurança na apresentação dos programas aos Partidos e ao MP, dentre os quais destacam-se os dois seguintes:

1. Dois terços do software das urnas eletrônicas, que incluía o Sistema Operacional VirtuOS da Microbase e a biblioteca de criptografia da ABIN, **foram mantidos secretos** aos partidos e até aos próprios funcionários do TSE.
2. Depois de homologado, gravado em CD-ROM e lacrado na frente do MP e dos Partidos em 06 de agosto de 2000, **o software das urnas foi modificado** de forma que **os programas de computador colocados nas urnas eletrônicas em 2000 eram diferentes da versão oficial homologada**.

Uma impugnação[39] a esses fatos, apresentada por partido político, foi rejeitada pela Justiça Eleitoral; as mesmas pessoas eram os juízes, peritos e réus no processo.

Essas ilegalidades praticadas pela autoridade eleitoral em 2000 acabaram sendo comprovadas pelos seguintes acontecimentos futuros:

1. O chamado *Relatório "Unicamp"* apresentou dados que desmentiam[40] o então secretário de Informática do TSE, revelando que eram falsos os argumentos usados para indeferir e arquivar a impugnação.
2. Numa entrevista ao Jornal do Brasil [41], os técnicos Oswaldo Catsumi e Paulo Nakaya, do TSE, confessaram que **os programas das urnas só ficariam prontos no dia 5 de setembro**, **um mês após sua lacração oficial**. Uma perícia em Camaçari [42], BA, comprovou que **os programas nas urnas eletrônicas não eram os mesmos homologados** em agosto de 2000 no TSE.
3. Em comunicado público[43], em 2006, a empresa Microbase confirma que o TSE **não cumpria a legislação em vigor** na apresentação e lacração dos sistemas.
4. Na audiência pública perante a CCJC da Câmara, em 25 de novembro de 2008, o Eng. Frederico Gregório, diretor da Microbase, confirmou que o software denominado VirtuOS, de sua autoria e usado em urnas até as eleições de 2006, **nunca teve seu código-fonte apresentado** ao MP, OAB ou partidos e nem mesmo aos funcionários do próprio TSE.

Embora as ilegalidades, denunciadas tempestivamente em 2002, tenham sido comprovadas por eventos posteriores, nenhuma consequência ou responsabilização daí adveio. O administrador eleitoral continua se omitindo sobre esses fatos, sem apresentar explicações ou esclarecimentos.

O CMTSE, nas conclusões na Subseção 4.1:5, reconhece o abuso no passado, mas não procura explicá-los. Satisfaz-se na esperança que não se repetirão, ao dizer:

> *"É verdade que, no passado, **em vários momentos o TSE não foi suficientemente responsivo às demandas por maior transparência**. Entretanto, as iniciativas dos últimos anos mostram claramente uma mudança de atitude, com várias medidas já implantadas"*

---

39 Ver em: *http://www.pdt.org.br/diversos/acaourna.htm*

40 Ver em: *http://www.votoseguro.org/textos/unicamp1.htm*

41 "*TSE abre programas após eleições*". Jornal do Brasil, Caderno Política, pág. 4 – 30 de agosto de 2000

42 Ver item (2.vi) do parecer em: *http://www.votoseguro.org/textos/camacari2.htm*

43 Ver item (5) da nota em: *http://www.votoseguro.org/arquivos/microbase06-nota1.pdf*

3.1.3 O Caso Diadema, SP - 2000

Foi nesse município, vizinho à cidade de São Paulo, que em 2000 primeiro se constatou e documentou um rol de irregularidades no processo de votação eletrônica e onde se revelaram, com clareza, as nefastas consequências da concentração de poderes da Justiça Eleitoral.

Para se ter ideia da truculência do administrador eleitoral naquela época, aos Partidos **era negado acesso a todos os *Arquivos Digitais de Auditoria*** gerados pelo sistema, sob o argumento de conterem informações próprias de segurança nacional.

Somente após 9 meses da eleição, e não antes de se recorrer ao TSE, os partidos concorrentes obtiveram acesso a apenas os *Arquivos de LOG* das urnas.

A análise desses arquivos revelou que **todas as urnas eletrônicas tinham sido carregadas fora da cerimônia oficial de carga e lacração**, dias antes da convocação por edital público, tendo todas ficado sem lacres durante dias.

A grande maioria das urnas eletrônicas utilizadas - 431 de 451 - foram inseminadas com o software de votação nos dias 22 e 23 de setembro, 2 em 24/9, 7 em 25/9, 2 em 26/9, sendo que todas elas só foram lacradas no dia 28/9.

Esses dados mostravam que a totalidade das urnas eletrônicas de Diadema em 2000, estiveram carregadas com os programas mas **sem lacre** e sem a presença de fiscais dos partidos políticos por vários dias, em **total oposição aos procedimentos de segurança apontados como salvaguardas na Subseção 2.1.3 do *Relatório CMTSE***.

O resultado do processo judicial aberto contra os procedimentos de preparação das urnas pelos funcionários da Justiça Eleitoral foi pelo **indeferimento do pedido**, alegando, a própria Justiça Eleitoral, não haver elementos suficientes para infirmar a alegação. **Perícia nas urnas não foi deferida**.

Este Caso Diadema 2000, é mais um bom exemplo de que "*no passado, em vários momentos o TSE não foi suficientemente responsivo às demandas por maior transparência...*", como foi citado no *Relatório CMTSE* em suas conclusões.

A indignação e **o sentimento de impotência** perante o tratamento autoritário e obscuro que o caso recebeu da autoridade eleitoral, levou o candidato denunciante das irregularidades, à atitude radical de iniciar uma greve de fome que durou 10 dias.

3.1.4 Assinaturas Digitais Divergentes - 2002 e 2008

Na Seção 2.1.2 do *Relatório CMTSE* é dito que geração de resumos digitais (*Tabelas de Hash*) durante a cerimônia de lacração dos sistemas no TSE, perante o MP, a OAB e os Partidos, é uma das salvaguardas do sistema. Porém, nem sempre esse procedimento de segurança foi cumprido com o rigor necessário para sua mínima eficácia.

Nas eleições de 2002 - 2º turno - e de 2008, fiscais de partidos, ao verificarem os arquivos carregados nas urnas eletrônicas, detectaram a presença de um **conjunto de arquivos com resumos digitais diferentes do oficial homologado** nas respectivas cerimônias de lacração dos sistemas (vide Anexo 2 desta Réplica).

Em 2002, a diferença foi descoberta pelo fiscal eng. Hebert Rodrigues Pereira na cidade de Campina Grande, PB, e em 2008 a fiscal adv. Maria Cortiz (coautora desta réplica) encontrou 16 arquivos não assinados ou *"sobrantes"* nas urnas de Timon, MA.

Nos dois casos, a providência dada pelo administrador eleitoral foi a de publicar novas *Tabelas de Hash,* **calculadas a portas fechadas, fora de uma cerimônia oficial perante os agentes fiscais externos**, impedindo-os de saber quais programas foram assinados, e considerar válido, *a posteriori,* o procedimento de carga das urnas onde os erros foram encontrados.

Detalhes do Caso Campina Grande 2002, podem ser acompanhados nas mensagens eletrônicas[44] trocadas entre os fiscais externos de então. A decisão do administrador eleitoral, naquela ocasião, foi de esconder o problema do público, da imprensa e até dos fiscais externos como mostra o memorando apresentado no Anexo 2.1, onde se passavam **instruções aos supervisores dos polos de carga das urnas para procurarem esconder o problema dos fiscais dos partidos e do MP**.

A perícia nas urnas foi indeferida. As *Tabelas de Hash* originais, que demonstravam a impropriedade, foram retiradas do sítio do TSE. Tabelas novas foram publicadas no lugar.

Em 2008 a reação do administrador eleitoral foi "*menos irregular*". Foi publicada uma nova tabela de *hashs*, mas as anteriores foram mantidas publicadas. No Anexo 2.2 apresenta-se o *fac-simile* da tabela complementar com as assinaturas dos "*arquivos sobrantes*" calculada, sem a presença de fiscais, em 25/10/2008, **dez dias depois** de encerrada a cerimônia oficial de apresentação dos sistemas.

Esses dois casos são exemplos acabados de como **a concentração de poderes é terreno fértil para a prática de abusos** que acabam por comprometer a transparência e segurança do processo eleitoral, podendo anular completamente a eficácia dos mecanismos de fiscalização externa permitidos.

O caso de 2002 comprova o dito pelo CMTSE, nas conclusões de seu relatório, que "*no passado, em vários momentos* ***o TSE não foi suficientemente responsivo às demandas por maior transparência****...*".

Já o **caso de 2008**, que praticamente repete a prática, **desmente o alegado** em seguida pelo CMTSE, de que "*... as iniciativas dos últimos anos mostram claramente uma mudança de atitude, com várias medidas já implantadas*".

---

44 Ver detalhes do Caso Campina Grande de 2002, nas mensagens eletrônicas em:
http://www.mail-archive.com/voto-eletronico@pipeline.iron.com.br/msg11814.html
http://br.groups.yahoo.com/group/votoseguro/message/784

3.1.5 O Caso Marília, SP - 2004

Os *Arquivos Digitais de Auditoria* das urnas usadas em 2004 na cidade de Marília, SP, foram obtidos no TRE, tempos depois da eleição, posto que os Juízes Eleitorais do município se recusaram a entregar os dados.

Esses arquivos indicavam ter ocorrido geração de *flashs de carga*[45] em duplicata e também discrepâncias no horário de recebimento dos Boletins de Urna da 400ª ZE.

Essas três informações, em conjunto, a saber:

1. Resistência dos juízes/administradores à auditoria;
2. Flash de carga em duplicata;
3. Discrepâncias nos recebimentos dos BU;

são compatíveis com a hipótese de fraude por "*clonagem de urnas*", que consiste num ataque interno no Cartório Eleitoral, no qual se prepara um conjunto de urnas com data antecipada para nelas efetuar uma votação prévia que gera documentos com resultados falsos, mas aceitáveis pelo sistema totalizador, e se prepara um outro grupo de urnas para serem enviadas às seções eleitorais. No momento de totalização, os disquetes de resultados dos dois grupos são trocados dentro do Cartório Eleitoral, o que caracteriza o tipo de fraude como um ataque interno.

O *Arquivo de Espelhos de Boletins de Urna* da 400ª ZE, gerado em 14/10/2004 às 15:22:55 h, indicava que **muitas seções eleitorais tiveram seus resultados recebidos para totalização antes do início da votação**.

Como exemplo, mostra-se o cabeçalho da página 45 do arquivo, referente à seção eleitoral 0008, apresentado a seguir:

Justiça Eleitoral/SP *pág.:45*
Sistema de Gerenciamento - Versão: 2.09 (Oficial) ***14/10/2004***
Eleições Municipais de 2004 ***15:22:55***
Espelho de Boletim de Urna *1º turno*

Município	ZT	Eleitores Aptos	Seções	Seções Agregadas	Seções Efetivas	N.vagas Vereadores
66818 - MARILIA	0070	141,159	309	7	302	13

Zona Eleitoral: 0400 Seção: 0008
Seções Agregadas: Esta seção não possui seções agregadas.
Aptos:530 Comparecimento: 445 Faltosos: 85
Tipo de Urna: Apurada Origem: URNA ELETRÔNICA
Data do Recebimento: 03/10/2004 6:40:28
Cód.UE: 148909 PM Cód. Carga: 090.225.521.369.572.240. 332.446
Data: 27/09/2004 Hora: 15:59:00 Cód.FC: 8D66079F

Nesse cabeçalho são apresentados a data e hora de três eventos, a saber:

1. Na segunda e terceira linha tem-se a data e hora em que o arquivo foi criado em 14/10/2004 às 15:22:55 h.
2. Na antepenúltima linha, destacado em negrito, tem-se a data e hora do recebimento do Boletim de Urna em **03/10/2004 às 6:40:28.**
3. Na última linha aparece a data e hora da carga da urna em 27/09/2004 às 15:59:00.

45 Cartões de Memória digitais usados para carregar os programas e dados oficiais nas urnas eletrônicas.

A eleição ocorreu em 03/10/2004. A hora 6:40:28 (item 2), é incompatível com o recebimento dos Boletins de Urna, os quais só são oficialmente gerados após às 17:00 h. Esse problema apareceu em todas as seções eleitorais da 400ª ZE.

Questionada a respeito, a Seção de Apoio às Eleições do TRE-SP emitiu parecer técnico em 28/02/2005, onde tentou explicar essa discrepância, afirmando que a hora de recebimento dos BU estaria grafada em padrão americano (12 h mais AM ou PM) devido ao arquivo ter sido gerado em computador no qual o sistema operacional Windows seria de versão em inglês.

O padrão brasileiro para data e hora segue o formato "*dia/mês/ano*" para a data e "*24h*" para a hora, enquanto o padrão americano usa "*mês/dia/ano*" para a data e "*12h mais AM ou PM*" para a hora.

A data e a hora de geração do arquivo em questão (item 1 - 14/10/2004 às 15:22:55), está obviamente em formato brasileiro pois não existe mês 14 e nem 15 horas no padrão americano. Isto indicaria que o arquivo fora gerado em computador configurado no padrão brasileiro.

A data e a hora da carga da urna (item 3 - 27/09/2004 às 15:59:00) também está obviamente em padrão brasileiro, mais uma vez indicando que o computador que escreveu esse dado no arquivo estava em padrão brasileiro.

A data do recebimento do boletim de urna (item 2 - data de 03/10/2004) só pode estar em padrão brasileiro, indicando o dia 3 de outubro de 2004, dia do 1º turno das eleições de 2004. Se essa data estivesse em padrão americano estaria indicando o dia 10 de março de 2004, data em que era impossível se receber Boletins de Urna, visto que o Sistema de Gerenciamento 2004 T1, segundo o parecer técnico, só foi instalado em setembro de 2004. Confirma-se, assim, que o computador que inseriu esse dado no arquivo estava em padrão brasileiro.

Já a hora de recebimento do BU (item 2 – hora 6:40:28) indica que os Boletins de Urna da 400ª ZE já tinham sido recepcionados pelo sistema de totalização **antes da eleição ter tido início**.

Houve dois processos judiciais decorrentes dessas constatações: um inquérito do Ministério Publico e uma representação de Partido Político.

Na primeira instância, o juiz que também era o responsável administrativo pelos procedimentos questionados, indeferiu os pedidos de perícia e recusou-se a mandar lacrar os computadores utilizados, para preservar eventuais provas.

Três anos depois, na terceira instância, foi reconhecida a necessidade de perícia e o processo retornou à primeira instância, mas, nesse momento, os equipamentos já haviam sido modificados pelo uso em outras eleições e as provas estavam perdidas.

Ambos processos se encerraram em 2009, **sem julgamento final, por decurso de prazo** devido a protelação dentro da própria justiça e administradora do sistema contestado. **Nenhuma perícia foi deferida** e as eventuais provas pereceram, não sendo mais possível a realização de perícia nos meios eletrônicos. **Sobre o juiz-administrador que não preservou as provas, nada recaiu**.

3.1.6 O Caso Campos do Goitacases, RJ – Eleição Suplementar 2006

Essa eleição suplementar em Campos do Goitacases, RJ, foi realizada em março de 2006 por anulação do pleito oficial de 2004.

As dificuldades de fiscalização, adiante descritas, são apresentadas pelo lado do candidato que venceu a eleição, desmentindo o refrão generalizante de que as denúncias contra as urnas eletrônicas são sempre fruto de "*choro de perdedor*".

Por interesse do candidato vencedor, foi montado um esquema de fiscalização preventiva do processo eletrônico de votação desde seu princípio.

No entanto, cada passo da fiscalização, para ser realizado, enfrentou autoritarismo e resistências nascidas dentro do corpo de membros da administração eleitoral. As cerimônias de fiscalização, obrigatórias, só foram marcadas depois de muita insistência e uma foi negada. As irregularidades encontradas só foram corrigidas quando enfrentado o autoritarismo do agente responsável.

Já de início, a autoridade eleitoral descumpriu frontalmente o Artigo 66 da Lei 9.504/97 que manda apresentar, com antecedência em cerimônia oficial, os programas de computador do sistema eleitoral aos partidos concorrentes, cerimônia esta que o CMTSE afirma ser umas das salvaguardas de segurança do sistema.

O argumento usado para justificar tal ilegalidade revela um exercício de autoritarismo desmedido. Alegou-se que **tal artigo de lei só se aplicaria a eleições oficiais que ocorrem no mês de outubro dos anos eleitorais**. Segundo essa interpretação da justiça-administração eleitoral, ela própria, nas demais eleições complementares, estaria desobrigada dessa norma legal que é, teoricamente, uma salvaguarda de segurança.

Devido ao calendário justo imposto pela mesma autoridade, não havia tempo suficiente ou mesmo órgão do poder judiciário capaz de rever a decisão.

Sem alternativa adequada, o candidato teve que desconsiderar padrões de segurança, e **foi forçado a participar de eleição eletrônica cujo software era totalmente secreto**, embora seus resumos digitais fossem publicados para "*conferência de integridade*".

O passo seguinte da fiscalização, a conferência das assinaturas no sistema gerador de mídias, foi dificultado por questões atinentes à logística e prazos. A cerimônia foi marcada, em cima da hora, na sede do TRE na capital estadual, forçando a fiscalização a idas e vindas, atravessando o Estado para acompanhar o trajeto das *Flashs-de-Carga*.

De volta a Campos do Goitacases, a fiscalização foi acompanhar as sete cerimônias de carga e lacração das urnas, que ocorriam em sequência durante 3 dias.

Constatada a regularidade das assinaturas dos programas das urnas eletrônicas, passou-se à conferencia dos dados dos candidatos concorrentes ao pleito. Verificou-se a ausência do nome de um deles no arquivo de candidatos.

O candidato, cujo nome não constava no arquivo de candidatos, estava em terceiro lugar nas pesquisas prévias e os votos que lhe fossem dados seriam anulados, afetando sobremaneira a quantidade de votos válidos, podendo resultar na vitória irregular de um dos candidatos em primeiro turno.

Para surpresa dos fiscais dos partidos, informada do fato, a Juíza eleitoral e chefe administrativa da cerimônia de carga mandou prosseguir os trabalhos de lacração das urnas, ignorando os protestos dos partidos presentes no local. Somente quando estes **exigiram que a decisão de manter a irregularidade constasse em ata**, a administradora-chefe mandou suspender a sessão e regularizar a situação.

Outra travessia do Estado foi necessária para acompanhar a nova geração de mídias e nova carga das urnas, mas, quando da conferência, verificou-se a ausência do nome do vice do mesmo candidato ausente na fase anterior. Essa ausência tinha o mesmo potencial de antecipar a eleição irregular em primeiro turmo de um candidato.

Premido pelo tempo, finalmente o administrador eleitoral teve o bom senso de realizar a terceira cerimônia de geração de mídias na própria cidade de Campos e a carga e lacração das urnas pôde se encerrar.

A cerimônia oficial obrigatória seguinte, chamada de Oficialização do Totalizador, **não foi marcada** pela autoridade eleitoral local. Levou horas de tratativas, para convencimento dos servidores eleitorais, de que havia necessidade de conferência das assinaturas digitais dos programas instalados nos computadores de totalização antes da oficialização do sistema.

Aberta a cerimônia, encontrou-se um programa instalado no sistema de totalização cujo resumo digital diferia da tabela obtida, a duras penas, no TSE.

Alertada a servidora do TRE/RJ, que chefiava os trabalhos, sobre a irregularidade, sua explicação é que seria um fato normal, insignificante e que a oficialização do totalizador poderia ser completada. Novamente, somente quando os fiscais presentes exigiram constar em ata a irregularidade encontrada, a cerimônia foi suspensa para reinstalação do sistema de totalização e, no dia seguinte com a votação já em andamento, nova oficialização pôde ser feita com todas as assinaturas digitais dos programas de totalização coincidindo com a tabela do TSE.

As tentativas das autoridades eleitorais locais, apoiadas em juízes, para dar continuidade aos preparativos oficiais mesmo diante de irregularidades constatadas e sua retração quando exigido que os fatos fossem registrados em ata, são mais exemplos de como o acúmulo de poderes no processo eleitoral brasileiro facilita o autoritarismo a ponto de inibir e até tornar inócua a fiscalização pelos partidos.

O CMTSE, no entanto, por não ter ido a campo e apenas ter como consultores os técnicos do TSE, não constatou essa realidade em seu relatório.

3.1.7 O Caso Alagoas - 2006

A eleição para governador de Alagoas em 2006 teve o resultado questionado pelo candidato que ficou em segundo lugar, uma vez que ele entendia que os resultados potenciais apontados pelas as pesquisas eleitorais prévias foram flagrantemente contrariados, até mesmo em seus redutos eleitorais.

Para avaliar a confiabilidade do resultado eleitoral foi promovida uma análise do *Arquivos Digitais de Auditoria* das urnas eletrônicas.

Resume-se a seguir o desdobramento técnico e jurídico desse caso, cujo detalhamento[46] e exemplos pode ser acompanhado em página no sítio do Fórum do Voto Eletrônico na Internet.

Na primeira semana após a eleição, para cumprir os prazos legais, foi desenvolvido um relatório preliminar[47] que detectou **corrupção nos *Arquivos LOG* em mais de 2,5% das urnas eletrônicas utilizadas,** colocando sob suspeição o resultado da votação e apuração nessas urnas. Entre a diversidade de lançamentos impróprios encontrados nos *arquivos LOG* de Alagoas 2006, havia o seguinte:

- Mudança do número do município da urna, depois de carregada e lacrada.
- Mudança do número da própria urna, depois de carregada e lacrada.
- Registro de eventos inexistentes como "*código para uso futuro*".
- Omissão de eventos reais ocorridos.
- Sequência de substituição de urnas com ordenação irregular.

Um processo judicial foi aberto propondo o desenvolvimento de perícias para determinar o comprometimento do resultado, em vista do comprovado funcionamento irregular das urnas eletrônicas.

A Secretaria de Tecnologia de Informação (STI/TSE), chamada a se manifestar na pessoa do coordenador do CMTSE, confirmou a ocorrência de "*arquivos de LOG que já apresentavam perda de integridade, parcial ou total, quando gerados"* nas urnas eletrônicas, mas afirmava, mesmo sem ter apresentado nenhuma análise dos *arquivos RDV* (de votos digitais) e dos *arquivos BU* (de resultados), que a **perda da integridade dos *Arquivos de Auditoria* não teria atingido os resultados**.

Impedindo que sua afirmação pudesse ser verificada, a Secretaria de Tecnologia de Informação do TSE, através da Informação nº 90/2006-ASPLAN/STI, de dezembro de 2006, **negou o acesso dos auditores externos aos *arquivos RDV*** para que sua integridade pudesse ser constatada ou não. Para manter os dados de auditoria do resultado distantes dos olhos dos auditores, a STI/TSE enfrentou até ordem do juiz-corregedor do TRE-AL e se negou a decifrar os arquivos para serem entregues aos requerentes.

Um segundo relatório[48] dos auditores externos[49], elaborado com mais profundidade e apresentado dois meses depois do primeiro, demonstrou que as explicações do relatório STI/TSE sobre os motivos da perda de integridade dos dados de controle eram insuficientes, apontando ainda o seguinte:

---

46 Ver em: *http://www.votoseguro.org/textos/alagoas1.htm*

47 **Carvalho, M.A.M.** et al. - *Laudo de Avaliação dos Dados Oficiais da Eleição de Alagoas 2006* . Alagoas: outubro de 2006 – *http://www.votoseguro.org/arquivos/AL06-laudoBCC.zip*

48 **Fernandes, C.T**. - *Radiografia das Urnas Eleitorais.* S. J. dos Campos: ITA, dezembro de 2006 - *http://www.votoseguro.org/arquivos/AL06-laudoFerITA.zip*

49 Todos os autores dos dois relatórios externos do Caso Alagoas 2006 são membros deste CMind.

- Havia 13 tipos diferentes de irregularidades nos *arquivos LOG*, que **atingiram 2282 (44%) das 5166 urnas utilizadas**.
- Mais de 25% dos *arquivos LOG* deixaram de registrar o evento de auto-teste, obrigatório segundo a regulamentação.
- Havia uma **diferença superior a 22 mil entre o total de votos válidos para o pleito de governador** registrados nos *arquivos LOG* e os registrados nos *arquivos BU*.

Para ilustrar e reforçar a tese de falta de confiabilidade dos resultados dessas urnas eletrônicas utilizadas em Alagoas, foi apresentado o exemplo a seguir, de *arquivo LOG* que estava mesclado com o *arquivo BU* :

trecho inicial (1024 caracteres) do *Arquivo LOG* de nome “10x48sdk.rl1 ”
da seção eleitoral 0139 da Zona Eleitoral 0035 do município de Senador Teotônio Vilela, AL

```
_____________________________________

Total de votos de Legenda       : 0022
Brancos                         : 0003
Nulos                           : 0008
Total Apurado                   : 0241

Código Verificador: 25054

=====================================

SENADOR(A)

Nome do candidato       Nro cand Votos

  RONALDO LESSA              123 0065
  GALBA NOVAES               222 0001
  NONÔ                       251 0006
  COLLOR                     288 0132
  OTAVIO CABRAL              500 0001

-------------------------------------
Total de votos Nominais         : 0205
Brancos                         : 0005
Nulos                           : 0031
Total Apurado                   : 0241

Código Verificador: 41574

=====================================

GOVERNADOR(A)

Nome do candidato       Nro cand Votos

  LENILDA LIMA                13 0005
  JOÃO LYRA                   14 0043
  ELIAS BARROS                19 0001
  ANDRE PAIVA                 28 0003
  TEOTONIO VILELA FILHO       45 0167
```

Esse texto acima **não é o conteúdo de um *arquivo LOG* normal**. É um trecho do Espelho do Boletim de Urna da própria seção eleitoral, que está seguido de registros de *log* com perda de integridade frequente e até com **inversão da ordem cronológica dos eventos**.

Está evidente que, nesse caso, o mau funcionamento do programa na urna provocou uma fusão do *arquivo LOG* com o *arquivo BU*, normalmente independentes, revelando que **também os procedimentos de apuração dos resultados foram atingidos pela impropriedade no processamento dos dados** ou, como concluiu o prof. Clovis Fernandes, autor do segundo relatório do Caso Alagoas 2006 : *"Não é possível afirmar que não tenha havido perda de integridade do RDV"*.

Porém, mesmo diante das evidências, no lugar de providenciar uma profunda auditoria a ser realizada de forma independente dos administradores do sistema, como ocorreu no caso das eleições em 2006 no Estado de Ohio nos EUA[50], a autoridade eleitoral brasileira, que ao mesmo tempo é responsável administrativa pelo sistema questionado e juiz nos recursos contra ele, **inviabilizou uma perícia independente** com as seguintes decisões:

- **Decretou** arbitrariamente que apenas os *arquivos RDV*, e não os *arquivos LOG*, devem ser usados para contar a quantidade de votos válidos, embora essa informação esteja registrada e disponível nos dois arquivos e que não poderia haver diferença entre os totais obtidos nos dois arquivos.
- Simultaneamente, **negou acesso aos *arquivos RDV*** pelos assistentes técnicos do requerente.
- **Transferiu para o requerente a cobrança antecipada de R$ 2 milhões** para que fosse desenvolvida uma perícia nas urnas eletrônicas.
- Diante do não pagamento desse de valor, proibitivo para qualquer candidato em todo o Brasil, **o requerente foi multado e condenado por litigância de má-fé**, mesmo tendo apresentado provas materiais inquestionáveis do mau funcionamento das urnas.
- **A perícia sobre as urnas não foi permitida**.

Desse conjunto de medidas autoritárias, os dois primeiros itens foram viabilizados a partir de **ativa participação do coordenador do CMTSE**.

Diante de todos esses aspectos técnicos e jurídicos, os membros deste CMind acompanham a conclusão do prof. Clovis Fernandes, apresentada em audiência pública na Assembleia Legislativa de São Paulo no dia 01 de junho de 2009, a saber:

> *"Com base na análise dos resultados do pleito de governador de Alagoas 2006 e na atitude do TSE* ***não dá para provar que houve fraude!***
>
> ***Nem que não houve fraude!***
>
> *Motivo:* ***a urna eletrônica brasileira não é auditável!****"*
>
> *Enfatiza-se que a "inauditabilidade" da urna brasileira é decorrente tanto da ação da STI/TSE na esfera judicial e administrativa, quanto da estrutura e técnica de programação temerária utilizada na urna pela STI/TSE. Para eleições do tipo brasileiro, que conta com muitos pleitos, não é possível tornar uma máquina DRE auditável.*
>
> *Ou seja, não se pode garantir com técnicas puramente computacionais que o voto dado pelo eleitor na urna foi registrado mesmo para o candidato de sua escolha e faz parte da totalização. Por causa disso, em qualquer eleição que se fizer uso deste modelo de urna eletrônica brasileira, será impossível provar que nela houve ou não fraude."*

50 Ver comparação entre os casos Alagoas e Ohio em: *http://www.votoseguro.org/textos/alagoas1.htm#4o*

3.1.8 O Caso Maranhão – 2006

Nesse Estado, também foi feita fiscalização preventiva do processo, nos dois turnos para governador, e as denuncias a seguir são apresentadas pelo lado vencedor da eleição, desmentindo o refrão generalizante de que as denúncias contra as urnas eletrônicas são sempre fruto de "*choro de perdedor*".

1º TURNO

O primeiro fato importante aconteceu na cerimônia de oficialização dos programas de totalização para o 1º turno das eleições. Naquele ato seriam conferidas as assinaturas digitais dos programas instalados nos computadores do TRE–MA.

Foram preparados quatro computadores para essa ocasião. Três deles, que ficavam na parte de baixo de um palanque, recepcionariam os *arquivos BU* vindos das Zonas Eleitorais e repassariam os dados para o quarto computador, que serviria ao Presidente do Tribunal e totalizava os demais. Este ficava sob os holofotes da imprensa e, por isso, num patamar superior.

No dia de Cerimônia de Oficialização dos programas, em que estavam presentes muitas autoridades e com maciça cobertura do imprensa local, um partido conferiu as assinaturas digitais no quarto computador, usado pelo Desembargador Presidente do Tribunal, onde se constatou a regularidade dos dados.

Ato contínuo, o fiscal pediu, então, para conferir os dados dos outros três computadores, recebendo a resposta de que não havia necessidade, porque os programas estariam interligados. O fiscal insistiu e, como não aceitou os argumentos de servidor do TRE, pôde conferir os demais dados.

Dois dos computadores estavam em situação regular, mas em um deles as assinaturas não correspondiam às dos programas oficiais. Muitas explicações foram apresentadas, inclusive que se poderia ir à totalização sem problemas, mas nenhuma delas foi capaz de demover o fiscal, que exigiu a regularização por reinstalação dos sistemas.

Após novas conferências, foi solicitada a lacração dos computadores, somente utilizados após as 17 horas do dia da eleição.

2º TURNO

Nessa etapa, verificou-se que o TRE-MA iria realizar *"uma atualização por recarga dos programas em 3% das urnas no dia da votação"*, posto que algumas delas, no ato da carga, acusavam ocorrência de um erro designado como **G-200**.

Esse erro teria ocorrido pelo desligamento antecipado de algumas urnas, no 1º turno, por mesários que não aguardaram o momento certo para o encerramento.

Como a nova carga recebida pela urna poderia camuflar eventuais problemas anteriores requereu-se permissão ao Tribunal para se verificar o *arquivo LOG* de uma das urnas que estariam nessa situação.

Aceito o requerimento pelo Tribunal, foi escolhida uma seção em cuja Ata de Cerimônia de Carga constava uma urna com o erro G-200. Realizada a análise do *arquivo LOG*, não constava qualquer problema com o encerramento da urna em 1º Turno, e a carga para o 2º Turno estava regular, não necessitando de qualquer atualização.

Ademais, verificou-se que o programa que seria utilizado para a "*atualização do software*" não inseria nenhum registro no *arquivo LOG* da urna depois de utilizado. Questionando os técnicos do TRE-MA, viu-se que não tinham conhecimento do problema e iam apenas obedecer "*ordem superiores*", o que causou imenso receio e preocupação.

A informação foi levada ao Ministério Público, à OAB e ao próprio Tribunal, a quem os candidatos requereram a não utilização de qualquer procedimento extra nas urnas no dia da votação.

Ressalte-se que as medidas preventivas foram possíveis, mesmo contra a disposição de alguns operadores, graças à permissão do Presidente do Tribunal Regional Eleitoral do Maranhão, o que resultou em nenhum questionamento técnico posterior ao pleito.

3.1.9 O Caso Itajaí, SC – 2008

Nas eleições municipais de 2008 em Itajaí, Santa Catarina, constatou-se uma **burla intencional**, como se descreve a seguir, na cerimônia de carga e lacração das urnas, cerimônia esta que na Subseção 2.1.3 do *Relatório CMTSE* é classificada como uma das salvaguardas de segurança dos sistemas.

Conforme Art. 32 da Resolução TSE 22.712/2008:

> *"Art. 32. No período que abrange o procedimento de carga e lacração,* ***deverá ser realizado teste de votação*** *acionado pelo aplicativo de Verificação Pré-Pós em* ***pelo menos uma urna por zona eleitoral, observado o mínimo de uma urna por município."***

O município de Itajaí é coberto pelas 16ª e 97ª Zonas Eleitorais de Santa Catarina, sendo que a 16ª ZE também engloba as seções eleitorais do município vizinho de Navegantes.

Na eleição de 2008, os juízes-administradores dessas duas Zonas Eleitorais decidiram fazer a carga das urnas numa única cerimônia conjunta. Na Ata da Cerimônia de Preparação e Lacração das urnas das 16ª e 97ª Zonas Eleitorais, aberta no dia 22 de setembro de 2008, consta o seguinte:

> *"Foi realizado o teste de votação a que se refere o art. 32 da Resolução TSE nº 22.712/2008 nas urnas das seções* ***236 (97ª ZE – Itajaí)*** *e 451 (16ª ZE – Navegantes), obtendo-se o resultado constante do boletim de urna anexo, que passa a integrar a presente ata,* ***sendo tais urnas submetidas a nova carga****."*

Nota-se, de imediato, que **nenhuma urna eletrônica de Itajaí da 16ª ZE foi sorteada para teste**.

Já na 97ª ZE, a urna da seção 236, sorteada para o teste obrigatório e estando então carregada e lacrada, **na hora do teste foi substituída por outra** preparada exclusivamente para o teste e que depois foi colocada à parte.

Os dados impressos anexados à ata e os dados constantes nos *Arquivos Digitais de Auditoria* da respectiva urna, mais especificamente, as tabelas de correspondências e o *arquivo LOG*, **comprovam de forma inequívoca** a ocorrência dessa burla que trocou a urna oficial a ser testada por outra preparada apenas para o teste, **fraudando o procedimento de segurança que o CMTSE reputa como salvaguarda**.

A Zerésima e no Boletim de Urna impressos anexados à ata, produzidos pela urna testada como sendo da seção 236 da 97ª ZE , apresentaram os seguintes dados:

Eleição de 23/09/2008
Hora do teste: 14:39:25
Município : 81612 – ITAJAÍ
Zona Eleitoral: 0097
Seção Eleitoral: 0236
Código de Identificação da urna : 00**852034**
Resumo da Correspondência : **902.000**

De forma contraditória, no Comprovante de Carga da urna da seção 236 da 97ª ZE, levada para a votação, e também constante da ata, está registrado o seguinte:

Município : 81612
Zona Eleitoral: 0097
Seção Eleitoral: 0236
Código de Identificação da urna : 00**842748**
Código de identificação de Carga : 592.799.644.230.781.622.007.290
Resumo da Correspondência : **007.290** *(os últimos seis dígitos do código acima)*
Flash de Carga: 88D2D957
Data da Carga: **22/09/2008**
Hora da Carga: 18:35:30

Existe diferença no código de identificação da urna e no resumo da correspondência (ou código de identificação da carga) **comprovando de forma absoluta** que **a urna que foi carregada, lacrada e levada a votação na seção 236 não é a mesma que foi levada ao teste de votação simulada**.

Os demais *arquivos de auditoria,* como a tabela de correspondência e o *arquivo LOG*, confirmam que a urna levada a votação foi a de nº 00**842748** e não a testada, que tinha o nº 00**852034**.

Ressalte-se, ademais, que o *arquivo LOG* da urna 00**842748**, levada para a votação real, **não registra a ocorrência do nenhum teste de votação e também não registra a ocorrência de uma nova carga de urna no dia 23 de setembro de 2008.**

Em síntese, **foi intencionalmente falsificado o teste de integridade** dos programas utilizados no município de Itajaí para as eleições de 2008, prescrito no art. 32 da Res. TSE 22.712/08, consubstanciado nos seguintes procedimentos:

- Da 16ª ZE não foi sorteada nenhuma urna de Itajaí para ser testada.
- Da 97ª ZE foi sorteada a urna da seção 236 para passar pelo teste.
- Essa urna, registrada sob nº 842748, tinha sido carregada em 22/09/2008 com o flash de carga 88D2D957, e gerou um Boletim de Urna aceito na Totalização.
- O *arquivo LOG* dessa urna não registra ter sido testada ou recebida nova carga, ao contrário do dito na Ata da Cerimônia de Carga e Lacração.
- A urna que passou pelo teste oficial, registrada sob nº 852034, foi carregada no dia 23/09/2008, depois do sorteio, momentos antes de ser testada.
- Essa urna usada no falso teste foi em seguida recarregada como urna de contingência, com o flash de carga F084DF12, destruindo-se todas eventuais provas nela gravadas.

Simplificando para um melhor entendimento: sortearam uma urna para o teste obrigatório mas, nesse momento, houve a troca desta urna, que já estava preparada, por outra urna que só foi preparada para passar pelo teste e depois posta à parte.

Portanto, **o Boletim de Urna e a Zerésima da seção 236 da 97ª ZE, anexados à ata da Cerimônia de Preparação e Lacração das Urnas eram falsos**, uma vez que a urna real, previamente preparada e levada para a votação real foi **intencionalmente** excluída do teste obrigatório.

Assim, com a omissão em testar urnas da 16ª ZE e com a falsificação do teste da urna da 97ª ZE, ao final:

- NENHUMA URNA PREPARADA PARA VOTAÇÃO EM ITAJAI PASSOU PELO TESTE OBRIGATÓRIO prescrito pelo Art. 32 da Res. TSE 22.712/08.
- Nenhum dos *Flash de Carga* que carregou as urnas de Itajaí foi testado quanto à sua integridade. Foram utilizados mídias diferentes para carregar as urnas levadas à votação e para realizar o teste de integridade.
- As condições complementares presentes nessa troca de urnas testadas, como o fato da urna real estar pronta para o teste desde o dia anterior e posteriormente ter sido levada à votação, afastam a possibilidade de erro, indicando a intencionalidade de burla do teste.

A ação jurídica, denunciando essa fraude interna contra salvaguarda de segurança, **não teve seu mérito avaliado** pela autoridade eleitoral.

Na primeira instância, foi indeferida pelo juiz que também era responsável administrativo pela cerimônia onde a burla ocorreu, sob **argumento escapista** de que as **impugnações** contra os procedimentos da cerimônia **só poderiam ser apresentados dentro da própria cerimônia, desconsiderando o fato de que a irregularidade só pôde ser detectada pelos fiscais dos partidos depois de terem recebidos os *arquivos LOG*** para análise, o que só ocorre após a eleição.

Na segunda instância, também se evitou a avaliação de mérito sob a alegação de intempestividade do pedido que, segundo eles, teria prazos diferentes dos regulados pelo Art. 184 do Código do Processo Civil.

Deve-se salientar, ainda, que na época do descobrimento dessa fraude, em outubro de 2008, o assunto foi levado a conhecimento e discussão com os técnicos da STI/TSE, posteriormente escolhidos para assessores pelo CMTSE.

Dessa forma, não se justifica que na Subseção 2.1.3 do *Relatório CMTSE* a cerimônia de carga e lacração das urnas seja apresentada de forma sucinta como uma das salvaguardas de segurança do sistema eleitoral **sem se apresentarem ressalvas quanto à sua eficácia**.

Torna-se este, mais um indicativo a apontar a incapacidade do CMTSE em criticar o sistema oficial, reforçando a impressão de sua parcialidade.

3.1.10 Diferenças no código-fonte – 2008

Até 2006, o programa de votação das urnas eletrônicas, após a confirmação final do voto pelo eleitor, procedia a seguinte sequência de eventos:

1) Somava um voto ao candidato votado e gravava no *arquivo BU*.
2) Gravava o voto no *arquivo RDV*.
3) Marcava o eleitor como tendo votado no arquivo de eleitores.
4) Registrava o evento "*voto computado*" no *arquivo LOG*.

Na prática, no entanto, ocorriam alterações quando, por qualquer motivo, a urna eletrônica desligava no meio deste processo podendo resultar que parte desses arquivos já estivessem atualizados com o novo voto e outra parte ainda não.

Isso resultava em diferenças entre os totais de votos registrados em cada um desses quatro arquivos, como foi detectado e descrito no relatório[51] de análise dos dados das urnas usadas na eleição em Alagoas 2006, pelo Prof. Clovis Torres Fernandes, coautor desta Réplica.

Para atenuar esse problema, em 2008, o TSE mudou a rotina e parou de calcular o BU a cada voto confirmado. Moveu-se esse procedimento para o final da votação, calculando o *arquivo BU* somente depois de gravados todos votos no *arquivo RDV*. Esperava-se que, pelo menos entre estes dois arquivos, deixariam de existir diferenças, difíceis de explicar, na quantidade total de votos.

No dia 11 de setembro de 2008, véspera da primeira compilação oficial dos sistemas, os fiscais de dois partidos, também coautores desta réplica, analisando essas rotinas encontraram uma incoerência numa comparação (comando *if*) entre a quantidade de eleitores que votaram e a quantidade de votos no *arquivo RDV*.

Pedindo esclarecimentos aos programadores do TSE, foram informados, no último dia da apresentação dos sistemas, que tal incoerência já tinha sido excluída dos código-fonte que estavam sendo compilados.

Esse acontecido comprova que **havia diferenças entre o código-fonte apresentado para análise aos partidos e o que de fato era usado na compilação dos sistemas;** nesse caso, essa **absurda impropriedade** foi descoberta por mero acaso.

Os representantes dos partidos não têm como saber quantas outras diferenças existiam, mas têm fortes motivos para supor que eram muitas diante da recusa do TSE de apresentar a lista de alterações feitas - mais de uma centena segundo um dos programadores do TSE - em função dos relatórios secretos citados no Anexo 1.

É por demais óbvio, **mesmo para leigos**, que a existência de diferenças entre o código apresentado para análise dos auditores e fiscais externos e o usado de fato nas urnas, **quebra toda a segurança pretendida** com uma cerimônia oficial de apresentação, compilação e lacração dos sistemas.

---

51 **Fernandes, C.T**. - *Radiografia das Urnas Eleitorais.* S. J. dos Campos: ITA, dezembro de 2006 - *http://www.votoseguro.org/arquivos/AL06-laudoFerITA.zip*

Além da impropriedade técnica, **ocorreu ainda ato autoritário** do administrador eleitoral ao se **recusar incluir na ata da cerimônia, citação a esse problema**. Um pedido formal apresentado por partido político à Secretaria de Tecnologia de Informação do TSE, em 12 de setembro de 2008, foi ignorado e jamais respondido. A ata não registrou o caso.

Mas **o CMTSE**, por apenas ter colhido informações sobre a cerimônia com os próprios técnicos do TSE, deixando de ouvir os fiscais externos presentes, **não detectou essas impropriedades e autoritarismo e apresentou como salvaguarda um processo frágil e com segurança totalmente comprometida**.

Destaque-se, ainda, que além dessa impropriedade na apresentação dos sistemas, a modificação da rotina de cálculo do BU para evitar divergências entre os totais de votos e de eleitores, **não resolveu o problema em sua totalidade**.

Em seis urnas eletrônicas de modelo 2008 usadas em cidades do interior de Alagoas na eleição de 2008, onde os respectivos *Arquivos LOG* registravam **desligamento imprevisto** da urna eletrônica, um fiscal de partido verificou que em quatro delas **havia divergência entre a quantidade de eleitores ausentes segundo o *arquivo BU* e a quantidade de comprovantes de votação não assinados na Folha de Votação** das respectivas seções eleitorais.

Essas diferenças não foram encontradas em dez outras seções analisadas cujas urnas não haviam sido desligadas durante a votação, mostrando que **ainda pode ocorrer erros na gravação dos *arquivos RDV* de onde se geram os *arquivos BU***.

Essa dificuldade do administrador eleitoral para conciliar os *Arquivos Digitais de Auditoria* entre si e entre os registros em papel, pode estar na raiz da forte repulsa de seus membros contra a ideia de *auditoria independente do software* (vide Seção 3.3 desta Réplica) por meio da recontagem do *voto impresso conferível pelo eleitor*.

Os técnicos da administração eleitoral **aparentam temer que potenciais erros** na apuração eletrônica, gerados por falhas e **que hoje passam despercebidos, comecem a ser detectados** provocando inevitável desconfiança no processo eletrônico de votação.

3.1.11 O Travamento de Urnas Eletrônicas - 2008

A urnas eletrônicas modelo 1998, entregues pela fabricante Procomp ao TSE, continham um lote de 90 mil cartões de memória (flash-cards) de marca Hitachi com defeito no seu firmware[52] de versão 5.1.1, que causava erro de gravação nos dados quando solicitada gravação de múltiplos setores.

Naquela ocasião, diante da premência de apresentar modelos funcionais, a Procomp solicitou à Microbase - empresa de software produtora do sistema operacional VirtuOS das urnas - que criasse um remendo (*patch*) em seu gerenciador de memória (*driver de bloco*) para substituir a gravação de múltiplos setores pela múltipla gravação de um setor, como solução provisória até que os flash-cards defeituosos fossem substituídos. O remendo no sistema operacional foi criado.

52 **Firmware** - software fixo gravado internamente em *chips* de memória não volátil, que não se apaga ao desligar.

Porém, a Procomp posteriormente optou por tomar essa solução como definitiva e decidiu o seguinte:

1) **Não substituiu os flash-cards defeituosos**, entregando-os assim mesmo ao TSE.
2) **Não comunicou o defeito nos cartões** e nem o remendo no sistema operacional.

Todos esses eventos foram descritos em audiência pública[53] pelo Eng. Frederico Gregório, Diretor Técnico da Microbase, perante a CCJC da Câmara dos Deputados no dia 25 de novembro de 2008. O depoente era o autor (terceirizado) da adaptação do software que depois o fornecedor da urna optou por esconder do TSE.

Para a eleição de 2008, visando padronizar o software de todos os seis modelos de urnas eletrônicas, o TSE adotou o Linux[54], de código aberto, como sistema operacional.

Por desconhecer o defeito dos 90 mil flash-cards instalados nas urnas modelo 98, os programadores do TSE não cuidaram de criar similar *"patch"* para substituir a gravação de múltiplos setores por múltipla gravação de um setor.

Agravando esta situação, uma vez que o processo de desenvolvimento do software eleitoral continua imaturo como denunciado em 2002 no *Relatório COPPE* [55] (vide Subseção 4.2.1 desta Réplica), inexiste roteiro de testes exaustivos para o software e o hardware, de forma que **a incompatibilidade do software de 2008 com os cartões Hitachi de 1998, defeituosos, não foi detectada até o final da cerimônia de lacração dos sistemas no TSE em 15 de setembro de 2008**.

No Maranhão, poucos dias antes do início das eleições, foi desenvolvida uma intervenção em massa por técnicos da Diebold-Procomp a fim de trocar Cartões de Memórias com o referido defeito.

No dia da eleição de 1º turno de 2008, as milhares de urnas que ainda estavam equipadas com flash-cards Hitachi com firmware versão 5.1.1 travavam e necessitavam ser substituídas.

Isso provocou muito atraso na votação nas cidades de Belém, Goiânia, Recife e seus arredores, onde a troca dos flash-cards ou das urnas **atingiu o índice alarmante de 30%**. Devido ao volume de intervenções e à falta de material, seções eleitorais tiveram a votação interrompida até as 14:30 h e a votação foi para além das 21 h.

Sob emergência, até helicópteros foram contratados no dia da eleição para transportar novos flash-cards para essas cidades.

Foi justamente a ocorrência desse problema, no Estado do Pará, que despertou a atenção do candidato a deputado federal Gerson Peres, como declarou na abertura das **audiências públicas que convocou em novembro de 2008 na CCJC da Câmara dos Deputados**, para obter esclarecimentos sobre a confiabilidade das urnas eletrônicas e que, ao final, gerou o *Relatório CCJC 2008.*

A análise desse caso, que é exemplo da anunciada **imaturidade do processo de desenvolvimento do software** do sistema eleitoral, foi ignorada no Relatório CMTSE onde tal processo é apresentado como salvaguarda de segurança.

---

53 Ver apresentação em: *http://www.votoseguro.org/arquivos/Hitachi-UE98.pdf*

54 Ver nota do TSE em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=966324*

55 **Rocha, A.R.C. Et al.** *Relatório de Avaliação do Software TSE realizada pela Fundação COPPETEC*. Brasília: COPPE/UFRJ, 09/08/2002 - *http://www.angelfire.com/journal2/tatawilson/coppe-tse.pdf*
ver resumo em: *http://www.votoseguro.org/textos/relcoppetec1.htm*

3.2 Dificuldades de Fiscalização pela OAB - Descrição dos Casos

A Lei nº 10.740, de 1º de outubro de 2003, ao revogar a impressão do voto que havia sido determinada em lei anterior, em contrapartida optou por instituir como forma de fiscalização o acompanhamento das *"fases de especificação e de desenvolvimento de todos os programas de computador de propriedade do Tribunal Superior Eleitoral, desenvolvidos por ele ou sob sua encomenda, utilizados nas urnas eletrônicas para os processos de votação, apuração e totalização"*.

Na mesma Lei, atribuiu-se essa prerrogativa não apenas aos Partidos Políticos, mas também à Ordem dos Advogados do Brasil – OAB - e ao Ministério Público – MP -. E os programas executáveis usados na eleição, inclusive os que rodam na própria urna, poderiam receber assinaturas digitais dessas entidades.

Este fato é muito explorado nas notas à imprensa[56] do TSE, comportamento esse repetido no *Relatório CMTSE* nas Subseções 2.1.2 e 2.1.3 e no Item 1 da Seção 2.2, sempre se apresentando as participações destas entidades como avalistas da confiabilidade do processo eleitoral eletrônico brasileiro. Mas a realidade é diferente.

Nesta seção, baseando-se nas observações e experiências dos advogados membros do CMind que já acompanharam o desenvolvimento dos sistemas junto ao TSE, representando Partidos Políticos ou a própria OAB, são descritas as dificuldades encontradas por esta entidade em auditar o sistema eleitoral brasileiro, a ponto de se poder dizer que tal tarefa foi, na prática, ineficaz.

3.2.1 2004 – A Tentativa de Fiscalização Correta

Em 2004, primeira eleição em que a OAB desempenhou essa função, foram indicados para participar dessa atividade dois advogados, então integrantes da Comissão de Tecnologia da Informação do seu Conselho Federal, e dois profissionais da área técnica que trabalhavam no Departamento de Informática da instituição.

Embora o TSE tenha desde logo divulgado[57] que a OAB, assim como o Ministério Público, estavam sendo agregados a essa tarefa fiscalizatória, o que possivelmente emprestava uma maior sensação de lisura ao sistema eletrônico de votação, na realidade tratou-se de uma fiscalização bastante limitada, em razão de fatores variados.

Uma primeira dificuldade foi financeira e estrutural: a entidade não dispunha de recursos materiais e humanos para desempenhar uma tarefa que, no correr dos trabalhos, mostrou-se hercúlea e dispendiosa.

Logo de início, foi necessária a contratação de uma empresa de desenvolvimento de *software*, que pudesse, em curto espaço de tempo, produzir programas de computador para assinar digitalmente e conferir tais assinaturas, tudo segundo as estritas especificações ditadas pelo TSE.

---

56 Ver, por exemplo, notícias do TSE em:
http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=13277
http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=13441
http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=14514
http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1099482
http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1117456

57 Ver notícia do TSE em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=13266*

A prestação desse serviço custou alguns milhares de reais à entidade, que **não recebe verbas públicas** e é custeada pelas contribuições pagas pelos advogados inscritos em seus quadros.

A etapa de **validação do software desenvolvido** incluía reuniões no TSE, visitas à sala onde o exame dos programas era realizado, ou o comparecimento às sessões finais em que os programas eram digitalmente assinados e **demandava outros gastos mais**, com o passagens aéreas e estadia de seus representantes, que eram baseados fora de Brasília.

Ao fim de tudo isso, assinados digitalmente os programas, **mostrou-se impossível de ser seriamente cumprida, no plano nacional, a tarefa que se seguia: a certificação dos programas instalados** nos computadores e urnas eletrônicas.

Para tanto, seria necessário gerar disquetes com o programa de conferência das assinaturas digitais – o que representava mais um gasto, ainda que desta vez mais módico – e distribuir essas mídias entre possíveis fiscais da entidade, nas diversas unidades da Federação. Conquanto o Conselho Federal tenha solicitado a cooperação das Seccionais da OAB, não nos consta que a conferência tenha sido feita senão em Minas Gerais e São Paulo.

Em Minas Gerais, como o TRE local optou por fazer a carga das urnas centralizada em Belo Horizonte, ainda foi possível fazer-se a conferência de cerca de vinte urnas, numa **amostragem quase simbólica**, dada a dimensão daquele Estado.

Em São Paulo, diferentemente, a carga das urnas foi feita em pontos variados do Estado, o que exigiu uma mobilização às pressas da OAB-SP, no sentido de recrutar em seus quadros de bacharéis em Direito, possíveis fiscais habilitados para realizar a conferência das assinaturas digitais. Gravaram-se disquetes, que foram enviados para cada uma das Subseções espalhadas por esse Estado - em torno de duzentas - juntamente com uma solicitação ao seu Presidente local para que desempenhasse a tarefa.

Esse esforço da OAB-SP desnudou uma outra dificuldade: a capacitação dos representantes, não versados em assuntos tecnológicos, **tornava aquela certificação difícil e aparentemente inócua**. Pareceu evidente que, não entendendo os meandros daquilo que está sendo fiscalizado, **uma pessoa sem conhecimentos técnicos não seria capaz de identificar qualquer tipo de falha ou problema** (como os descritos na Subseção 3.1.4 e no Anexo 4), caso viesse a presenciar a ocorrência de algum. **Não mais do que uma dezena de representantes** compareceram para conferir as assinaturas das urnas, em nome da OAB-SP.

Não há notícia de que a fiscalização da OAB tenha sido realizada noutros estados da Federação, no ano de 2004.

Mas, além disso, outra dificuldade decorria das próprias condições em que o acompanhamento era efetuado. Na etapa de validação, **foi permitido um acesso bastante mitigado ao código-fonte dos programas**: não era possível analisá-los com independência.

O acompanhamento, no caso, restringia-se a poder ler os códigos-fontes na tela dos computadores do próprio TSE, em uma sala de acesso restrito aos fiscais indicados pelos Partidos, OAB e MP. A OAB enviou, por vários dias, seu gerente de informática à sala restrita do TSE; mas tudo que lhe era possível “fiscalizar” resumia-se a ver, nos monitores, os códigos-fonte de cerca de 4.000 arquivos.

Poder ler o código-fonte de um sistema não é, por si só, uma auditoria ou validação técnica. Para se validar um código-fonte corretamente seria necessário ter total acesso a ele, de modo que seja possível testar, simular, inserir alterações e recompilar para verificar as consequências de situações não previstas.

Esse código-fonte, que, nas condições dadas, já não pôde ser minuciosamente conferido, foi compilado – isto é, vertido para código executável final - nos computadores do TSE, sem que qualquer auditoria pudesse ser feita sobre os mesmos.

Fazendo-se resumo crítico, **não há como se ter certeza de que o código-fonte visto, que já não foi adequadamente examinado, seria o mesmo que estava sendo compilado** (vide caso descrito na Subseção 3.1.10 desta Réplica).

Os programas executáveis que foram digitalmente assinados pela OAB, MP e Partidos, foram os que resultaram dessa operação, em si repleta de pontos de interrogação.

3.2.2 2006 e 2008 – O Abandono da Fiscalização Efetiva

Já nas eleições seguintes, 2006 e 2008, dadas as dificuldades vividas em 2004, optou-se por um acompanhamento mínimo, eliminando-se despesas.

A experiência de 2004 demonstrara que o acompanhamento envolvia uma relação custo/benefício desbalanceada: pode-se dizer que os custos da entidade mais o tempo dedicado voluntariamente pelos seus representantes não compensava o pouco benefício que tal tipo de fiscalização, bastante limitada, poderia trazer para a sociedade. E, em reforço do que já foi dito, a OAB não recebe verbas públicas para fazer frente às despesas impostas por este tipo de atividade.

Durante os 180 dias disponíveis para validação do software produzido, em cada eleição, não compareceu nenhum advogado membro da Comissão de Tecnologia da Informação da OAB ou técnico em informática.

No último dia, na Cerimônia de Assinatura e Lacração, compareceu um profissional técnico e, **mesmo não tendo previamente estudado o código-fonte, após sua assinatura digital nos sistemas em nome da OAB**, como apenas para cumprir a formalidade prevista em lei.

Tanto foram simbólicas as assinaturas digitais pelo técnico da OAB em 2006 e 2008, que não foi dada sequência aos procedimentos de fiscalização. A **OAB não desenvolveu nenhum trabalho ordenado para a conferência das assinaturas digitais** nos arquivos executáveis inseridos nas urnas eletrônicas em todo o Brasil.

Em 2008, a OAB e o MP chegaram a receber do TSE "*programas próprios*" verificadores de assinaturas, mas, comprovando o puro formalismo da suas participações e o abandono da fiscalização, nenhum representante da OAB ou do Ministério Público, conseguiu detectar a existência dos "*arquivos sobrantes"*, sem assinaturas, incluídos nas 400 mil urnas eletrônicas em todo o Brasil, como citado na Subseção 3.1.4 desta Réplica.

Destarte, embora a participação da OAB seja apresentada pelo TSE como uma forma de abonar, perante a sociedade, os métodos e programas utilizados, **pode-se dizer que, em 2006 e 2008, a atuação dessa entidade foi meramente figurativa**, diante das limitações financeiras e das restritas possibilidades de auditagem que lhe são franqueadas.

3.2.3 Resumo das Dificuldades da OAB

Em resumo, apesar da participação da OAB na fiscalização do processo eleitoral brasileiro transmitir uma certa sensação de tranquilidade à sociedade, a experiência no acompanhamento deste processo fiscalizatório demonstrou que:

a) **tais tarefas exigem fiscais com elevado grau de compreensão tecnológica**, do contrário participarão como meros figurantes, incapazes de detectar qualquer problema, mais ou menos grave, que eventualmente existisse nos programas carregados na urna eletrônica, como, por exemplo, os "*arquivos sobrantes*" presentes nas urnas em 2008 (vide Subseção 3.1.4 desta Réplica);

b) **o custo dessa fiscalização é elevado** e a OAB não recebe verbas públicas para desempenhar essa tarefa para a sociedade;

c) mesmo superando os dois obstáculos acima, algo que parece difícil, a eficácia da fiscalização continuará ínfima, eis que o **sistema é examinado segundo as regras criadas pelo próprio fiscalizado**, isto é, o TSE e seu corpo técnico;

d) finalmente, caso ocorra uma infiltração criminosa nesse corpo técnico, determinada a fraudar as eleições, restou evidente que **a fiscalização, deste modo como é feita, será incapaz de detectá-la**.

Desde 2006, a participação da OAB tem sido apenas formal. Na prática, **a fiscalização foi abandonada** e é abusiva a exploração da imagem da OAB como participante desses procedimentos como, por exemplo, na Subseções 2.1.2, 2.1.3 e na Seção 2.2 do *Relatório CMTSE*, onde a fiscalização pela OAB é citada de forma a induzir que seria efetiva.

A opção do CMTSE por não ouvir e conhecer a experiência própria dos fiscais externos - dos Partidos e da OAB - levou-o a também ignorar as dificuldades aqui descritas e que, na prática, tornam ineficazes muitas das salvaguardas projetadas para a segurança das eleições.

Esse comportamento do CMTSE caracteriza mais uma OMISSÃO sua e demonstra sua **dependência** e sua **incapacidade de criticar o discurso oficial** da autoridade eleitoral.

As descrições dos casos, aqui apresentadas, revelam a ineficácia absoluta da fiscalização externa sobre o processo eleitoral, demonstrando que, atualmente, a sociedade brasileira **não detém recursos para auditar o resultado eleitoral eletrônico de uma forma que seja independente dos próprios operadores do sistema**.

3.3 Independência do Software em Sistemas Eleitorais

No meio acadêmico e no meio eleitoral internacional, o conceito de ***Independência do Software em Máquinas de Votar*** vem ganhando cada vez mais espaço e tem sido adotado como referência técnica.

> *A Independência do Software em Máquinas de Votar não significa que tais máquinas não devam possuir software e, sim, que a* ***auditoria da apuração eletrônica dos votos*** *deve ser feita de forma que* ***não dependa de confiar na integridade lógica do software*** *das próprias máquinas.*
> *Ou seja, a conferência do resultado e recontagem dos votos deve dar um resultado que represente fielmente a vontade do eleitor e que não possa ser afetado, qualquer que seja o estado do software do equipamento no momento da votação e da auditoria.*

Esse conceito já aparecia em 2004 nas recomendações "*ACM Policy Recommendations on Electronic Voting Systems*" [58], da ACM - *Association for Computing Machinery*, pioneira e maior sociedade de profissionais de informática em todo o mundo:

> *"Recomendações sobre Política para Sistemas Eletrônicos de Votação – Set/2004*
>
> *Sistemas Eleitorais [eletrônicos] deverão permitir que cada eleitor possa conferir um documento físico (isto é, em papel) para verificar que seu voto foi gravado com precisão e para servir para uma* ***auditoria independente do software*** *sobre o resultado produzido e registrado no sistema.*
>
> *Tornando permanentes essas gravações (isto é,* ***não baseadas apenas em memórias dos computadores****), propiciam-se os meios pelos quais uma* ***recontagem precisa*** *possa ser feita.*
>
> *Assegurar confiabilidade, segurança e verificabilidade de eleições públicas é* ***fundamental para estabilizar a democracia****. Conveniências e velocidade da apuração de votos não são substitutos para a precisão dos resultados e para a confiança do eleitorado no processo."* (tradução pelo CMind)

O conceito de Independência do Software em Máquinas de Votar foi formalizado em 2006 por Ronald Rivest (MIT) e John Wack (NIST) no artigo "*On the notion of software independence in voting systems*" [59], declaradamente para enfrentar o problema da "*complexidade e dificuldade de testar a integridade de software de sistemas de votação*", onde explicitamente propõem o seguinte:

> *"Propomos que sistemas de votação independentes do software sejam preferidos e que sistemas de votação dependentes do software sejam abandonados."*

Primeiramente, é necessário destacar e registrar a importância do matemático Ph.D. Ronald Linn Rivest no contexto do voto eletrônico.

Foram de sua concepção três inovadores e importantes conceitos de segurança que, de algum modo, permeiam os sistema eleitorais existentes e em construção, inclusive o sistema eleitoral brasileiro.

---

58 *ACM Policy Recommendations on Electronic Voting Systems.* EUA: Association for Computing Machinery (US-ACM), 09/2004 - *http://usacm.acm.org/usacm/Issues/EVoting.htm*

59 **Rivest R.R. , Wack, J.P.** - *On the notion of "software independence" in voting systems.* EUA : National Institute of Standards and Technology (NIST), 28/07/2006 - *http://vote.nist.gov/SI-in-voting.pdf*

São suas principais criações e contribuições:

- **Assinatura Digital RSA** (1978) – Desenvolvida para garantir a integridade de arquivos digitais e apontada no *Relatório CMTSE* como uma das principais salvaguardas do sistema brasileiro.
- **Three Ballot Voting System**[60] (2004) – Sistema criptográfico de votação, ainda em desenvolvimento acadêmico, baseado no Sistema Chaum[61], com entrega do voto criptografado ao eleitor para que este possa conferir que o seu voto foi devidamente apurado, sem, no entanto, ter como provar a terceiros em quem ele efetivamente votou.
- **Independência do Software em Máquinas de Votar** (2006) – aqui resumido e já incorporado ao Art. 5º da Lei 12.034/09, que deverá ser aplicado ao sistema eleitoral brasileiro a partir de 2014.

A técnica matemática de **assinatura digital** para garantir integridade de dados, foi proposta em 1978 como mecanismo de autenticação digital genérica.

Com sua adoção em sistemas eleitorais, inclusive no Brasil, Rivest verificou[62] que **o uso da assinatura digital não conseguia cumprir a esperada garantia de integridade lógica do software eleitoral no momento da votação** e, então, envolveu-se na criação de novas técnicas autenticatórias para essa área de aplicação, que desaguou no conceito de **Independência do Software em Sistemas Eleitorais**, aqui abordado.

Rivest participou dos três principais grupos de estudos sobre voto eletrônico nos Estados Unidos:

- Membro do *CalTech-MIT Voting Technology Project* [63];
- Coautor do *Relatório Brennan* (New York University).
- Colaborador na elaboração das *Diretrizes VVSG* (NIST e US-EAC).

Nas *Diretrizes VVSG, a* **Independência do Software foi adotada como absolutamente necessária para o credenciamento de sistemas eleitorais eletrônicos**, conforme descrito nos itens traduzidos e listados no Anexo 3 desta Réplica, de onde destacamos o seguinte trecho:

> *"Todos os sistemas de votação* ***precisam ser independentes do software para estar conformes com esta norma****.*
>
> *Um exemplo de sistema dependente do software são as* ***máquinas DRE, que não estão conformes com estas normas****.*
>
> *Equipamentos de votação DEVEM criar um registro independente do voto que o eleitor possa conferir sem auxílio de software.*
>
> *Atualmente, os sistemas de votação em uso oficial que podem satisfazer a definição de independência do software empregam os registros em papel conferível pelo eleitor"*

---

60 Ver em: *http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf*

61 **Chaum, D.** - *Secret-Ballot Receipts: True Voter-Verifiable Elections* – USA: IEEE Computer Society, 2004. *http://people.csail.mit.edu/rivest/voting/papers/Chaum-SecretBallotReceiptsTrueVoterVerifiableElections.pdf*
Adaptação ao Brasil por Pedro Rezende em: *http://www.votoseguro.org/textos/chaum-voting1.htm*

62 Ver citações na Seção 4.3, adiante, e no Anexo 5.

63 *CalTech-MIT Voting Technology Project: http://vote.caltech.edu/drupal/about*

4 ANÁLISE DOS ARGUMENTOS TÉCNICOS DO CMTSE

Inicia-se a análise de mérito, nesta Réplica, na Seção 4.1 apresentando-se comentários sobre os temas citados no *Relatório CCJC 2007,* mas que foram ignorados no *Relatório CMTSE*.

Em seguida, nas Seções 4.2 a 4.5, são analisados os argumentos técnicos da CMTSE, na mesma ordem em que foram apresentados, relativos à descrição das salvaguardas do sistema eleitoral brasileiro, à identificação do eleitor, à impressão do voto e às suas conclusões.

4.1 Temas Omitidos pelo CMTSE

O *Relatório CCJC 2007* analisou Projetos de Lei existentes na Câmara dos Deputados e propôs novos Projetos de Lei sobre os seguintes temas:

a) Consequências da concentração de poderes no processo eleitoral brasileiro.
b) Dificuldades práticas e falta de verba oficial para as entidades encarregadas da fiscalização eleitoral.
c) *Auditoria Independente do Software* sobre a *Apuração*, por recontagem de 2% dos *votos impressos conferíveis pelo eleitor* (VICE).
d) Uso de software de código aberto à inspeção nas urnas eletrônicas.
e) Permissão do voto em trânsito.

Apenas o item (c) acima foi avaliado pelo CMTSE. Comenta-se, a seguir, a importância dos outros temas que o CMTSE ignorou.

4.1.1 Direito do Eleitor de Conferir o Destino do seu Voto

Porque gado a gente marca.
Tange, ferra, engorda e mata.
Mas com gente é diferente...

Geraldo Vandré e Theo de Barros – canção: *Disparada*

O *Relatório CCJC 2007* aborda a questão da percepção do eleitor sobre o destino do seu voto ao propor o projeto de lei para a materialização do voto, justificando da seguinte forma:

> *"A materialização deve ser entendida como a possibilidade de recontagem física dos votos, **garantindo ao eleitor a conferência visual de seu voto**, sem qualquer manipulação [64]....*
> *Trata-se, enfim, de **uma sistemática de fácil entendimento, mesmo para os cidadãos eleitores mais humildes**, e que combina as vantagens da agilidade da informática, com a possibilidade de eventual verificação dos votos consignados eletronicamente."*

64 Nota dos autores: Além de poder conferir o conteúdo do voto impresso, **o eleitor deve ter direito ao repúdio**, isto é, ter como poder decidir por duas ações: aceitar o voto ou cancelá-lo. Para total garantia do eleitor, os botões que permitem estas ações devem ser somente mecânicos, ou seja, **independentes do software** da urna eletrônica.

Dada a sua importância, esse direito do eleitor é tratado como fundamental já no parágrafo único do Artigo 1º da Constituição Federal: *"Todo o poder emana do povo, que o exerce por meio de **representantes eleitos** ou diretamente, nos termos desta constituição".*

E, para a escolha dos eleitos, agregam-se os três princípios eleitorais básicos:

1. Direito do Cidadão Votar e ser Votado.
2. Princípio da Inviolabilidade do Voto.
3. Princípio da Publicidade, no processo eleitoral.

O primeiro encontra sustentáculo no Art. 14 *caput* e § 3º da Constituição Federal, que resulta nas modalidades ativa e passiva de garantia ao pleno exercício da soberania popular, nos termos:

- Direito ativo – de votar e eleger seus representantes – Art. 14 *caput* da CF.
- Direito passivo – de ser votado e ocupar um cargo público – § 3º do Art. 14 da CF.

Como um dos substratos do Art. 14 da Carta Magna, tem-se que a **SOBERANIA POPULAR** será exercida pelo **VOTO DIRETO E SECRETO**, núcleo desse preceito e que permite eleições livres e honestas.

Ressalte-se que o direito ao **sigilo do voto é irreversível**, o que o diferencia de outros sigilos, como o telefônico ou o bancário, que podem ser revertidos por ordem judicial.

Desse núcleo se extraem a liberdade da expressão da vontade popular e os atributos essenciais do voto: **SINCERIDADE, AUTENTICIDADE e EFICÁCIA**.

O voto é, nesse quadro, um direito e ao mesmo tempo uma obrigação, além de selar o destino político de um povo, posto que numa democracia o poder de tomar decisões políticas está nas mãos do cidadão, que elege seus representantes.

Assim, o direito do cidadão deverá ser exercido livre e soberanamente, e sua vontade deve ser respeitada e obedecida**.** Mas esse respeito e obediência deverá perseguir o processo até sua etapa final - a divulgação dos resultados - **pois somente ali o voto preencherá os atributos essenciais, em especial o de sua EFICÁCIA**.

A Soberania do Eleitor

Em 2002, os Procuradores da República Celso Antônio Três[65] e Marco Aurélio Aydos[66] já abordavam a tese da soberania do eleitor médio poder fiscalizar o processo eleitoral sem deter conhecimentos especiais.

Em defesa da fiscalização pelo homem-médio, preleciona Celso Antônio Três:

> *"A soberania do povo, em nome do qual todo o poder é exercido, tem no direito ao voto universal e secreto o meio de expressão da soberania popular. Tal direito carece de amplo exercício de fiscalização para sua completa efetivação.* ***Fiscalização esta que deve ser exercida e compreendida, motu próprio, pelo eleitor comum, mediano, titular primeiro desta soberania****."*

65 **Três, C.A.** - *A Soberania do Povo na Fiscalização do Exercício de sua Soberania* in Seminário do Voto Eletrônico. Brasília: Câmara dos Deputados, 29/05/2002 – *http://www.votoseguro.org/arquivos/SVE-Tres.pdf*

66 **Aydos, M.A.D.** - *A Mulher de César.* Observatório da Imprensa, 2002 - *http://www.observatoriodaimprensa.com.br/artigos/mid100720025.htm*

Para o Ilustre Procurador, a tecnicidade do processo não deve subjugar o exercício da soberania pelo eleitor-médio:

> *"(...) Contudo, mesmo fosse cientificamente possível garantir a segurança técnica [do voto eletrônico], **isso não seria suficiente**. Impõe-se disponibilizar ao cidadão, **através de suas faculdades normais**, motu próprio, a possibilidade de sindicar a devida observância à sua vontade eleitoral.*
>
> *(...) **De que vale um poder, uma prerrogativa, desprovido dos instrumentos necessários à sua efetivação?!?!?***
>
> ***Soberania pressupõe poder supremo**. Onde está a supremacia do povo em um processo cuja apuração não é instrumentado por mecanismos que permitam-lhe certificar-se da soberania de sua vontade?!?!?.*
>
> ***Soberano que não é instrumentado a fiscalizar o exercício de sua soberania não é soberano."***

Em sua conclusão defende a tecnologia do processo, porém conjugada a um modelo simples de confirmação dos resultados:

> *"**Urge conciliar a irremovível instrumentação da soberania popular com as conveniências da tecnologia**. Proceder-se a votação e a apuração eletrônica, acompanhada da impressão física das cédulas, de forma a garantir a palpável, testemunhável, eventual aferição que venha a fazer-se necessária, uma das soluções."*

Recentemente, em março de 2009, essa mesma tese foi acatada pelo Tribunal Constitucional Federal da Alemanha ao julgar o uso de máquinas de votar *Nedap ESD1 e ESD2* - do tipo *máquinas DRE sem VICE* - na eleição para o parlamento em 2005.

Num longo acórdão[67], a corte suprema alemã criou jurisprudência, demarcando princípios e fundamentos sobre o uso de máquinas de votar e considerando contrário ao **Princípio da Publicidade e à Constituição** o uso de *máquinas DRE sem Voto Impresso Conferível pelo Eleitor*.

Desse acórdão da corte suprema alemã, se destaca o seguinte, de acordo com tradução para o português realizada pelo CMind:

> *"**Princípios***
>
> *2. Na utilização de máquinas eletrônicas de votar, **é necessário que o cidadão, que não possui experiência especial sobre o assunto, possa controlar de forma confiável** os passos essenciais da ação de votar e da aferição dos resultados.*
>
> ***Decisão***
>
> *2. A utilização de máquinas de votar Nedap ESD1 e ESD2 [máquinas DRE sem VICE] na eleição do 16º Parlamento Alemão **não estava de acordo com o PRINCÍPIO DE PUBLICIDADE no processo eleitoral** implícito no artigo 38, conjugado ao artigo 20, parágrafos 1 e 2 da Constituição.*

67 Decisão original do Tribunal Constitucional Federal da Alemanha em 03/03/2009 (em alemão): *http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html*
Princípios e Sentença (em português): *http://www.votoseguro.org/arquivos/Alemanha-ini-port.pdf*
Notícia: *Tribunal alemão considera urnas eletrônicas inconstitucionais*. Deutsche Welle, 03/03/2009 - *http://www.dw-world.de/dw/article/0,,4070568,00.html*

> ***Fundamento 111***
>
> *O **PRINCÍPIO DA PUBLICIDADE** exige que todos os passos essenciais da eleição estejam sujeitos à comprovação pública. **A contagem dos votos é de particular importância no controle das eleições**.*
>
> ***Fundamento 155***
>
> *Os votos foram registrados somente em memória eletrônica. Nem os eleitores, nem a junta eleitoral ou os representantes dos partidos poderiam verificar se os votos foram registrados corretamente pelas máquinas de votar. Com base no indicador no painel de controle, o mesário só pode detectar se a máquina de votar registrou um voto, mas não se os votos foram registrados sem alteração. **As máquinas de votar não previam a possibilidade de um registro do voto independente da memória eletrônica, que permitisse aos eleitores uma conferência dos seus votos**.*
>
> ***Fundamento 156***
>
> ***As principais etapas no processamento dos dados pelas máquinas de votar não poderiam ser entendidas pelo público**. Como a apuração é processada apenas dentro das máquinas, nem os oficiais eleitorais, nem os cidadãos interessados no resultado podiam conferir se os votos dados foram contados para o candidato correto ou se os totais atribuídos a cada candidato eram válidos. Com base num resumo impresso ou num painel eletrônico, **não era suficiente conferir o resultado da apuração dos votos na central eleitoral**. Assim, **foi excluída qualquer conferência pública da apuração que os próprios cidadãos pudessem compreender e confiar sem precisar de conhecimento técnico especializado**."*

Tendo traduzido a decisão da corte alemã para o espanhol, o cientista político teuto-portenho Manfredo Koessl, em artigo no jornal argentino Clarin[68], comentou o seguinte:

> *"La Corte Constitucional alemana **afirma algo que muchos políticos y consultores olvidan**: "En la República la elección es cosa de todo el pueblo y asunto comunitario de todos los ciudadanos" y que la función del proceso electoral es la "delegación del poder del Estado a la representación popular". Por ello, **su legitimidad no puede ser sacrificada en función de la comodidad de funcionarios o la ansiedad de políticos por conocer los resultados**."*

Assim, o Princípio da Publicidade no processo eleitoral, citado na Decisão e no Fundamento 111 acima, vem se entrelaçar ao Direito de Votar e ser Votado e ao Princípio da Inviolabilidade do Voto para compor os **PRINCÍPIOS ELEITORAIS FUNDAMENTAIS**.

Mas como conciliar, num mesmo processo, um princípio de publicidade e transparência com um princípio de sigilo?

Essa conciliação é propiciada pelo ***Registro do Voto***, que é o ente que trafega entre os três princípios eleitorais para lhes dar consistência e simultaneidade.

O Registro do Voto recebe, sob sigilo, a vontade do cidadão-eleitor e a leva, sem quebrar o sigilo da identidade, para ser vista e contada em cerimônia aberta perante o fiscal do cidadão-candidato.

---

68 **Koessl, M.** - *Voto electrónico, descartado.* Buenos Aires: Jornal O Clarin, 30/05/2009 - *http://www.clarin.com/diario/2009/05/30/opinion/o-01929084.htm*

A Exclusão do Eleitor

O **Princípio da Publicidade** no processo eleitoral era perfeitamente atendido no sistema de votação manual. **O eleitor via o conteúdo do Registro do Voto** - a cédula eleitoral – antes de ser colocada na urna. Na apuração, **todos esses Registros do Voto eram abertos para serem vistos** e contados perante os representantes dos candidatos.

Porém, com a adoção das *máquinas DRE* no Brasil em 1996, o **Princípio da Publicidade no processo eleitoral eletrônico teve seu alcance restringido**.

Como ressaltado pelo tribunal alemão nos Fundamentos 155 e 156, **o eleitor não tem como ver ou conferir o que foi gravado no *Registro Digital do Voto***, porque essa gravação só ocorre DEPOIS que ele encerra sua participação ao digitar a tecla CONFIRMA e, assim, **nunca terá como saber** se o *RDV* teria registrado o seu voto conforme digitado.

Além disso, o resultado da apuração – **o *Boletim de Urna* – é calculado e oficialmente publicado sem que os fiscais dos candidatos possam antes ver cada *RDV*** para conferi-los e contá-los [69].

O CMTSE, posiciona-se em direção contrária ao Princípio da Publicidade e **desconsidera o direito do cidadão médio de entender e fiscalizar o processo,** defendendo soluções tecnológicas mesmo que não compreendidas pelo cidadão comum, como em suas considerações finais na Seção 4.3, "*verbis*":

> *"O fato de que o uso de criptografia e mecanismos sofisticados tecnologicamente **não serem entendidos pela maioria dos eleitores, candidatos e público em geral**, não diminui os benefícios que essas ferramentas modernas trazem para a segurança das eleições."*

Essa tese esposada pelo CMTSE reflete o posicionamento de seu coordenador e da própria Justiça Eleitoral. Vem crescendo como linha diretriz da autoridade eleitoral nas seis últimas eleições desde a adoção das urnas eletrônicas. Suas normatizações têm seguido uma tendência constante de desconsideração desses direitos constitucionais dos eleitores.

O argumento do CMTSE repete esse entendimento, mas fere de morte o princípio de publicidade e os direitos contidos no Artigo 14 da Constituição Federal, pois **distancia-se da supremacia do direito do eleitor em ver**, de forma a si compreensível, a sua vontade preservada tanto no ato de votar quanto na destinação dada a seu voto, posto que é no final do processo que o voto preencherá os **requisitos de eficácia**, atributo essencial da obediência à vontade popular.

Com essa abordagem da autoridade eleitoral brasileira, **a importância do eleitor fica restrita à obrigação de comparecer, identificar-se, votar e acreditar que seu voto foi mesmo registrado e computado**, pois daí em diante vale tão somente o que o resultado eletrônico indicar.

---

69 O RDV, só acrescentaria "auditabilidade" ao processo, se fosse independente do software e conferível pelo eleitor, conforme exigido na *Part 1: 2.7 das Diretrizes VVSG* (vide Anexo 3 deste relatório). Não é o caso do RDV das urnas brasileiras. Portanto, a análise do seu conteúdo depende da análise do código-fonte do próprio software da urna. Como não é viável economicamente nenhuma verificação de integridade do software eleitoral (vide Seções 3.3, 4.1.3 e Anexo 5) que seja totalmente independente do próprio software da urna, qualquer resultado produzido por ele mesmo não pode ser usado para demonstrar sua integridade lógica.

Eficiência significa fazer um trabalho de boa qualidade e sem desperdícios. Eficácia é fazer um trabalho correto, sem erros, que atinja totalmente um resultado esperado.

Ao divulgar os resultados com rapidez, o TSE tem sido eficiente. Mas, como o eleitor não tem como conferir o apurado, entende-se que esse trabalho não alcançou o resultado esperado, **não foi eficaz no atendimento ao Princípio da Publicidade,** e é essa **uma grande lacuna conceitual** do sistema eletrônico de votação brasileiro.

Regulamentação do Sigilo do Voto

Essa postura de descaso ao princípio de publicidade quando relacionado à soberania do eleitor, fica claramente revelada, por exemplo, na regulamentação das garantias do sigilo do voto, outro direito constitucionalmente garantido.

Para o sistema de votação manual, essas garantias estão listadas no Art. 103 do Código Eleitoral, nos seguintes termos:

> *"Art. 103. **O sigilo do voto é assegurado** mediante as seguintes providências:*
>
> *I **uso de cédulas oficiais** em todas as eleições, de acordo com modelo aprovado pelo Tribunal Superior;*
>
> *II isolamento do eleitor em **cabine indevassável** para o só efeito de assinalar na cédula o candidato de sua escolha e, em seguida, fechá la;*
>
> *III verificação da autenticidade da cédula oficial à vista das rubricas;*
>
> *IV emprego de **urna** que assegure a inviolabilidade do sufrágio e seja **suficientemente ampla para que não se acumulem as cédulas na ordem** que forem introduzidas. "*

São regras simples e, para o homem-médio – cidadão comum de cultura técnica mediana -, é fácil e intuitivo compreender que, com o uso de cédulas oficiais - que não contêm identificação do eleitor -, com votação em cabine isolada e com embaralhamento dos votos nas urnas, **se garante o sigilo do voto sem ferir a publicidade do registro do voto**.

Porém, com a adoção, pelo TSE em 1996, do modelo *Máquinas DRE sem VICE* como urnas eletrônicas, apenas o inciso II acima pôde ser atendido. Os demais acabam não sendo satisfeitos.

Saliente-se que essas regras do nosso Código Eleitoral seriam **perfeitamente atendidas** por outro o modelo de máquinas de votar como, por exemplo, as máquinas digitalizadoras (*scaners*) do voto em papel [70], como as que foram usadas em 2008 nas eleições na Rússia e em mais de 30 Estados norte-americanos.

Para contornar essa impropriedade legal do modelo de urna eletrônica que adotou, a cada eleição desde 1996, a autoridade eleitoral edita instruções onde, no lugar de descrever procedimentos simples e compreensíveis para o eleitor, simplesmente **declara de ofício que a integridade e o sigilo do voto estariam irrefutavelmente garantidos desde que usada sua urna eletrônica e o sistema da própria autoridade eleitoral**, como no Art. 41 da Resolução TSE 23.218 de 2010, "*verbis"*:

---

70 Ao contrário das *Máquinas DRE sem VICE*, o modelo de *Máquinas Digitalizadoras para Votação* é compatível com a norma técnica norte-americana *Diretrizes VVSG*.

> *"Art. 41. **A integridade e o sigilo do voto são assegurados** mediante o disposto nos incisos I a IV do art 103 do Código Eleitoral, **devendo ser adotadas, também**, as seguintes providências:*
>
> *I – **uso de urna eletrônica**;*
>
> *II – **uso de sistemas de informática exclusivos da Justiça Eleitoral**."*

Basicamente, essa norma infra-legal do TSE acrescenta novos incisos ao artigo de lei para contornar o descumprimento da lei pelo modelo de urna que escolheu, o que já é questionável. Agrava esse abuso, o fato de que a redação desses novos incisos não permite ao cidadão comum entender como o sigilo do voto estaria garantido, pois apenas **estabelece por decreto** que seus próprios sistemas gerariam tal garantia.

Um partido político apresentou, agora em 2010, sugestão formal à autoridade eleitoral para que fosse incluído um Inciso III no art. 41 acima, com a seguinte redação:

> "*III - inexistência de conexão entre o sistema ou equipamento de identificação do eleitor e as urnas eletrônicas (§ 5º do Art. 5º da Lei 12.034/09)*."

Essa sugestão visava mostrar ao eleitor médio, de uma forma fácil de entender, que **o sigilo do voto digital seria garantido pelo fato de não existir nenhuma conexão lógica ou eletrônica entre o equipamento que será usado para identificar o eleitor e a máquina que registra o seu voto**, impossibilitando que a identidade do eleitor e seu voto pudessem ser correlacionados, como estabelece o § 5º do Art. 5º da Lei 12.034/09.

Mas, valendo-se do poder de normatizar sobre seu próprio ato administrativo, o TSE ignorou essa sugestão sem apresentar nenhuma justificativa e, **na eleição de 2010, o administrador eleitoral, mais uma vez, não vai separar os equipamentos de identificar o eleitor da máquina de votar, como agora pede a lei**, ampliando a brecha para a fraude do Voto-de-Cabresto-em-massa, descrita na Subseção 3.1.1 desta Réplica.

Pela óptica da autoridade eleitoral, se o sigilo do voto será mesmo mantido ou se o voto será ou não computado corretamente, **não cabe ao eleitor compreender como ou porque**. Nessa sua norma, simplesmente **estabelece por decreto** que o modelo de sistema que adotou garante o sigilo do voto. Ao eleitor e candidatos resta aceitar sem questionar.

A Posição dos Partidos na Regulamentação Eleitoral

No bojo do desinteresse do TSE em dar guarida e, em consequência, eficácia ao direito e soberania do eleitor, também acaba inserindo um constante **descaso aos direitos dos candidatos**. Esses agentes têm que estar sob a tutela de partidos, que têm sido forçados a absorver e cumprir as decisões unilaterais impostas pelo administrador eleitoral.

Como no exemplo acima, pode-se observar que a postura do administrador frente aos agentes passivos do processo é sempre de defesa ao absolutismo de suas ideias, soluções e decisões. Não se vê uma parceria ou conjugação de interesses, mas sim um antagonismo, onde ao administrador interessa terminar as eleições com eficiência.

A busca pelo requisito da eficácia é tida como uma interferência não desejada, que pode pôr em risco a confiança no processo, torná-lo lento ou macular sua veracidade.

Reitera-se, por pertinente, que autoridades eleitorais de mais de 50 Nações aqui estiveram para conhecer nosso sistema eleitoral eletrônico, mas do conhecimento adveio a rejeição por todos ante a falta de segurança imanente à ausência de instrumentos de rastreabilidade e auditabilidade material do voto, ou seja, instrumentos que permitam ao eleitor comum, ao final, conferir se o voto cumpriu o seu requisito de eficácia.

Contextualizando tais alegações, tome-se como exemplo da **condição de exclusão dos Partidos Políticos perante a administração eleitoral** a recente decisão expressa na Resolução TSE 23.090/09, sobre os testes de segurança nas urnas eletrônicas.

Os testes tiveram origem na petição PET TSE 1896/06, de maio de 2006, onde dois partidos políticos solicitaram a realização de experimentos para testar, perante uma comissão deliberativa independente, a eficácia do voto dado pelo eleitor. Em maio de 2008, um terceiro partido aderiu e, em conjunto, pleitearam indicar membros da comissão deliberativa, **sem o que entenderiam indeferido o pedido inicial.**

Através da Informação nº 002/2008-STI, de dezembro de 2008, no seu parágrafo 2 (ver no Anexo 1), o secretário do TSE Guiseppe Janino defendeu a inclusão de quatro indicados seus com direito a voto na comissão deliberativa, alegando o seguinte:

> *"... **os [quatro] representantes da justiça eleitoral constituirão minoria no quorum deliberativo**, pois **a comissão será composta por um representante de cada partido político**, que em outubro de 2008, já totalizaram 27"*

Porém, **negando sua própria informação**, em julho de 2009, editou-se a Resolução TSE 23.090/09, estabelecendo que os *testes de segurança* seriam controlados por **duas comissões**[71] **compostas exclusivamente por indicados da justiça eleitoral**.

Todos os membros do CMTSE foram nomeados para essas comissões, mas **não foi permitido aos partidos pleiteantes indicar ninguém, caracterizando intencional fuga ao contraditório.**

Essa decisão radical e autoritária, mostra como era importante para o administrador eleitoral deter controle absoluto da comissão deliberativa como também não permitir, dentro dela, **nenhuma voz independente** sequer.

Com o controle absoluto sobre os testes, os membros do CMTSE optaram por um equivocado modelo bipolar de segurança (vide final do Anexo 5). Ignorando a possibilidade de colusão interna, não permitiram testes de ataque sobre o código-fonte dos programas, que pudessem revelar a fragilidade do sistema a ataques internos.

A **exclusão dos partidos da função deliberativa** durante os testes de segurança, **por decisão unilateral da autoridade eleitoral**, levou os partidos peticionários a confirmar o condicional que haviam comunicado em 2008. Considerando indeferido o pedido inicial, afastaram-se do processo de preparação e execução de um teste limitado de segurança envolvendo a urna eletrônica oficial.

Em suas considerações finais, onde defende soluções tecnológicas mesmo que não compreendidas pelo eleitor, o **CMTSE mostra-se alinhado à postura ideológica do administrador eleitoral**, ao desconsiderar que o **atributo essencial da eficácia do voto** só se materializa quando o eleitor e os partidos podem "*CONTROLAR de forma confiável para si os passos essenciais da ação de votar e de aferir os resultados.*"

Por certo, é mais fácil administrar eleições cujo resultado não possa ser auditado por potenciais interessados ou prejudicados, mas a soberania do eleitor deveria ser respeitada, para levar a resultados eleitorais mais confiáveis quando submetida à auditoria independente dos próprios administradores.

---

71 *http://www.tse.gov.br/internet/eleicoes/arquivos/portaria_comissao_disciplinadora_assinado.pdf*
http://www.tse.gov.br/internet/eleicoes/arquivos/portaria_comissao_avaliadora_assinado.pdf

4.1.2 Concentração de Poderes no Processo Eleitoral Brasileiro

> *"Não haverá também liberdade se o poder de julgar não estiver separado do Poder Legislativo e do Executivo. Se estivesse ligado ao Poder Legislativo, o poder sobre a vida e a liberdade dos cidadãos seria arbitrário, pois o juiz seria legislador. Se estivesse ligado ao Poder Executivo, o juiz poderia ter a força de um opressor. Tudo estaria perdido se o mesmo homem ou o mesmo corpo dos principais, ou dos nobres, ou do povo, exercesse esses três poderes: o de fazer leis, o de executar as resoluções públicas e o de julgar os crimes ou as divergências dos indivíduos"*.
>
> **Montesquieu**, "Do espírito das leis", capítulo VI, Livro IX

> *"La raison du plus fort est toujours la meilleure. Nous l'allons montrer tout à l'heure"*
> *(A razão do mais forte é sempre a melhor. Vamos demonstrá-lo a seguir)*
>
> **La Fontaine** – fabula: *O Lobo e o Cordeiro* - 1668

O *Relatório CCJC 2007* aborda a distribuição dos poderes no processo eleitoral brasileiro ao avaliar o Projeto de Lei nº 5.057/2005. Mesmo tendo argumentado contra aspectos formais do projeto, conclui o seguinte:

> *"Nada obsta, entretanto, que a Comissão de Constituição e Justiça e de Cidadania (CCJC) estude, oportunamente, o modelo brasileiro de **distribuição de competências eleitorais** sob o ângulo do direito comparado."*

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 especializada, em outros o contencioso eleitoral é decidido na Justiça Comum. A administração do processo eleitoral pode ficar nas mãos do executivo municipal, do executivo estadual, do executivo federal ou ainda ser independente dos três Poderes tradicionais, como no Chile, por exemplo.

No Brasil, um único aparelho público, chamado Justiça Eleitoral, concentra faculdades características dos três poderes do Estado que, na clássica tripartição de Montesquieu até hoje adotada nos Estados de Direito, são o Legislativo, o Executivo e o Judiciário, independentes e harmônicos entre si e com suas funções reciprocamente indelegáveis (Art. 2º da Constituição Federal).

Esses Poderes são imanentes e estruturantes do Estado em contraposição aos poderes administrativos, que são incidentais e instrumentais. A cada um deles corresponde uma função que lhe é atribuída com precipuidade.

Nessa linha, somente excepcionalmente é admitido pela Constituição que cada ente desempenhe funções e pratique atos que a rigor seriam de outro Poder.

Segundo a doutrina de Montesquieu, há necessidade de equilíbrio entre os poderes, do que resultou entre ingleses e norte-americanos o sistema de "*checks and balances"* e que corresponde ao nosso método de freios e contrapesos, em que um Poder limita o outro.

O modelo brasileiro faz da Justiça Eleitoral uma fração especializada do Poder Judiciário, instituída pelo Código Eleitoral de 24 de fevereiro de 1932. A Constituição Federal de 1988, inclui no Capítulo III, relativo ao Poder Judiciário, disposições específicas quanto aos Tribunais e Juízes Eleitorais (na Seção VI, artigos 92,V e 118 a 121).

Porém, o Tribunal Superior Eleitoral é o único órgão integrante da Justiça Brasileira que detém funções administrativa e normativa que extrapolam seu âmbito jurisdicional. Por conter a palavra "*tribunal*" em seu nome, é comumente chamado de Justiça Eleitoral, mas exerce e é de fato o verdadeiro Administrador Eleitoral, assumindo toda administração executiva, operacional e boa parte da normatização do processo eleitoral.

A Justiça Eleitoral não conta com um quadro próprio de magistrados e, embora heterogênea, tem órgãos centralizados no próprio poder Judiciário, compostos seja por Ministros do Supremo Tribunal Federal e do Superior Tribunal de Justiça, seja por Desembargadores dos Tribunais de Justiça e Juízes Estaduais, além de Juízes Federais e Juristas, estes últimos escolhidos dentre advogados.

Segundo os juristas Roberto Amaral e Sérgio Sérvulo da Cunha [72], o que torna *sui generis* nossa justiça eleitoral é sua faculdade de realizar o seguinte:

a) Expedir instruções para execução da lei eleitoral.

b) Responder consultas sobre matéria eleitoral.

c) Julgar ações judiciais contra atos que ela própria tenha praticado.

Acrescentam ainda o seguinte:

> *"Assim, **a "justiça eleitoral" acumula a administração e o contencioso eleitoral**... Vê-se que o objeto do contencioso eleitoral - a solução de controvérsias pertinentes ao processo eleitoral - consiste em grande parte em atos praticados pelos órgãos ou agentes da justiça eleitoral, o **que representa uma contradição** em termos, e uma ameaça à objetividade e juridicidade do processo eleitoral em concreto. Esse é nódulo que reclama solução: **trata-se de uma ampla área de atividades do governo - num dos setores mais sensíveis para a caracterização do Estado democrático de Direito - que se subtrai ao controle jurisdicional**."*

Uma das decorrências malévolas da concentração das três funções de Estado num único órgão, é atribuir-se à 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 desse processo, é destinada e controlada por essa super-entidade.

Formas semânticas dão respaldo legislativo a esse arcabouço, impondo unilateralmente suas ideias e decisões, como se vê com a junção do Art. 61 da Constituição com o Parágrafo Único, Art. 1º do Código Eleitoral, que permite a propositura de leis pelo TSE, regulamentadas ao seu livre alvitre, que devem ser obedecidas por todos os cidadãos.

Dessa legalidade advêm também comandos para validar o cerceamento do direito dos eleitores, dos candidatos e das aglomerações de partidos e coligações, tanto mais substancialmente quanto mais informatizado se torna o processo eleitoral.

Também daí, decorre talvez a maior e mais preocupante consequência da referida concentração de poderes, qual seja a **imodificabilidade habitual das suas decisões** quando imbuída na função judicial.

---

72 **Amaral, R., e da Cunha, S.S.** - *Manual das Eleições. 3ª ed.* – São Paulo: Saraiva, 2006
O trecho citado encontra-se no subcapítulo "*Autenticidade das Eleições*".

Esse modelo leva a que os órgãos da Justiça Eleitoral estejam protegidos por membros dos demais órgãos judiciais, tanto nos TRE quanto no TSE. Em termos de recurso a outra corte e exercício normal do direito de produzir provas, o administrado se reencontrará com julgador que compôs, compõe ou comporá um daqueles Tribunais.

Trazendo à baila o processo eletrônico de votação, o administrado terá ainda como adversários os próprios idealizadores, desenvolvedores e operacionalizadores dos sistemas (pais do processo): os técnicos das Secretarias de TI dos referidos tribunais.

Cabe a esses profissionais de Tecnologia da Informação, além das funções acima, a de elaborar os pareceres técnicos em processos que requeiram perícias nas urnas ou no sistema todo, o que torna fácil entender seja a parcialidade jurisdicional, seja as dificuldades na produção de provas como os casos descritos, na Seção 3.1 desta Réplica, exemplificam.

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

Como 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 desses males.

Juiz e Réu no mesmo Processo

Em processos jurídicos normais perante a Justiça Eleitoral, como em casos relativos a publicidade eleitoral, a pesquisas e a abusos de poder econômico, identificam-se com precisão três agentes: no polo ativo o denunciante, no polo passivo o denunciado e um juiz independente, perfazendo a clássica relação triangular.

Mas na grande maioria dos processos sobre irregularidades no sistema de voto eletrônico, detectadas pela fiscalização eleitoral, o polo passivo é o agente administrativo responsável pelo problema que se questiona, ou seja, é o próprio servidor da administração eleitoral, muitas vezes um juiz!

Não é raro que um juiz eleitoral julgue causa em que ele próprio é, por extensão de comando, o réu. Citem-se, como exemplos, os casos de Marília-SP 2004 e Itajaí-SC 2008 descritos nas Subseções 3.1.5 e 3.1.9 desta Réplica, respectivamente.

Mais um exemplo clássico da distorção provocada pelo acúmulo de poderes delegados à Justiça Eleitoral, é o episódio ocorrido em Araçoiaba da Serra[73], onde um erro no preenchimento da tabela de candidatos não foi devidamente corrigido a tempo de evitar danos, porque quem julgava era também o superior responsável administrativo pelo erro.

Na eleição municipal de 2000, oficiais do Cartório Eleitoral esqueceram de incluir o nome de alguns candidatos a vereador no arquivo de dados carregados nas urnas eletrônicas. No dia da eleição, os candidatos excluídos não puderam ser votados. A solução óbvia seria anular a eleição, porque viciada. Mas, para tanto, o juiz teria que reconhecer erro administrativo cometido sob seu próprio comando e responsabilidade.

Julgando onde era o réu, o juiz indeferiu todos os pedidos de anulação que lhe foram apresentados, inclusive pelo Ministério Público. Na instância estadual todos os recursos também foram negados. Somente na instância superior, 3 anos depois, a eleição foi anulada. Os novos vereadores regularmente eleitos tiveram menos de 12 meses de mandato.

73 Há uma descrição e comentários sobre este caso em: *http://jus2.uol.com.br/doutrina/texto.asp?id=1553*

Normatização Restritiva de Direitos

Tendo poder de emitir normas legais sobre o processo eleitoral eletrônico que administra, inclusive sobre a fiscalização de seus atos, o administrador eleitoral acaba usando esse poder para restringir a fiscalização, como percebido pelos fiscais da OAB (vide Subseção 3.2.1 desta Réplica), nas limitações que impõe nas verificações das assinaturas digitais (vide Anexo 4), na não entrega dos *arquivos RDV* (vide Anexo 7), ou forçando sua sofisticação a ponto de inviabilizá-las financeiramente (vide Subseções 3.2.3 e 4.1.3 desta Réplica).

Merece especial destaque a criação das normas relacionadas à auditoria do processo eleitoral. Por elas são disponibilizados aos fiscais, como ferramentas para fiscalização do processo eletrônico, os seguintes recursos tecnológicos:

a) Arquivos LOG

b) Programas de verificação de assinaturas digitais dos partidos, MP e OAB

c) Tabelas de resumos digitais (*hashs*)

d) Registros Digitais dos Votos – *arquivos RDV*

Mas **a própria autoridade eleitoral**, em cujas plataformas tecnológicas essas ferramentas devem operar, **turva a função e quebra a possível eficácia desses instrumentos de auditoria**, como se explica a seguir:

a) Os *arquivos LOG* eram apresentados como instrumento essencial para auditoria, como assegurava o coordenador do CMTSE em entrevista[74] em 6/09/2006 ao jornal eletrônico IDGNow, respondendo a uma pergunta sobre a possibilidade de fraudes nas urnas eletrônicas, quando afirmou o seguinte:

"... ainda assim, existe a possibilidade de se verificar que a fraude realmente foi implementada buscando os registros de todas as operações realizadas nos sistemas ***por meio de logs****, que permitem que seja feita uma auditoria e detectada uma fraude."*

Porém, logo que os *arquivos LOG* revelaram problemas e falhas nas urnas eletrônicas no caso Alagoas 2006 (ver Subseção 3.1.7 desta Réplica), o coordenador do CMTSE mudou de posição e já na audiência pública na CCJC em maio de 2007, passou a desqualificar os *arquivos LOG* como instrumentos de auditoria com afirmações do seguinte tipo:

"*o fato do LOG não registrar um evento não significa que o evento não ocorreu"*

"deve-se usar apenas o RDV e não o LOG para contar os votos computados".

São afirmações falaciosas. Os arquivos de RDV, LOG e BU das urnas, por serem produzidos pelo próprio sistema, são mais confiáveis para detecção de falhas do que de fraudes, mas, com certeza, seus conteúdos deveriam ser internamente coerentes e sempre indicar os mesmos resultados.

b) Como descrito no Anexo 4 desta Réplica, a verificação das assinaturas digitais nos sistemas instalados pelos fiscais externos foi implementada de forma ineficaz, através da respectiva regulamentação feita pela autoridade eleitoral.

74 Em: *http://idgnow.uol.com.br/seguranca/2006/09/25/idgnoticia.2006-09-25.7125404963/paginador/pagina_3*

Essa regulamentação contraria recomendação de segurança apresentada na Seção 5.5 do chamado *Relatório "Unicamp"*[75] e ainda determina[76] que cópias dos programas verificadores dos fiscais fossem distribuídas *para treinar os técnicos* dos cartórios, dando ao fiscalizado a possibilidade de conhecer, antes do fiscal, o resultado das verificações, verdadeiras ou falsas, e de interferir conforme o seu propósito**.**

c) Tabelas de resumos digitais (*hash*) – que deveriam sempre ser produzidas na presença dos fiscais externos - têm sido recalculadas a portas fechadas, como ocorreu nas eleições de 2002 e de 2008 (vide Subseção 3.1.4 e Anexo 2).

d) Como descrito no Anexo 7, os *arquivos RDV*, **no seu formato original**, nunca foram disponibilizados aos fiscais externos desde que criados em 2004. Até 2006 os pedidos de acesso eram ignorados e em 2008 os arquivos eram fornecidos modificados, depois de "*pré-processados*" pela equipe do coordenador do CMTSE.

Julgamentos Contraditórios

É comum, para quem já participou de fiscalização em processo eleitoral, verificar a ocorrência de atitudes autoritárias dos administradores/juízes. Para ilustrar, apresenta-se apenas um exemplo peculiar desse autoritarismo, pelo inusitado, conforme se manifestou.

Em 2004, implantou-se o Registro Digital do Voto para atender à Lei 10.740/03. Mas como esta não estabelecia como dispor esses dados, decidiu-se criar um programa denominado "*Sistema de Impressão do Boletim de Voto Digital*" - SIBVD – para que cada Registro Digital do Voto pudesse ser impresso individualmente pela própria urna eletrônica.

Porém, o SIBVD abria possibilidade para a violação de votos em locais onde os mesários fossem cooptados para imprimir cada voto depois de confirmado pelo eleitor.

Em junho de 2006, através da PET TSE 1897/06, um partido preocupado com esse fato, requereu que o programa SIBVD fosse excluído das urnas, pelos riscos que propiciava.

Na prática o pedido foi atendido. Reconhecendo o risco do programa SIBVD, o administrador eleitoral o excluiu das urnas, **como se comprova** pela relação oficial[77] dos programas das urnas eletrônicas usadas em 2006, onde não se encontra relacionado o arquivo "*sibvd.exe*". Também, nas resoluções do TSE, que regulamentavam as práticas de fiscalização em 2006, não havia nenhuma previsão de impressão dos votos pelo SIBVD.

No entanto, com base em relatório produzido pelo coordenador do CMTSE, o administrador eleitoral negou os riscos denunciados e **indeferiu formalmente a petição,** por voto unânime dos ministros do TSE, mandando-se arquivá-la em 01/08/2006.

Em situação constrangedora, a autoridade atende de fato o pleiteante, mas nega formalmente o pedido para cultivar, na história oficial, uma imagem de infalibilidade.

---

75 **Tozzi, C.L. et al.** - *Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica). Campinas:* TSE, maio de 2002 - *http://www.tse.gov.br/internet/eleicoes/relatorio_unicamp/rel_final.pdf*

76 Ver Art. 28 da Resolução TSE n. 22.712/08.

77 Ver relação dos arquivos em cada modelo de urna eletrônica usada em 2006, em: *http://www.tse.gov.br/internet/eleicoes/resumos_digitais/hash_2006_1.htm*

4.1.3 Verba para Fiscalização

Segundo informa o portal do TSE[78], a informatização do processo eleitoral se iniciou em 1986 com o recadastramento eletrônico de aproximadamente setenta milhões de eleitores. Desde então, constata-se forte aumento nos custos do processo eleitoral.

Na reportagem "*A despesa dos Poderes autônomos*"[79], do Jornal Valor Econômico em 27/05/2009, é mostrado que no período que coincide exatamente com a informatização eleitoral entre 1985 e 2007, **o custeio do TSE passou de 0,02% para 0,12% do PIB**, com um crescimento de 705% segundo o jornalista Marcos Mendes [80].

Naturalmente, esse crescimento de custos afeta a fiscalização do processo eleitoral, agora eletrônico. Na forma como concebida, a "*fiscalização eletrônica*" tornou-se muito cara (vide Seção 3.2), de maneira que a **incapacidade financeira dos agentes fiscais** (Partidos, OAB e MP) soterra a oportunidade de verificação da eficácia do voto.

Uma simples comparação das atividades necessárias para fiscalizar a preparação e o conteúdo das urnas comuns e das urnas eletrônicas evidencia a enorme diferença dos custos de fiscalização nesses dois casos.

A fiscalização do conteúdo das urnas comuns - de lona – antes da sua lacração demanda apenas que a entidade fiscalizadora mobilize, por um dia, fiscais capazes de verificar se as urnas de lona estão de fato vazias antes de receberem os lacres. É uma tarefa que não exige nenhum conhecimento especializado do fiscais e historicamente é feita em 100% das urnas comuns lacradas.

Já a fiscalização do conteúdo e da integridade do software nas urnas eletrônicas antes da sua lacração demanda às entidades fiscalizadoras a seguinte mobilização de pessoas especializadas, baseando-se na regulamentação proposta pela autoridade eleitoral:

1. Montar e instalar em Brasília, por seis meses antes da eleição, uma equipe de pelo menos 6 analistas e programadores especializados nas diversas linguagens de programação usadas no sistema eleitoral, para avaliar o código-fonte dos programas e fiscalizar a compilação e lacração dos sistemas.
2. Desenvolver programa próprio para assinatura digital de todos os sistemas.
3. Acompanhar as Cerimônias de Geração das Mídias, nos 27 TRE ou em centenas de Polos de Carga, para verificar as assinaturas digitais dos sistemas instalados nos computadores.
4. Acompanhar a inseminação das 400 mil urnas, em mais de 3500 zonas eleitorais, para verificar as assinaturas digitais do software nelas carregados.
5. Acompanhar a Cerimônia de Votação Paralela nos 27 TRE.
6. Solicitar cópias dos *Arquivos Digitais de Auditoria* (RDV, BU, LOG, etc.) disponibilizados, cada um, em locais diferentes e dispersos como no TSE, nos 27 TRE e nas milhares Zonas Eleitorais, antes, durante e depois da eleição.
7. Montar equipe de analistas suficientemente competente e equipada para, em apenas 3 dias, recolher, processar, tabular, cruzar e analisar os dados desses milhares de arquivos de auditoria em busca de incoerências e provas.

---

78 Ver em: *http://www.tse.gov.br/internet/eleicoes/votoeletronico/informatizacao.htm*

79 Ver em: *http://colunistas.ig.com.br/luisnassif/2009/05/27/as-despesas-dos-poderes-autonomos/*
http://www.valoronline.com.br/?impresso/opiniao/96/5587183/a-despesa-dos--poderes-autonomos
http://www.braudel.org.br/pesquisas/pdf/mmendes04.pdf

80 Nota dos Autores: trata-se de crescimento em porcentagem do Produto Interno Bruto. O crescimento porcentual em valores nominais foi muito superior.

A título ilustrativo, observa-se que, para uma tarefa similar apenas ao item (1) acima, de estudo e avaliação do software eleitoral para fins internos, o TSE contratou[81], em 2008, a fundação FACTI, vinculada ao Ministério da Ciência e Tecnologia, pelo valor de **R$ 670 mil mais despesas de viagens, hospedagem e translados** dos técnicos envolvidos.

As dificuldades técnicas e custos maiores da fiscalização eletrônica são reveladas na Tabela1.

Local	Item	**Urnas Comuns**	**Urnas Eletrônicas**
TSE	Capacitação especial e treinamento dos fiscais	Nenhum	Analistas e programadores habilitados ao menos nas linguagens: C++, Delphi, Assembly, Oracle
	Tempo médio	Nenhum	Seis meses
Zona Eleitoral ZE	Capacitação especial e treinamento dos fiscais	Nenhum	Habilitados em informática, treinados para conferência de assinaturas digitais e testes de simulação
	Tempo médio	Meio dia	Três dias por ZE
	Porcentagem real de urnas conferidas com "zero votos"	100,00%	0,50 % (uma por ZE)

Tabela 1- tarefas de fiscalização: urna comum e urna eletrônica

O mesmo problema de custos proibitivos, vale para os outros agentes fiscais do voto eletrônico, como o Ministério Público e a OAB (vide Subseções 3.2.1 e 3.2.3 desta Réplica), que receberam a atribuição de fiscalização do voto eletrônico com a edição da Lei 10.740 de 1º de outubro de 2003, a qual deu nova redação ao § 1º do Art. 66 da Lei 9.504/97, mas sem definir de onde viria a verba para viabilizar essa nova tarefa cidadã .

A contratação e manutenção de tantos profissionais especializados quanto necessários para fiscalizar milhares de locais de carga e preparação das urnas espalhados pela Federação, tornou-se inviável e até impossível aos partidos, ao MP e à OAB, o que significa **obstacularização econômica do direito de se fiscalizar as eleições**.

Este fato **indubitável** é confirmado pela seguinte constatação em 2008, 13 anos após a adoção das urnas eletrônicas:

- Nem o MP, nem a OAB e e nem 24 dos 27 Partidos **indicaram representantes técnicos para acompanhar o desenvolvimento dos sistemas** no TSE.
- Nem o MP, nem a OAB e nenhum Partido sequer, nem mesmo os 3 acima, **esboçou a montagem de um esquema nacional para fiscalização técnica** da geração de mídias e das cargas e lacração das urnas eletrônicas.

Essa situação ocorre porque a autoridade eleitoral, que ainda detém o poder de regulamentar a fiscalização, não admite a possibilidade de conjugar os benefícios da tecnologia com a adoção de métodos simples, descomplicados e baratos de fiscalização.

81 Contrato TSE nº 032/2008, disponível nos arquivos do TSE em Brasília.

O *Relatório CCJC 2007* procurou enfrentar essa realidade com duas propostas em Projetos de Lei:

1. Uma pequena alteração na Lei 9.096/95 (Lei Orgânica dos Partidos Políticos) a fim de exortar os partidos a investir parte do fundo partidário que recebem na capacitação técnica de seus fiscais.
2. Uma alteração na Lei 9.504/97 (Lei das Normas Eleitorais) para criar uma auditoria automática da apuração por recontagem do voto materializado conferível pelo eleitor (VICE).

Não cremos que a proposta (1) surta efeito.

As verbas do fundo partidário estão longe de sustentar a economia partidária nos seus níveis nacional, estadual e municipal, o que leva à realidade constatada: **nenhum Partido tem recurso financeiro para a custosa capacitação para uma fiscalização tecnológica plena** do sistema eletrônico de votação.

A proposta (1) tampouco soluciona o problema da falta de verba para fiscalização do voto eletrônico pela OAB e pelo MP.

Já a proposta (2) tem efetivo potencial de viabilizar financeiramente a fiscalização pelos Partidos, MP e OAB, e coincide com as propostas de *Auditoria Independente do Software* contida no *Relatório Brennan*, nas *Diretrizes VVSG* e no Art. 5 da Lei 12.034/2009.

A *Auditoria Independente do Software* não exige treinamento especializado dos fiscais e é possível de ser realizada por todo e qualquer cidadão comum, com nível de conhecimento técnico elementar e independente de seu grau de instrução, posto que consiste em simples recontagem dos votos impressos (VICE).

Na Tabela 2 comparam-se as tarefas necessárias para auditoria do resultado eleitoral entre urnas eletrônicas com e sem VICE.

Local	Item	**Urna-E com VICE**	**Urna-E sem VICE**
	Método de Auditoria	Independente do Software, por recontagem dos VICE	Validação e certificação do software instalado nas urnas
TSE	Capacitação especial e treinamento dos fiscais	Nenhum	Analistas habilitados ao menos nas linguagens: C++, Delphi, Assembly, Oracle
	Tempo médio	Nenhum	Seis meses
Zona Eleitoral ZE	Capacitação especial e treinamento dos fiscais	Nenhum	Habilitados em informática, treinados para conferência de assinaturas digitais e testes de simulação
	Tempo médio	Meio dia para assistir a recontagem dos votos em 2% das seções	Três dias acompanhar a carga de todas as urnas e depois verificar assinaturas digitais e testar até 3% das urnas

Tabela 2 - tarefas de fiscalização: urna eletrônica com e sem VICE

Assim como os partidos conseguem enviar fiscais sem especialização tecnológica para mais de 300 mil seções eleitorais, conseguiriam, com mais facilidade, enviar fiscais a pouco mais de 3 mil Cartórios Eleitorais, para acompanhar a recontagem dos votos impressos de apenas 2% das urnas eletrônicas.

Esse método de **auditoria independente do software significa um barateamento imenso do processo de fiscalização**, o qual tem o condão de demonstrar aos agentes políticos, ativos e passivos, que o voto completou seu ciclo jungido pelos requisitos de **eficácia, sinceridade e autenticidade**, em respeito a vontade soberana dos eleitores, candidatos e partidos políticos.

No *Relatório CMTSE*, a questão da incapacidade fiscalizatória dos Partidos, do MP e da OAB **foi simplesmente ignorada** embora conste no *Relatório CCJC 2007* como objeto de um Projeto de Lei e, indubitavelmente, o tema coubesse no estudo das salvaguardas do sistema eleitoral brasileiro, uma vez que, impõe o bom senso, a **eficiência da fiscalização deveria ser a principal das salvaguardas de qualquer sistema eleitoral**.

O **princípio de segurança por transparência**, onde tudo que não seja sigiloso por princípio absoluto é aberto à fiscalização pela sociedade civil, é o modelo de confiança indicado para processos, como o eleitoral, onde os interesses em jogo potencialmente conflitantes são multipolares, entre mais de dois grupos de agentes.

Porém, há forte tendência dentro da autoridade eleitoral, por sua natureza concentradora de poderes, para a adoção do **princípio de segurança por obscurantismo** (vide Anexo 1 desta Réplica), onde se alega que o sigilo sobre o sistema protegeria o eleitor contra fraudes por terceiros, ignorando a possibilidade de fraudes de origem interna ou por colusão envolvendo agentes internos, que sempre acabam blindadas pela barreira de sigilo (vide final do Anexo 5 desta Réplica).

Assim, a exclusão, pelo CMTSE, do tema da incapacidade econômica dos agentes fiscais não ocorre isoladamente. Ela coincide com a estratégia do administrador eleitoral de tentar criar confiança popular no sistema baseado no centralismo, no autoritarismo e no princípio da segurança por obscurantismo.

Porém, como efeito colateral, resulta numa imprópria garantia ao administrador-normatizador de que não haverá agentes capacitados a investigar a verdade eleitoral, restando todos **impossibilitados de aferir a eficácia do trabalho por eles prestados**.

4.1.4 Voto em Trânsito

O voto em trânsito foi eliminado do processo eleitoral brasileiro em 1996, quando da adoção das urnas eletrônicas, sob o argumento de dificuldades tecnológicas apresentado pelo administrador eleitoral.

O argumento técnico não é muito claro, vinculando o voto em trânsito à necessidade de interligar "*online"* as urnas eletrônicas.

Em audiência pública no Senado, em 12 de agosto de 2009, para tratar da minirreforma eleitoral vinda da Câmara, o coordenador do CMTSE reiterou a desaprovação da Justiça Eleitoral ao "*voto em trânsito eletrônico*", alegando que seriam **proibitivos os recursos tecnológicos para criar defesas contra a fraude de um eleitor votar em duas circunscrições diferentes**.

No ***Relatório CCJC 2007*** **se propôs a reintrodução do voto em trânsito**, justificando-se da seguinte forma:

> *"No tocante ao voto em trânsito, entendemos que o direito constitucional do eleitor manifestar, de modo secreto, sua vontade* ***não pode sofrer restrições graves em decorrência da tecnologia empregada****. Atualmente, milhões de eleitores, a cada certame, apenas justificam o descumprimento do direito-dever de votar.*
>
> *Neste tópico, é compreensível que as limitações tecnológicas tenham obrigado a este caminho,* ***mas já há alternativas*** *que permitem ao eleitor escolher seus candidatos, observada a circunscrição eleitoral"*

O voto em trânsito também está posto no Art. 6 da Lei 12.034/2009, recém sancionada, revelando existir uma forte vontade do legislador que vinha sendo subjugada por um argumento tecnológico pouco claro do administrador eleitoral.

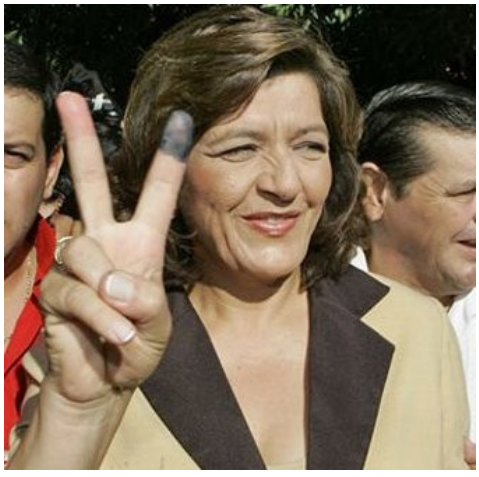
Nesse argumento, é ignorada uma técnica muito simples e eficiente, adotada em muitos países onde este tipo de fraude viceja, que é a pintura do dedo do eleitor, que já votou, com tinta indelével.

Esse recurso, de baixa tecnologia mas **suficiente para enfrentar os empecilhos alegados ao voto em trânsito** (um eleitor votar mais de uma vez) tem excelente relação custo-benefício para garantir a regra *"um eleitor, um voto".* Foi citado no ***Relatório CCJC 2008*** da seguinte forma:

> *"... como solução para o problema do eleitor que vota mais de uma vez, … a* ***adoção de tinta indelével para pintar um dedo do eleitor que já votou****, é solução largamente empregada em todo o mundo devido à sua insuperável relação custo/eficácia (qualquer eleitor pode fiscalizá-la e certificar votantes)."*

As fotos abaixo, tiradas nas últimas eleições do Chile, do Paraguai e da Venezuela, mostram como este recurso é usado sem restrições ou constrangimentos. Pelo contrário, se vê a **ex-presidente Michele Bachelet do Chile e a candidata presidencial Blanca Ovelar do Paraguai** exibindo o dedo pintado com orgulho do dever cívico cumprido.

ex-Pres. Michele Bachelet
Chile - 2009



Candidata presidencial Blanca Ovelar
Paraguai - 2008

2008
Venezuela

Já o CMTSE, em mais uma demonstração da superficialidade de sua análise, em seu relatório **se omitiu** do debate sobre esse tema proposto pelo legislador, mas que não conta com a aprovação da autoridade eleitoral representada por seu coordenador.

4.1.5 A Experiência com o Voto Impresso em 2002

No *Relatório CCJC 2007* são citados os problemas ocorridos durante a experiência, em 2002, com o voto impresso conferível pelo eleitor (*VICE*) em 5% das urnas eletrônicas. Denuncia-se ter havido "*sabotagem*" ao voto impresso durante essa experiência.

É uma denúncia de grave teor que, certamente, demandaria uma avaliação cuidadosa quanto a sua procedência.

Porém, no *Relatório CMTSE* tal avaliação resumiu-se a breves observações na Seção 3.2 e no item 5 da Subseção 3.2.1, onde é citada a ocorrência de problemas com o voto impresso em 2002 mas, como explicação, **apenas se reproduz o relato oficial**[82], apresentando os problemas ocorridos como se fossem consequências inevitáveis do voto impresso em si.

Nada é dito ou avaliado sobre uma eventual sabotagem, evidenciando que a procedência da grave denuncia contida no relatório dos deputados federais não chegou a ser averiguada.

Apresenta-se, a seguir, alguns dados documentados para essa averiguação.

Na eleição de 2002 não havia obrigação legal para a impressão do voto.

A experiência com o voto impresso em 2002 ocorreu por iniciativa exclusiva da autoridade eleitoral com o objetivo de "*testar esse mecanismo de fiscalização*", o qual, declaradamente, não contava com sua aprovação prévia.

Naquela ocasião, os procedimentos de preparação e votação nas urnas com *VICE* incluíam algumas diferenças relativas às urnas eletrônicas sem *VICE*. Três desses procedimentos eram significativos:

1. Para preparar a urna para votação na seção eleitoral, o mesário deveria **retirar os lacres** do módulo impressor externo (MIE) e da urna plástica descartável (UPD) antes de acoplá-los.
2. O eleitor teria que digitar a tecla CONFIRMA **uma vez a mais** para aprovar o voto impresso [83];
3. Ao eleitor só era permitido digitar a **tecla CANCELA uma única vez**, sob pena de ser levado a votar com voto manual (escrito).

Nas instruções e treinamento do eleitor por meio de vídeo divulgados nos canais de TV abertos, que normalmente o administrador eleitoral apresenta a cada eleição, **o TSE não incluiu esclarecimentos sobre as diferenças de votar em máquinas com VICE**.

Assim, **não existiu vídeo de treinamento nem respectivo plano de mídia em 2002** para explicar ao eleitor como votar em urnas com o voto impresso.

---

82 Ver em: *http://www.tse.gov.br/internet/eleicoes/votoeletronico/voto_impresso.htm*

83 Nessa experiência em 2002, os botões para confirmar e para cancelar o voto impresso **não eram independentes do software da urna**.

Vejam-se, por exemplo, as **instruções oficiais** divulgadas no sítio do TSE, quatro dias antes[84] e na véspera[85] da eleição de 2002 onde se diz, "*verbis*":

> *"- Como funciona a votação eletrônica?*
>
> *O teclado da urna eletrônica é igual ao teclado de um telefone, com mais três teclas coloridas logo abaixo. Primeiro o eleitor digita os quatro números do seu candidato a deputado federal. Confere na tela da urna a foto dele, o número e o partido. Se os dados estiverem corretos, o eleitor deve apertar a tecla verde, para confirmar o voto. Se não, aperta a tecla laranja e recomeça a votar. Depois, é a vez de votar, na seqência, para deputado estadual ou distrital (no DF) - cinco números -, dois senadores, o que ocorrerá em um único painel, ocupando cada voto a metade da tela da urna eletrônica - três números -, governador - dois números - e Presidente da República - dois números.* ***Quando o eleitor acabar, vai aparecer na tela a palavra Fim****.*
>
> *- E se o eleitor digitar errado o número de seu candidato na hora de votar?*
>
> ***É só cancelar toda a operação, apertando a tecla laranja, e começar o processo novamente****.*
>
> *- Quem não conseguir usar a urna eletrônica vai poder usar a cédula tradicional?*
>
> *Não.* ***A votação será manual apenas se houver algum defeito na urna eletrônica.****"*

Ou seja, o **TSE não informou ao eleitor** que nas máquinas com *VICE*:

- Teria que conferir e confirmar o voto impresso.
- Só poderia digitar a tecla CANCELA uma vez apenas.
- **Seria levado ao voto manual** caso cancelasse o voto impresso uma segunda vez.

Ademais, a Resolução TSE 21.129/02 – que dispunha sobre a utilização das urnas eletrônicas com o MIE em 2002 - estabelecia no seu Art. 5º que tanto o MIE (inciso II) quanto a UPD (inciso III) deveriam receber lacres antes de serem enviados à seção eleitoral, como destacados em negrito no texto da resolução do TSE, *verbis*:

> *"Art. 5° **Na preparação das urnas eletrônicas** das seções eleitorais que utilizarem o sistema eletrônico de votação **com módulo impressor externo – MIE**, além do que prescreve o art. 23 da Res./TSE n° 20.997, **deverão ser adotados os seguintes procedimentos**:*
>
> *II – **verificar** se foi feita a identificação dos MIE com os dados da zona eleitoral, município e seção a que se destinam ou se se trata de um MIE de contingência, e **se foram lacrados os compartimentos da bobina de papel presentes nos MIE**, tendo os lacres sido previamente assinados pelo juiz eleitoral, pelo representante do Ministério Público e pelos fiscais ou delegados dos partidos políticos ou coligações presentes;*
>
> *III – verificar se as **urnas plásticas descartáveis**, que serão utilizadas para coleta dos espelhos dos votos impressos, estão completamente vazias e, em seguida, identificar com os dados da zona eleitoral, município e seção a que se destinam e **vedá-las com os lacres**, previamente assinados pelo juiz eleitoral, pelo representante do Ministério Público e pelos fiscais ou delegados dos partidos políticos ou coligações presentes;*

84 *Saiba como Votar . http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=12214*

85 *TSE responde as principais dúvidas sobre as eleições .* Brasília: TSE, 04/10/2002 - *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=12247*

No entanto, o Art. 8º da mesma resolução do TSE, **determinava que o mesário que deveria retirar apenas o lacre da UPD** para acoplá-la ao MIE, *"verbis"*:

> *Art. 8° Estando em ordem o material de votação, **o presidente da mesa romperá o lacre da urna plástica descartável - UPD, instalando-a em seguida no módulo impressor externo - MIE**, à vista dos fiscais ou delegados dos partidos políticos ou coligações presentes."*

O mesários que seguiram estritamente essas regras e orientações oficiais, não retiravam o lacre que vedava a saída da impressora (MIE), **provocando inevitável atolamento do papel**.

Naturalmente, desinformados o eleitor e o mesário, problemas surgiram durante a votação, como relatado no sítio do TSE, de onde se destaca os seguintes comentários:

> *"- o **desconhecimento do novo mecanismo**, por parte de eleitores e de mesários, **trouxe dificuldade aos trabalhos**;*
>
> *- **o eleitor agiu como se não existisse o voto impresso**;*
>
> *- a **demora na votação foi maior que nas seções onde não havia voto impresso** (com tempo médio de votação de aproximadamente 10 minutos por eleitor);*
>
> *- ao corrigir o voto duas vezes, muitos **eleitores se negaram a votar em cédula de papel,** retirando-se da seção eleitoral;*
>
> *- o **número de panes foi expressivo** nas impressoras, **por atolamento de papel**;"*

Todos estes problemas apontados pelo administrador eleitoral **são diretamente decorrentes da falta de treinamento mínimo adequado** dos eleitores e dos mesários **por omissão ou erro do próprio administrador eleitoral**.

Para se avaliar possível sabotagem ao voto impresso, como citado no *Relatório CCJC 2007*, **resta determinar por qual motivo o administrador eleitoral, sempre tão zeloso no treinamento de eleitores e mesários, deixou de informar e treinar aqueles que se haveriam com o voto impresso em 2002** quando, espontaneamente, se propôs "*testar esse mecanismo de fiscalização*" que não contava com sua aprovação.

Como informação relevante sobre a impressão do voto para conferência pelo eleitor, lembre-se que **em outros países tem-se usado *máquinas DRE com VICE* sem maiores problemas**.

Na Venezuela, por exemplo, desde 2004 está em prática a auditoria independente do software por meio da recontagem do voto impresso e, devidamente treinados eleitores e mesários, a eleição com voto impresso acontece sem empecilhos.

No seu relatório, o CMTSE **apenas reproduz o relato oficial** acima, sem constatar que a desinformação dos eleitores e dos mesários que provocou o insucesso da experiência, foi consequência direta de atos e omissões da própria autoridade eleitoral.

Em mais um exemplo de sua parcialidade e incapacidade de criticar seu contratante, **o CMTSE omitiu-se totalmente** de avaliar a denúncia de sabotagem contida no *Relatório CCJC 2007,* **sobre a responsabilidade do administrador eleitoral por não ter dado o necessário treinamento aos mesários e eleitores durante a experiência com o voto impresso em 2002**.

4.2 Salvaguardas do Sistema Eletrônico de Votação Brasileiro

Inicia-se, nesta seção, a análise dos argumentos técnicos presentes no *Relatório CMTSE*.

No Capítulo 2 do *Relatório CMTSE* é apresentada uma descrição das salvaguardas de segurança atuais e previstas para Sistema Eletrônico de Votação.

A descrição do CMTSE consiste numa **reprodução fiel dos argumentos apresentados anteriormente por seu coordenador**, Sr. Guiseppe Dutra Janino, nas audiências públicas na Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados.

Essa descrição oficial e teórica das salvaguardas também estava apresentada no *Sumário do Voto Eletrônico*[86], disponibilizado na Internet antes da eleição de 2008, de onde se extrai a seguinte lista de salvaguardas:

1. *Processo de desenvolvimento dos softwares da urna que inclui a apresentação dos códigos-fonte aos partidos.*
2. *Assinatura digital e lacração (do software), que inclui: a geração de resumos digitais dos programas; assinatura digital pelo TSE e pelos Partidos, OAB e MP (com programa próprio); gravação e lacração dos sistemas em mídia não regravável.*
3. *Processo de distribuição do software que inclui: geração de mídias; carga das urnas; (auto-)verificação da assinatura digital; comparação do resumo digital; teste de votação; e lacração física das urnas.*
4. *Votação paralela – auditoria.*
5. *Processo de contabilização dos votos (apuração) – emissão de zerésima; arquivos de auditoria (LOG, RDV, BU e outros).*
6. *Auditoria da Totalização e processamento do BU incluindo: criptografia e decriptografia; tratamento de pendência usando a Tabela de Correspondências; publicação dos BUs na Internet.*

Essa lista teórica das salvaguardas é repetida, de modo quase que literalmente idêntico, nas Seções 2.1 e 2.2 do *Relatório CMTSE,* mostrando que **o trabalho do CMTSE teve mais natureza descritiva da versão oficial do que analítica sobre ela**.

Trata-se, enfim, de uma **visão interna e eminentemente teórica** do processo eleitoral uma vez que os seus autores não estiveram presentes e nem acompanharam em campo o desenvolvimento dos procedimentos descritos e, além do mais, optaram por não ouvir a opinião dos agentes externos credenciados, representantes dos partidos, da OAB e do MP que fizeram esse acompanhamento, assistindo na prática como se operavam tais procedimentos de segurança nas eleições passadas.

O caso real é muito diferente da explicação abstrata do CMTSE e revela que muitos pontos das salvaguardas descritas perdem, por vício de implementação ou de forma, totalmente a efetividade, como se exemplifica nos capítulos seguintes.

86 *Sumário do Voto Eletrônico* - TSE, 2008 - *http://www.tse.gov.br/internet/eleicoes/votoeletronico/sumario.htm*

4.2.1. Processo de desenvolvimento dos softwares da urna eletrônica

A Subseção 2.1.1 do *Relatório CMTSE* aborda a apresentação do software dos sistemas aos partidos, **mas restringe-se a dois parágrafos**. Apenas diz que a lei prevê a apresentação dos sistemas durante 180 dias aos representantes externos e que não seria possível modificar ou executar qualquer trecho de código naquele ambiente onde os sistemas são apresentados.

Os membros do CMTSE, à exceção do seu coordenador e mentor, não estiveram presentes na apresentação dos sistemas aos partidos nem na cerimônia de compilação e lacração dos sistemas de 2008. Não presenciaram as dificuldades e até impropriedades que ali ocorreram, o que os levou a essa **descrição tão sucinta e superficial** do processo.

O tema do **desenvolvimento seguro** de sistemas computacionais é denso e complexo dentro da disciplina de Engenharia de Software.

Como já dito na Seção 3.2, ler o código-fonte de um sistema não é, por si só, uma auditoria. Para se validar um código-fonte corretamente é necessário ser possível testar, simular e inserir alterações para verificar as consequências de situações imprevistas.

Nessa área, uma análise de profundidade sobre o desenvolvimento do software eleitoral brasileiro foi desenvolvida em 2002 por quatro professores da Fundação COPPETEC da UFRJ, especialistas em Engenharia de Software, os quais, autorizados pelo TSE, assistiram "*in loco*" os procedimentos e cerimônias oficiais.

Essa avaliação de fôlego foi apresentada num relatório[87] de **116 páginas** – sendo 13 páginas do relatório e mais 103 páginas com tabelas geradas durante o estudo - que apresentava conclusões opostas às do CMTSE relativas à eficácia da apresentação dos sistemas aos partidos. Extrai-se do *Relatório COPPE* de 2002, "*verbis*":

- *"Trata-se de **uma metodologia incompleta e em alguns aspectos ultrapassada e incoerente** .*
- *A metodologia **não tem procedimentos claramente estabelecidos para garantia da qualidade do produto** [o software das urnas].*
- *a documentação **não indicou o uso de um processo adequado de desenvolvimento e garantia da qualidade**.*
- ***Não há registros sobre os testes realizados**, nem sobre os índices de confiabilidade.*
- *o que se pode deduzir da documentação colocada para exame, **não garante que este tenha a qualidade esperada e necessária**. Foi utilizado um **processo de software bastante ad-hoc e IMATURO,** o que em geral conduz a produtos de qualidade imprevisível.*
- *Vários documentos fazem referência a datas de término da codificação.. (que) mostram que a **codificação ultrapassou a data de avaliação dos partidos."***
- *Com base no exame da documentação disponibilizada **não se pode fazer afirmativas sobre a confiabilidade do produto**.*
- *A organização interna das aplicações demonstra que **não ocorreu preocupação com o projeto do software**, e, **a fase de projeto do software parece não ter sido realizada**.*
- *Há alguns absurdos na documentação..."*

87 **Rocha, A.R.C. Et al.** *Relatório de Avaliação do Software TSE realizada pela Fundação COPPETEC*. Brasília: COPPE/UFRJ, 09/08/2002 - *http://www.angelfire.com/journal2/tatawilson/coppe-tse.pdf*
ver resumo em: *http://www.votoseguro.org/textos/relcoppetec1.htm*

A qualidade e a importância desse trabalho do COPPE foram reconhecidas pelo próprio TSE ao contratar seus autores em 2004 para colaborar no projeto do novo software.

Porém **em 2008**, apesar da adoção de software de código-fonte aberto nas urnas, os procedimentos de projeto seguro de software foram abandonados voltando-se ao um **sistema imaturo de desenvolvimento envolto com improvisações, ausência de especificações prévias, planos de testes incompletos**, etc.

Apenas três agentes externos (partidos) enviaram representantes técnicos para acompanhar a apresentação dos sistemas em 2008.

Todos esses representantes foram convidados a contribuir com o CMind e são coautores da presente réplica. Testemunham que quase todos os problemas apontados pelo COPPE em 2002 **continuavam presentes em 2008**, tais como:

- **Não existia documentação prévia detalhando o projeto do software**. Essa documentação foi sendo escrita durante o próprio desenvolvimento e só terminou muito dias depois de lacrados os sistemas. Por exemplo, a especificação dos *arquivos LOG* das urnas, solicitada para consulta em maio de 2008, só foi escrita e apresentada no final de setembro, 10 dias depois de encerrado o período de análise previsto em lei.
- **Documentos relativos a testes e análise de segurança do sistema**, desenvolvidos sob o Contrato TSE 032/2008, e que resultaram em muitas alterações no projeto de software, **foram mantidos secretos** por decisão do coordenador do CMTSE (vide Anexo 1 desta Réplica), impedindo-se os fiscais externos de identificar quais modificações foram implantadas.
- Constatou-se, no último dia do prazo de 180 dias para análise dos sistemas, que **havia diferenças entre o código-fonte apresentado aos representantes externos e o que era efetivamente compilado** (vide Subseção 3.1.10 desta Réplica), esvaziando complemente a possível eficácia dessa "salvaguarda" e, pior, **acobertando uma via oculta de preparação do processo eleitoral**.
- Apesar de ser dito na Subseção 2.1.1 do *Relatório CMTSE* que "*não é possível modificar ou executar qualquer trecho de código neste ambiente de acompanhamento externo*", ao contrário, alguns **roteiros de compilação (*scripts)* foram alterados de última hora naquele ambiente para corrigir erros** que impediam a compilação plena.
- A inexistência de um plano de testes exaustivos, preconizado no *Relatório COPPE*, impediu a detecção de uma grave incompatibilidade do software das urnas com um lote de 90 mil cartões flash-cards de marca Hitachi, resultando no **travamento de milhares de urnas eletrônicas no dia da eleição** (ver detalhes deste caso na Subseção 3.1.11 desta Réplica).

Tais fatos, graves, reais e testemunhados, **desvirtuam totalmente a função da *Apresentação dos Sistemas* como salvaguarda, a tornam inócua como garantia**, mas não foram considerados pela análise do CMTSE que apenas replicou o discurso oficial**.**

Comparando-se o conteúdo e conclusões nas **116 páginas do *Relatório COPPE*** com os **dois sucintos parágrafos que o *Relatório CMTSE*** gastou para avaliar o mesmo processo, desnuda-se a inaceitável **superficialidade deste.**

4.2.2 Lacração dos sistemas de software da urna

Na Subseção 2.1.2 do *Relatório CMTSE* é dito que:

> *"Do ponto de vista técnico, os procedimentos que garantem essa lacração [como salvaguarda] são:*
> - *Geração de resumos digitais de cada arquivo lacrado*
> - *Assinatura digital de representantes do TSE*
> - *Lacre físico de mídia não regravável"*

No entanto, o CMTSE deixou de informar que, **quebrando a referida salvaguarda**, nem todos os resumos digitais dos arquivos oficiais foram calculados na **cerimônia oficial de lacração** no dia 15 de setembro de 2008, como se comprova no Anexo 2.2, onde é apresentado o *fac-simile* da tabela de resumos digitais que foram calculados apenas no dia 25 de setembro, 10 dias depois do encerramento da cerimônia oficial de lacração.

O motivo que levou ao cálculo dos novos resumos digitais no dia 25 de setembro foi que, dois dias antes, a adv. Maria Cortiz, coautora desta Réplica, detectou a presença de 16 arquivos não assinados nas urnas eletrônicas do município de Timon, MA, como consta na ata da cerimônia de carga e lacração das urnas daquela Zona Eleitoral (vide Subseção 3.1.4, onde também é relatado caso similar ocorrido em 2002).

Para contornar essa impropriedade, a Secretaria de Tecnologia da Informação do TSE decidiu calcular o valor dos resumos digitais desses arquivos "*sobrantes*" a portas fechadas, longe dos olhos dos fiscais dos partidos, do MP e da OAB, e publicar outra tabela de resumos digitais em seu portal, em **frontal desrespeito ao que exige o § 4º do Art. 66 da Lei 9.504/97** como salvaguarda de segurança. Novamente, tal fato esvazia complemente a possível eficácia de mais uma "*salvaguarda*" e, pior, a omissão do CMTSE acoberta vias ocultas no desenvolvimento do sistema eleitoral.

Adicionalmente, o CMTSE foi ambíguo ao afirmar, na Subseção 2.1.2, o seguinte:

> *"Com o objetivo de aumentar a transparência do processo eleitoral, o uso de softwares de assinatura digital de terceiros foi permitido, por Resolução do TSE.* ***Isso possibilitou aos partidos políticos, Conselho Federal da Ordem dos Advogados do Brasil e Ministério Público Eleitoral, o desenvolvimento de seus próprios programas de assinatura digital e verificação"***

De imediato, o CMTSE ignora que tal uso de "*softwares de assinatura digital de terceiros"* NÃO FOI SOLICITADO pelos agentes fiscalizadores e sim a eles imposto pela regulamentação da autoridade eleitoral (vide Subseção 3.2.3 desta Réplica).

Na realidade, durante a cerimônia de lacração dos sistemas em 2008, os partidos presentes abriram mão de usar programas de verificação de assinaturas pelos motivos expostos no Anexo 4 desta Réplica e o MP e a OAB também nada desenvolveram, apenas receberam, *pro-forma*, programa desenvolvido pelo próprio TSE.

O CMTSE também esconde, com a redação ambígua do seu texto, que devido as dificuldades e custos que o procedimento impõe **nenhum dos agentes por ele citado (partidos, OAB e MP) desenvolveram, de fato, plano para fazer a tal verificação com programas próprios**, ou qualquer outra forma de verificação de assinaturas digitais, em nível nacional e de forma sistemática.

Além do alto custo dos procedimentos comentado na Subseção 4.1.3 desta Réplica e da insegurança nos procedimentos de verificação das assinaturas relatado no Anexo 4, a recusa dos partidos em desenvolver programas próprios se deu porque o programa é distribuído, com antecedência, aos TRE e cartórios eleitorais de todo o Brasil para fins de "*treinamento de seus técnicos*", conforme previa o artigo 28 da Resolução TSE nº 22.714/2008, *verbis*:

> *Art. 28. Os programas de verificação de assinatura digital dos partidos políticos, da Ordem dos Advogados do Brasil e do Ministério Público,incluindo a respectiva chave pública e assinaturas geradas, poderão ser utilizados pela Justiça Eleitoral para fins de treinamento de seus técnicos.*

Como se vê, o instrumento de auditoria permitido pelo TSE aos fiscais, **é conhecido e disponível por todos os fiscalizados antes do momento da fiscalização** e, essa prerrogativa é legalmente garantida pela regulamentação do próprio fiscalizado.

Em resumo, **ao contrário do que leva a entender o CMTSE, em 2008 nenhuma entidade citada desenvolveu programa próprio e, simplesmente, não aconteceu nenhuma verificação sistemática de assinaturas digitais por esses agentes**.

Tudo isto clareia pontos significativos para a confiabilidade do sistema eleitoral:

1. A lacração dos sistemas como salvaguarda não funcionou de forma correta, já que, **por erro do administrador eleitoral** (e também assessores do CMTSE), nem todos os resumos digitais foram calculados na presença dos fiscais.
2. Para contornar o seu erro, **o administrador eleitoral desrespeitou artigo de lei** referente justamente às salvaguardas jurídicas do processo de desenvolvimento do sistema eleitoral.
3. **Nenhuma consequência recaiu sobre a instituição responsável** pelo desrespeito à lei porque essa instituição também é a responsável pelo julgamento de processos eleitorais em que ela ou seus membros são réus;
4. A detecção de 16 arquivos sem resumos digitais nas urnas já inseminadas e prontas, **não implicou no refazimento da carga das urnas e nem impediu que fossem usadas na eleição**;
5. As ferramentas de verificação de integridade dos sistemas, além de ineficazes (vide Anexo 4), ficaram disponíveis para uso pelo fiscalizado antes do momento da fiscalização.
6. **Os agentes autorizados** a desenvolver verificações das assinaturas digitais, **nada fizeram por causa do custo proibitivo e da insegurança técnica dos procedimentos permitidos**.

Todavia, **nada disso foi revelado no *Relatório CMTSE***, mais uma vez evidenciando omissão, superficialidade e incapacidade de se opor ao discurso do seu coordenador.

4.2.3 Processo de distribuição e carga do software nas urnas eletrônicas

Na Subseção 2.1.3 do *Relatório CMTSE* novamente é apresentado apenas um resumo sucinto e teórico do que ocorre nas Cerimônias de Carga e Lacração das Urnas.

Um conjunto complexo de procedimentos de fiscalização, muito pouco entendido pelos presentes, fiscais inclusive, é descrito como se eficazes fossem.

Não é o que ocorre na prática. Nas cerimônias de carga de urnas nos cartórios eleitorais é comum ocorrer casos de quebras de segurança e, nesses casos, os fiscais, por despreparo próprio ou por autoritarismo do administrador-juiz, não alcançam sucesso nas suas tarefas de fiscalização.

Apenas como pequena amostra de um grande elenco de problemas já presenciados pelos membros da CMind, citam-se os seguintes:

- **Nunca é permitida a verificação independente das assinaturas digitais** dos programas instalados. **Toda verificação permitida é auto-verificação** feita a partir do próprio software da urna (ver detalhes no Anexo 4 desta Réplica).
- Simulação dos testes obrigatórios por lei (ver Caso de Itajaí-2008 na Subseção 3.1.9 desta Réplica).
- Embora algumas irregularidades na carga das urnas só possam ser identificadas por análise dos *Arquivos LOG*, **que só são disponibilizados depois das eleições**, eventuais impugnações só são aceitas se feitas na hora (ver também no Caso de Itajaí-2008 na Subseção 3.1.9 desta Réplica).
- Cerimônias de carga feitas na surdina, com posterior publicação retroativa do edital de convocação (ver Caso Diadema-2000 na Subseção 3.1.3 desta Réplica).
- Divergências nos resumos digitais em arquivos gravados nas urnas (vide Anexo 2, a Subseção 3.1.4 e o Caso Timon-2008 na Subseção 4.2.2 desta Réplica), sem causar nenhuma consequência na prática.
- Autoritarismo de alguns juízes-administradores que impedem o sorteio livre das urnas a serem testadas.
- Cerimônias conjuntas de carga das urnas durando até 7 dias, quebrando a atenção, a disponibilidade e a eficiência da fiscalização.

Sendo que basta o primeiro desses problemas – a impossibilidade de verificação independente das assinaturas digitais dos arquivos carregados nas urnas - detalhada no Anexo 4 desta Réplica - **para derrubar a eficácia da "*salvaguarda*" de segurança idealizadas para o processo de carga e lacração das urnas eletrônicas**.

No entanto, o CMTSE, em vez de denunciar a ineficácia dos procedimentos relativos a assinatura digital adotados, **cita esses procedimentos de segurança quebrada como salvaguarda** do sistema eletrônico de votação, sem dar nenhuma explicação do porquê renegam a posição do próprio inventor da técnica de assinatura digital quando este denuncia incontornável a "*complexidade e dificuldade de testar a integridade de software de sistemas de votação*", como pode ser visto no Anexo 5, na Seção 3.3 e na Seção 4.3 desta Réplica.

4.2.4 Histórico de apuração de alegações de fraudes

Na Seção 2.4 do *Relatório CMTSE* é dito que "*não existem fraudes comprovadas no sistema eletrônico de votação brasileiro*" e se explicam as crescentes reclamações e denúncias de fraudes como causadas pela *"falta de conhecimento do processo eletrônico de votação"* pelo público em geral ou por "*estelionatários que se aproveitam dessa característica [de falta de conhecimento] para aplicar um golpe configurado como um estelionato eleitoral*".

Dada a concentração de poderes da autoridade eleitoral, já aqui exposta, tal argumento constitui uma *petitio principii* [88] por demais elementar num trabalho que, pela titulação de autores, se arvora de cunho acadêmico. Como se conseguiria "*comprovar fraudes*", se a produção de provas está sob controle absoluto dos fiscalizados ou até acusados inicialmente de omissão ou inépcia?

No Anexo I daquele relatório (também referido como Anexo A) são apresentados esclarecimentos para 3 casos denunciados como fraudes: 1) Caxias, MA, 2008; 2) Guarulhos, SP, 2004; e 3) Rondônia, 2008.

No Anexo 6 desta Réplica, refuta-se a explicação do CMTSE dada ao Caso Caxias, na parte relativa à entrevista dada por membro deste CMind.

Mesmo assim, apenas três casos explicados estão muito longe de atender a mais de centena de denúncias[89] registradas apenas em 2008 e, por simples lógica, não servem como prova, por indução, da invulnerabilidade do sistema.

Em audiência pública no Senado, no dia 12 de agosto de 2009, o adv. Fernando Neves[90], que atuou como **Ministro do TSE entre 1997 e 2004**, apesar de sua total confiança na Justiça Eleitoral e no sistema eletrônico de votação que ajudou a regulamentar, declarou que: "***a Secretaria de Tecnologia de Informação do TSE não vinha conseguindo apresentar explicações convincentes*** *para as* ***crescentes denúncias de problemas*** *e fraudes nas urnas eletrônicas*".

Na Seção 3.1 desta Réplica foram descritos alguns casos documentados de problemas e impedimentos à livre fiscalização que nunca receberam, por parte do administrador eleitoral, explicações que pudessem eliminar as dúvidas e os sentimentos de insegurança gerados.

Esses casos são exemplos de possível sentido para ilocuções do gênero "*não existirem fraudes comprovadas no sistema eletrônico de votação brasileiro*", como lavrada no *Relatório CMTSE*.

São casos de impropriedades evidentes, todas devidamente documentadas, e em nenhum deles foi permitido auditoria independente ou perícia dos sistemas envolvidos (urnas e computadores de totalização). Sem perícia, não se gera prova nesses casos.

---

88 ***petitio principii*** (em português: **petição de princípio**) é um estratagema de argumentação circular ou auto-referente, que adota premissas tão questionáveis quanto a conclusão desejada. Por ex: *"Sócrates tentou corromper a juventude da Grécia, logo foi justo condená-lo à morte."*

89 Ver em: *http://www.fraudeurnaseletronicas.com.br/2008/12/relacao-municipios-suspeita-fraude.html*

90 **Fernando Neves**: advogado, foi ministro do TSE entre 1997 e 2004, sendo o Relator das Instruções de 2002 e de 2004, quando permitiu acesso dos partidos aos *Arquivos LOG* das urnas eletrônicas.

Além de exemplos de que o TSE "*não foi suficientemente responsivo às demandas por maior transparência*", como reconhecido pelo CMTSE, os casos aqui descritos revelam táticas que dificultam e até impedem a geração provas, como as seguintes:

- Autoritarismo para criar obstáculos à fiscalização.
- Protelação do processo, chegando até a causar perda do objeto.
- Arquivamento sem julgamento.
- Indeferimento baseado em argumentos esdrúxulos e contraditórios.
- Cobrança de custos proibitivos ao requerente da perícia.
- Ocultação ou bloqueio do acesso a provas documentais sob sua guarda.
- Distorcer fatos em relatórios produzidos internamente.
- Aceitação como prova judicial irrefutável ou perícia técnica imparcial, relatórios elaborados por seus próprios técnicos, funcionários públicos vinculados ao processo, em desrespeito ao artigo 138 do Código do Processo Civil.

Por escolher a própria autoridade eleitoral como fonte exclusiva de sua informação, **o *Relatório CMTSE* não captou nenhum desses fatores que limitam e impedem a revelação e produção de provas** e apenas fez repetir o discurso oficial de que "*não existem fraudes comprovadas no sistema eletrônico de votação brasileiro*".

Em vista dessas táticas, há, também, que se ponderar a quem deve ser debitada a responsabilidade por, após 13 anos de uso das urnas eletrônicas, ainda grassar entre os eleitores a *"falta de conhecimento do processo eletrônico de votação que abre espaço para ação de estelionatários"*, como alegado pelo CMTSE.

Seria culpa exclusiva dos agentes ativos e passivos (eleitores e partidos), desatentos e indolentes, que não procuram compreender a sofisticada engrenagem de segurança do sistema eleitoral depois de 13 anos de uso?

Ou, como bem colocaram os membros da Corte Constitucional Alemã (vide Subseção 4.1.1 desta Réplica), seria a complexidade do sistema que impede a compreensão desse mecanismo pelo cidadão comum, desrespeitando o Princípio da Publicidade no processo eleitoral?

Tal percepção, de natureza eminentemente jurídica, escapou ao CMTSE, composto exclusivamente por membros da área da Tecnologia da Informação, e que só conseguiu ver responsabilidade do próprio eleitor por sua "*falta de conhecimento do processo eletrônico de votação*".

Omitir citação à inerente complexidade do sistema escolhido - complexidade esta que parece ter se tornado um fim em si mesmo - e a óbvia responsabilidade do administrador eleitoral pelas escolhas que levam à falta de compreensão dos eleitores comuns e dos candidatos, é mais um ponto que desnuda a **parcialidade** do CMTSE.

4.3 Identificação do Eleitor

No *Relatório CCJC 2008* se propõe a separação física entre as máquinas de votar e as máquinas de identificar o eleitor, argumentando-se o seguinte:

> *"um programa malicioso, que porventura seja inserido em urnas eletrônicas durante o processo de preparação das mesmas, possa identificar sistematicamente o voto de cada eleitor ..."*

Na Seção 3.1 do *Relatório CMTSE* esse argumento é enfrentado em dois sucintos parágrafos nos quais se afirma que, dentro das urnas eletrônicas, o processo de identificação do eleitor é independente do processo de votação e que eventual comunicação entre os processos poderia ser evitada, como no seguinte texto:

> *"Ainda que se possa argumentar que esses processos possam ser modificados, de forma que haja comunicação entre eles, isso pode ser evitado por meio da auditoria de código e da garantia de que os softwares que rodam na urna são íntegros"*

Ora, auditoria de código complexo e garantia de integridade do software eleitoral **não é tarefa trivial**.

Como descrito no Anexo 5 desta Réplica, é marcante a posição da grande maioria dos profissionais de renome na área de segurança de dados, que também estudam o voto eletrônico, de que construir sistemas eleitorais comprovadamente confiáveis em muito suplanta a capacidade técnica e econômica disponíveis.

São vozes quase solitárias que se alinham com o CMTSE para, de forma simplória e superficial, afirmar que basta "*auditar o código e garantir a integridade do software eleitoral*", como se tarefa simples fosse.

Na Subseção 2.1.2 do seu relatório, o CMTSE afirma que se obtém tal garantia de integridade do software eleitoral pelo uso das técnicas de assinatura digital.

Esta proposta pode ser refutada, recorrendo-se à **avaliação do próprio inventor da técnica de assinatura digital**, Ronald Rivest, no seu artigo[91] que apresenta o conceito de Independência do Software em Sistemas Eleitorais (vide Seção 3.3 desta Réplica) justamente para enfrentar o problema da "*complexidade e dificuldade de testar a integridade de software de sistemas de votação"*, onde ele diz o seguinte:

> "*2 – Problema: A Complexidade do Software de Sistemas Eleitorais*
>
> *Sistemas eletrônicos de votação são complexos e estão ficando cada vez mais, conforme se tornam mais complexas as eleições e a interface com o eleitor.* ***Os requisitos para um sistema eleitoral*** *também são exigentes: precisão da apuração final, inviolabilidade do voto e segurança contra ataques e* ***mantêm graves conflitos entre si****...*
>
> *Encontrar todos os erros em sistemas amplos* ***beira o impossível ou é muitíssimo caro****. Nossa habilidade de desenvolver software complexo de longe excede nossa habilidade de provar sua exatidão ou de testá-lo satisfatoriamente a custos razoáveis. "* (tradução do CMind)

91 **Rivest R.R. , Wack, J.P.** - *On the notion of "software independence" in voting systems.* EUA : National Institute of Standards and Technology (NIST), 28/07/2006 - *http://vote.nist.gov/SI-in-voting.pdf*

Na Subseção 4.1.3 e no Anexo 4 desta Réplica elencam-se, respectivamente, as limitações financeiras e as dificuldades técnicas dos fiscais externos para confirmar a integridade do software de mais de 400 mil urnas eletrônicas por meio da verificação das assinaturas digitais.

Enfim, longe de ser tarefa simples, **é impossível na prática a proposta do CMTSE para garantir a inviolabilidade do voto** pela auditoria do código e verificação de sua integridade com assinatura digital, **como corrobora a experiência de todos os representantes das entidades fiscalizadoras externas** que acompanham a produção dos sistemas do TSE desde 2004, e que também são todos membros do CMind.

Ademais, em sua análise sucinta e simplória do tema, o CMTSE deixou de considerar e avaliar o **efeito psicológico negativo** da vinculação da identificação do eleitor com a máquina de votar sobre a possibilidade de **coação dos eleitores em larga escala**, independente da integridade do software instalado.

Na Subseção 3.1.1 desta Réplica foram apresentados os casos documentados de coação de eleitores em larga escala, na modalidade denominada **Voto-de-Cabresto-em-Massa,** ocorridos em Porto Alegre (1998) e no Rio de Janeiro (2008).

É uma fraude eleitoral, de natureza psicológica, que sobrevive e cresce a cada eleição, explorando a equivocada forma de identificar os eleitores na mesma máquina de votar que a autoridade eleitoral decidiu adotar, e **as urnas biométricas**, que já têm sido o objeto de larga campanha publicitária do TSE, **vão realimentar as condições psicossociais que tornam viável essa modalidade de fraude**.

Desta forma, **independente de estar integro ou não o seu software**, máquinas de identificar o eleitor acopladas a máquinas de votar facilitam e até estimulam o **Voto-de-Cabresto-em-Massa**, problema este que, para ser enfrentado, tem gerado desgaste ao administrador eleitoral e custos adicionais crescentes de publicidade em larga escala, sem que se saiba até onde, e como, a propaganda resolveria o problema.

O CMTSE praticamente se omitiu em relação a este problema, não apresentou nenhum argumento consistente a respeito, desconheceu a experiência real da fiscalização eleitoral externa no Brasil, ignorou o que é discutido e proposto no meio acadêmico internacional sobre as dificuldades de validar e certificar software eleitoral e **propôs solução impossível na prática**.

Enfim, deu tratamento leviano à proposta do legislador de separar as máquinas de votar e de identificar o eleitor.

4.4 Impressão do Voto

O principal argumento apresentado pelo CMTSE para justificar sua defesa do uso de *máquinas DRE sem VICE* foi apresentado na Seção 3.2 do seu relatório, onde está especificamente dito:

> "***relevantes estudos***[1] *advogam a tese de que todos os sistemas eletrônicos de votação em uso têm deficiências, mas que* ***cada sistema é passível de medidas de mitigação dos riscos*** *em cada caso. Desta forma, escolhida uma das tecnologias, há que se atentar para as salvaguardas como custo necessário da opção feita.* ***Isso se aplica no caso brasileiro também, cujo sistema é do tipo conhecido como DRE (Direct Recording Electronic), sem impressão do voto.***
>
> 1 ***Brennan****; Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission AUGUST 31, 2007).*" (sic)

Como detalhado na Subseção 2.3.2 desta Réplica, essa referência bibliográfica (1), acima transcrita, é ambígua e aponta para dois estudos diferentes, ambos relevantes: o *Relatório Brennan* e as *Diretrizes VVSG.*

No sumário executivo[92] do *Relatório Brennan* se encontram as seguintes colocações:

> ***"****DESCOBERTAS PRINCIPAIS*
>
> - *As vulnerabilidades mais preocupantes de cada sistema podem ser substancialmente eliminadas se* ***contra-medidas APROPRIADAS forem implementadas*** *no nível estadual e municipal.*
>
> *VULNERABILIDADES DOS SISTEMAS DE VOTAÇÃO*
>
> *Depois de uma revisão de mais de 120 ameaças a sistemas de votação, a Força-Tarefa chegou às* ***conclusões cruciais*** *a seguir:*
>
> - *Quando o objetivo é mudar o resultado de uma eleição apertada, ataques que envolvem a* ***inserção de programas de computador maliciosos ou outros softwares corrompidos é o que há de mais fácil****.*
> - ***Máquinas DRE sem VICE não contam com uma poderosa medida*** *para impedir ataques de software: as rotinas de auditoria automáticas pós-eleição que comparem os* ***registros em papel*** *com os registros eletrônicos.*
>
> *RECOMENDAÇÕES DE SEGURANÇA*
>
> 1. *Efetuar Auditorias Automáticas de rotina comparando os Votos Impressos Conferíveis pelo Eleitor com os Registros Eletrônicos após cada eleição. O Voto Impresso Conferível pelo Eleitor acompanhado de uma sólida Auditoria Automática pode ser um bom caminho para tornar os ataques mais simples, bem mais difíceis. "*

De fato, o *Relatório Brennan* diz que cada sistema deve ter suas vulnerabilidades mitigadas por contra-medidas **apropriadas**, porém, **ao contrário do citado pelo CMTSE**, literalmente declara que a principal contra-medida **apropriada** para máquinas DRE é o uso do *Votos Impressos Conferíveis pelo Eleitor* em auditorias de rotina sobre a apuração.

92 sumário executivo em português em: *http://www.votoseguro.org/textos/brennan-pt.pdf*

A sua primeira e principal recomendação de segurança para sistemas eleitorais é justamente *"efetuar Auditoria Automática de rotina comparando os Votos Impressos Conferíveis pelo Eleitor com os RDV*" o que **não é possível em máquinas DRE sem voto impresso**.

Portanto, **o conteúdo do *Relatório Brennan* NÃO CORROBORA O ARGUMENTO DO CMTSE** que o citou.

Também nas *Diretrizes VVSG*, **máquinas DRE sem voto impresso são explicitamente rejeitadas**.

Na seção de introdução do VVSG já é colocada sua posição:

> "*Intro: 2.4 Software Independence*
> *All voting systems must be software independent in order to conform to the VVSG...*
> *One example of a software dependent voting system is the **DRE, which is now non-conformant to this version of the VVSG**."*

Que traduzimos para:

> *"Intro: 2.4 Independência do Software*
> *Todo sistema [eletrônico] de votação precisa ter **independência do software** para estar conforme com estas diretrizes...*
> *Um exemplo de um sistema que é dependente do software é **o modelo DRE** [das urnas brasileiras], **que não está conforme com estas diretrizes**."*

Também está evidente que, **AO CONTRÁRIO DO CITADO PELO CMTSE**, as *Diretrizes VVSG* **explicitamente descredenciam** o uso de *máquinas DRE sem VICE*.

Em resumo, os dois relevantes estudos apontados pela referência ambígua do CMTSE afirmam o oposto ao citado. Ou seja, **dizem literalmente o contrário daquilo que os autores do CMTSE lhes imputam pelo contexto da referência.**

Os membros do CMTSE houveram por bem apresentar a citação de forma imprecisa, sem indicar os capítulos ou itens que confirmassem a tese alegada, encobrindo, assim, o fato de que **tais itens corroborantes à sua posição simplesmente inexistem nas obras citadas**.

Por óbvio que inexistem! O que há nos trabalhos citados mostra o oposto, já que são trabalhos sérios e seus autores são profissionais de grande projeção com eméritas reputações a zelar.

Indicar obra de grande renome como referência bibliográfica, mas sob forma mal especificada e **cujo conteúdo é literalmente oposto ao citado**, para emprestar crédito a ponto de vista polêmico que se pretende defender, **é vício que retira toda credibilidade do *Relatório do Comitê "Multidisciplinar" TSE* e do seus autores.**

Tão grave atitude tem o potencial **de vir até macular a imagem da Justiça Eleitoral, pois esse relatório, com tais inveracidades, foi formalmente entregue**[93] **aos Deputados da CCJC como sendo a palavra oficial do TSE**, e também poder vir macular as imagens das demais instituições as quais seus autores estão profissionalmente vinculados, a saber: **o Ministério de Ciência e Tecnologia, a UnB e a UNICAMP**.

93 Notícia do TSE: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1187457*

4.4.1 Votação manual e vulnerabilidades da impressão do voto

Na Subseção 3.2.1 do seu relatório, o CMTSE lista as vulnerabilidades da impressão do voto para fundamentar o argumento de que "*a impressão não elimina a possibilidade de fraudes no processo, mas introduz uma série de outros riscos*".

Porém é muito diferente o rigor sob o qual o CMTSE analisa o voto impresso daquele sob o qual avalia o voto eletrônico. Por exemplo, pode-se utilizar em ambos - voto virtual ou voto impresso - as técnicas de assinatura digital para garantia de autenticidade e de originalidade dos dados. Quando aplicadas ao voto eletrônico, o CMTSE denomina-as de salvaguardas, sem nenhuma restrição. Mas quando aplicadas ao voto impresso, o CMTSE assume posição fortemente crítica e afirma no item 3 da Subseção 3.2.1:

> *"3. A adição de evidências criptográficas, que têm sido proposta como um método para evitar a inserção de votos [impressos] não autorizados, não é efetiva pois o* ***eleitor nunca vai saber se o seu verdadeiro voto continha as evidências corretas, quando foi criado****. Neste caso, os votos poderão não ser apurados durante a recontagem"*

É evidente o desequilíbrio de tratamento. Essa mesma observação acima poderia ser aplicada ao voto eletrônico, já que neste **o eleitor não tem como sabe**r se as "*evidências criptográficas*" (assinatura digital) colocadas nos *Registros Digitais do Voto* (o voto eletrônico) garantem que estes contenham "*as evidências corretas*" do seu voto.

O CMTSE não explica porque rejeita para o registro impresso do voto a mesma técnica de segurança que declara como salvaguarda do registro digital do voto.

A ideia de acrescentar a assinatura digital da própria urna eletrônica ao voto impresso tem por função **garantir a autenticidade da origem**, ou seja, que o voto foi impresso em determinada urna, detentora única de uma chave privada de assinatura digital, e que possa ser conferida contra a chave pública correspondente em plataforma neutra.

A verificação dessa assinatura digital, em voto impresso de origem duvidosa, pode ser feita em qualquer plataforma computacional, sem prejuízo das outras salvaguardas protegidas pela autoridade eleitoral. E quem irá, conferir as "*evidências criptográficas com as evidências do voto impresso*", será quem estiver na posição de auditor após a eleição e não o eleitor ao votar, exatamente como ocorre com o *RDV*.

O CMTSE volta a dar trato desequilibrado ao voto impresso quando descreve, no item 7 da Subseção 3.2.1, possível fraude ao voto impresso em *máquinas DRE*.

Essa modalidade de fraude em urnas eletrônicas mesmo com o voto impresso é uma daquelas 128 descritas no *Relatório Brennan*. Consiste no seguinte procedimento:

1. em *máquinas DRE com VICE,* o software de votação e apuração poderia ser adulterado para imprimir o voto errado numa primeira tentativa de desviar o voto de um candidato para outro;
2. Se o eleitor, **desavisado**, não conferir o voto impresso e o confirmar, o software desonesto completa a fraude, criando um *RDV* igualmente falso. A **fraude está consumada**;
3. Se o eleitor, **atento**, rejeitar o voto impresso adulterado, cancelando-o, o software desonesto disfarça a tentativa de fraude, imprimindo um novo voto, agora correto, para confirmação do eleitor. Nesse caso, **o *RDV* também será gravado com o voto correto** para não deixar rastros e gerar suspeitas.

Primeiro, destaque-se o fato do CMTSE ter apresentado essa fraude como viável, pois, nesse momento, **passou a aceitar implicitamente que o software de *máquinas DRE* são passíveis de adulterações fraudulentas para desviar votos.**

E, se o software de *Máquinas DRE com VICE* podem ser adulterados para tentar desviar votos, certamente também podem o de *Máquinas DRE sem VICE*.

Assim, numa avaliação imparcial, essa possibilidade deve ser analisada em ambos os casos, ou seja, em *Máquinas DRE com e sem VICE.*

No caso do voto impresso, vimos acima, o **eleitor atento consegue se defender da fraude**. No caso de *Máquinas DRE sem VICE* a fraude fica assim:

1. o software de votação e apuração poderia ser adulterado para criar um Registro Digital do Voto errado diferente do visto e confirmado pelo eleitor;
2. O eleitor, **qualquer que seja sua atenção**, não tem como conferir se o gravado no *RDV* é mesmo o seu voto. **A fraude está consumada**;

É evidente que **o Voto Impresso Conferível pelo Eleitor criou para o eleitor a alternativa de se defender da fraude de adulteração do software**. Essa alternativa não existe em *Máquinas DRE sem VICE*.

E para defender o eleitor desavisado - aquele que, sem treinamento, não confere o voto impresso - deve-se fazer uma campanha instrutiva e motivadora, ensinando o eleitor a votar corretamente em *máquinas com VICE*.

Porém, o CMTSE sofisma para se alinhar com o pensamento do seu coordenador. Contaminando-se de parcialidade, distorce o caso e **descreve essa defesa contra a adulteração do software** das urnas eletrônicas como se fosse vulnerabilidade do voto impresso, enquanto omite que nenhuma defesa é possível ao eleitor nas mesmas urnas sem voto impresso.

Também é importante lembrar que a efetividade dessa defesa em *máquinas DRE com VICE* **não exige que TODOS os votos impressos sejam conferidos de fato**. Para que funcione, basta que, em ordem aleatória, alguns eleitores confiram o voto impresso ao votar.

Essa consideração também derruba outro sofisma argumentado no item 10 da Subseção 3.2.1 do *relatório CMTSE*, de que eleitores portadores de deficiências e analfabetos *"seriam prejudicados"* por não conseguirem conferir o voto impresso.

Sem o voto impresso, esses eleitores, e mais todos os que enxergam e leem, já estão completamente prejudicados em seu direito a conferir o destino do voto.

Doutra feita, uma eventual repetição de impressão errada do voto, para eleitores que veem e leem, serve como forte indício ou suspeita de disfunção ou desvio, tornando esse tipo de fraude arriscado, enquanto sem o *VICE* a fraude seguirá invisível para todos.

É falacioso, portanto, o raciocínio do CMTSE. Desde que cegos e analfabetos votem em ordem aleatória, misturados com outros eleitores habilitados a conferir o voto impresso, TODOS ESTARÃO PROTEGIDOS pelo Voto Impresso Conferível pelo Eleitor contra a fraude de adulteração do software em *máquinas DRE*. **Mesmo cegos e analfabetos resultam beneficiados por esta defesa com o voto impresso**.

É por isso que todos, incluindo as *Diretrizes VVSG* que normatizam o voto eletrônico nos EUA, dizem voto impresso CONFERÍVEL pelo eleitor e não CONFERIDO. Para sua eficácia, não é necessário que todos o confiram, **mas que possam conferi-lo**.

A parcialidade com que o CMTSE avalia o voto impresso chega ao extremo, beirando a húbris, no item 8 da Subseção 3.2.1, onde afirma:

> *"8. A impressão do voto requer um re-exame do significado dos termos "voto" e "voto oficial". Isto não é um exercício meramente semântico, mas uma grande questão legal e de significância constitucional. Pode um pedaço de papel ser considerado voto se ele não é nem marcado ou mesmo tocado pelo eleitor? Neste caso, mudanças legais significativas deverão ser feitas...."*

Neste momento é importante demarcar uma diferença crucial entre o voto impresso e o voto virtual:

- o voto impresso é gravado no papel **ANTES de ser visto e confirmado** pelo eleitor;
- o voto virtual é gravado no *arquivo RDV* **DEPOIS de confirmado** pelo eleitor.

Assim, **o voto impresso é conferível pelo eleitor enquanto o *RDV* não tem como ser conferido**. Lembre-se que o CMTSE reconheceu implicitamente, ao criticar o voto impresso, que o software de *máquinas DRE* pode ser viciado para adulterar o *RDV*.

O administrador eleitoral sempre considerou válido o *RDV* como expressão do voto, mas ao colocar este item 8, o CMTSE questiona se um pedaço de papel impresso **que o eleitor viu mas não tocou** pode, semântica e juridicamente, ser considerado seu voto!

É indubitável que **o *VICE***, visível e conferível, **reúne qualidades semânticas e ontológicas muito superiores às do invisível *RDV*** para representar o voto do eleitor.

Esse tipo de sofisma, colocado pelo CMTSE no item 8 acima transcrito, só faria sentido sob a tácita presunção de que quem manipula o software gerador do *RDV* são sempre incorruptíveis anjos-do-bem.

A pérola final dos argumentos equivocados e absurdos do CMTSE contra o voto impresso está no item 9 da Subseção 3.2.1 e que também foi apresentado pelo Sr. Amândio Ferreira Balcão Filho, membro do CMTSE, em audiência pública na Assembleia Legislativa de São Paulo no dia 01 de junho de 2009.

Afirma que um dos problemas de existir o voto impresso é que havendo uma forma alternativa de conferir e recontar os votos eletrônicos, **"todos"** os candidatos vão querer se valer desta possibilidade e vão querer conferir a apuração eletrônica.

É uma posição obscurantista, que coloca a vontade do candidato de conferir a apuração do voto como se fosse algo condenável e não um direito soberano e objetivo nascido da conjunção do direito constitucional de ser votado com o Princípio da Publicidade no processo eleitoral, como insculpido em lei e discutido na Subseção 4.1.1 desta Réplica.

Essa surpreendente colocação em público do Sr. Amândio Filho causou indignação na plateia na Assembleia paulista, provocando apupos e tornando necessária a intervenção do presidente da mesa para pedir ordem para prosseguimento da audiência.

É mais um exemplo de como o acúmulo de poderes da autoridade eleitoral brasileira tem-na levado a relegar direitos dos eleitores e dos partidos, e que, também neste caso, foi postura encapada pelos membros do CMTSE.

4.5 Sobre as Conclusões e Recomendações do CMTSE

Nas conclusões do CMTSE, apresentadas na Seção 4.1, de início, **há completa omissão sobre os aspectos jurídicos levantados pelos deputados da CCJC,** tais como as consequências do acúmulo de poderes no processo eleitoral brasileiro e os diretos dos eleitores comuns e candidados a um sistema eleitoral que lhes permita acompanhar o destino do voto sem recorrer a conhecimentos especiais e diferenciados.

No item 3 das suas conclusões, o CMTSE volta a repetir citação imprecisa e ambígua ao *Relatório Brennan* e às *Diretrizes VVSG*, **novamente invertendo o mérito do citado para tentar justificar seu discutível argumento**, como já descrito na Seção 4.4 desta Réplica.

No item 4 das conclusões, o CMTSE faz interessante observação, em rebuscada linguagem, dizendo:

> *"...é o caso do Processo Eleitoral Brasileiro, que peculiarmente possui um complexo processo organizacional, com modos precisos de verificação e auditoria, impondo altos custos/benefícios na exploração de possíveis vulnerabilidades identificadas."*

No entanto, **em nenhum local do mesmo *Relatório CMTSE* é apresentado algum estudo ou esboço de estudo** sobre a citada relação custo/benefício de eventuais fraudes, que justifique ou embase essa conclusão.

Uma proposta[94] de elaboração desse tipo de estudo foi apresentada em 2000 durante o Simpósio de Segurança em Informática SSI'2000, no ITA. A proposta chegou ao conhecimento da secretaria de informática do TSE por meio de seus assessores técnicos convidados para assistir a apresentação pelo organizador do evento, o prof. Clovis Torres Fernandes, membro do CMind.

A proposta nunca foi aceita pelo corpo técnico do TSE e surpreende que o coordenador do CMTSE assine essa conclusão apontando para uma direção de estudo que sempre desconsiderou.

O *Relatório Brennan*, de 2006, contém um extensivo e bem elaborado - único conhecido - **estudo de riscos e custos sobre fraudes em sistemas eleitorais** e argumenta contra *máquinas DRE sem VICE*:

> *"Depois de uma **revisão de mais de 120 ameaças a sistemas de votação**, a Força-Tarefa chegou às conclusões cruciais a seguir:*
>
> *Quando o objetivo é mudar o resultado de uma eleição apertada, ataques que envolvem a **inserção de programas de computador maliciosos ou outros softwares corrompidos é o que há de mais fácil**.*
>
> *Máquinas DRE sem VICE **não contam com uma poderosa medida** para impedir ataques de software: as rotinas de auditoria automáticas pós-eleição que comparem os **registros em papel** com os registros eletrônicos."*

94 **Brunazo F., A.** A*valiação da Segurança da Urna Eletrônica Brasileira,* in *Anais do Simpósio de Segurança em Informática SSI 2000.* São José dos Campos: ITA, 10/2000 - *http://www.votoseguro.org/textos/SSI2000.htm*

Essas conclusões sobre riscos e custos de mais de 120 modalidades de fraudes no voto eletrônico, contidas no *Relatório Brennan,* estão fundamentadas em regras de avaliação explicitadas e em dados e tabulações apresentados, às claras, ao longo de suas quase 200 páginas.

Totalmente diferente da conclusão oposta que o CMTSE apresenta num sucinto parágrafo desassociado de qualquer estudo que a fundamente, sem mostrar dados, sem definir regras e métricas de avaliação e valendo-se aqui e ali de referências falsas.

Ainda, no item 5 das suas conclusões, o CMTSE coloca que "*o sistema vem funcionando sem comprovações concretas de fraude até o momento*".

Mais uma vez, é uma **conclusão fruto de análise superficial e incompleta**, onde deixou-se de ouvir aqueles que denunciam as dificuldades de produzir provas num processo sob total concentração de poderes como relatado nas Seções 3.1, 4.1.2, 4.2.3 e 4.2.4 desta Réplica.

Por fim, as quatro recomendações do CMTSE, presentes na Seção 4.2, refletem a superficialidade da análise desenvolvida. Resumidamente, são as seguintes:

1. Criar uma comissão pública para propor melhorias ao TSE.
2. Melhorar a comunicação do TSE com o público.
3. Criar um portal na Internet para atender o item 2.
4. Estabelecer cronograma para apresentação dos programas das urnas eletrônicas.

São recomendações diversionistas, que não focam os problemas apontados nos relatórios da CCJC

Por vazias que são, não causaram nenhuma reação ou aceitação pelo destinatário, o TSE. Passados 9 meses do seu enunciado, nada mudou.

Não se vislumbra como essas recomendações vazias possam atender a revindicação por formas mais simples de fiscalização que viabilizem técnica e financeiramente a auditoria do resultado eleitoral eletrônico pela sociedade.

5 Conclusões Finais e Recomendações do CMind

5.1 Conclusões sobre o Relatório CMTSE

A análise dos argumentos técnicos defendidos, bem como dos **OMITIDOS**, no *Relatório do CMTSE* revelou perceptível **PARCIALIDADE E SUPERFICIALIDADE**, como repetidamente demonstrado ao longo desta Réplica.

A **parcialidade na avaliação do tema** parece ter sido consequência direta da composição do CMTSE, que recaiu exclusivamente em membros comprometidos com o projeto do seu coordenador e assessorados apenas por funcionários da equipe técnica responsável direta pelo sistema criticado nos relatórios da CCJC.

Ao contrário da CCJC, que, como recomenda a prudência e o método científico, se abriu para ouvir defensores de diversas linhas de pensamento, o CMTSE se fechou e **evitou conhecer o contraditório**. Não procurou ouvir diretamente nenhum dos especialistas com visão discordante da administração eleitoral, citados nos relatórios da CCJC.

A **superficialidade da análise** desenvolvida pelo CMTSE se manifesta por diversas peculiaridades, tais como:

- **Referências bibliográficas escassas, imprecisas, generalizadas e, por vezes, falsas,** sem especificação clara e correta dos objetos, itens e capítulos citados (ver exemplos nas Seções 2.3 e 4.4 e Anexo 4 desta Réplica).
- **Omissão perante problemas denunciados** (vide Seção. 4.1 desta Réplica) **-** como o acúmulo de poderes do administrador eleitoral, a responsabilidade deste pela desinformação do eleitor durante a experiência com voto impresso em 2002 ou a falta de recursos e a inviabilidade prática para a fiscalização dos partidos.
- **Análises sucintas ou excessivamente reduzidas** (vide Seções 4.2.1, 4.2.2 e 4.3) **–** por exemplo, a descrição em apenas dois parágrafos do processo de desenvolvimento dos softwares eleitorais, declarando sua efetividade, quando conhece-se o estudo detalhado da Fundação COPPE-UFRJ, que precisou de 116 páginas, descrevendo as falhas que ainda persistem no mesmo processo.
- **Incoerência nos argumentos -** como apresentar a auto-verificação do software das urnas como se fosse auditoria independente do software (vide Anexo 4 desta Réplica) e ao indicar como salvaguardas o uso de Urnas Biométricas e os Testes de Votação Paralela, que são dois **recursos incompatíveis e mutuamente excludentes**, revelando que nem se percebeu a incompatibilidade.

Verifica-se que o *Relatório CMTSE* **consiste numa reprodução fiel dos argumentos** apresentados anteriormente por **seu coordenador** em audiências públicas na Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados mostrando sua natureza muito mais descritiva da posição oficial do que crítica sobre ela.

Para tomar emprestado créditos, **o CMTSE foi a extremos** chegando a citar, **com explícita inversão de mérito**, trabalhos técnicos de terceiros como justificativa de seus argumentos (vide Seção 4.4 e Anexo 4 desta Réplica).

Diante dessas condições, conclui-se que **o *Relatório do Comitê "Multidisciplinar" do TSE* não construiu a credibilidade necessária para o fim que se propôs**, devendo ser desconsiderado em qualquer análise séria com o fim de aperfeiçoar o nível de confiança e de segurança do sistema de votação eletrônica brasileiro.

...alguém pode enganar poucos por muito tempo,
muitos por pouco tempo,
mas não todos por todo o tempo.
Abraham Lincoln

5.2 Conclusões Gerais e Recomendações do CMind

A conclusão final do CMind é que o TSE pode e deveria fazer mais.

Além do sistema de **apuração rápida**, que já nos oferece, o TSE deveria propiciar uma sistema eleitoral de **apuração conferível** pela sociedade civil.

Com relação a todo o processo eleitoral brasileiro concluiu-se que nele há **exagerada concentração de poderes**, resultando em **comprometimento do Princípio da Publicidade e da soberania do eleitor** em poder conhecer e avaliar, *motu próprio*, o destino do seu voto.

Como consequência disso, constata-se que no sistema eleitoral brasileiro atual **É IMPOSSÍVEL para os representantes da sociedade conferir e auditar o resultado da apuração eletrônica dos votos**.

Em outras palavras, **desde 1996 a sociedade civil brasileira não tem como conferir e confirmar o resultado publicado pela autoridade eleitoral** e foi esta impossibilidade de auditoria independente do resultado que levou à **rejeição de nossas urnas eletrônicas em todos os mais de 50 países** que aqui vieram estudá-la.

As recomendações dos membros do *Comitê Multidisciplinar Independente* são as seguintes:

1. Propiciar **separação mais clara de responsabilidades nas tarefas de normatizar, administrar e auditar o processo eleitoral brasileiro**, deixando à Justiça Eleitoral apenas a tarefa de julgar o contencioso.

   Em especial, dentro da estrutura administrativa eleitoral, as funções de projeto, de operação e de auditoria interna deveriam ser totalmente separadas, não devendo as mesmas pessoas se ocuparem destas tarefas, como hoje ocorre.

2. Possibilitar uma **auditoria externa dos resultados eleitorais totalmente independente das pessoas envolvidas** na sua administração.

   Em especial, as regras de fiscalização e auditoria externa não podem ser estabelecidas pelos próprios administradores e operadores, os fiscalizados enfim.

3. **Regulamentar mais detalhadamente o princípio de independência do software em sistemas eleitorais** definindo claramente as regras de auditoria com o Voto Impresso Conferível pelo Eleitor.

   Em especial, na regulamentação do Art. 5º da Lei 12.034/09, deve-se cuidar para que não se volte a inviabilizar a conferência da apuração eletrônica.

ANEXO 1

Informação 002/2008-STI do TSE

Emitida no dia 11 de novembro de 2008, pelo Secretário de Informática do TSE e Coordenador do CMTSE

Comentários:

Esse ofício do TSE, cuja integra é apresentado adiante, foi emitido em resposta à petição de 12 de agosto de 2008 feita pelos **representantes dos partidos** que acompanhavam a apresentação dos sistemas no TSE e que pretendiam conhecer os **relatórios parciais** elaborados pela empresa FACTI, que estavam induzindo correções e modificações no software das urnas eletrônicas.

A **decisão, negando a apresentação dos relatórios**, foi dada em 12 de novembro de 2008, depois de **já encerrada a cerimônia de apresentação dos sistemas** em 15 de setembro de 2008.

Para justificar o impedimento de acesso dos representantes dos partidos aos relatórios parciais que afetavam os programas, no parágrafo 5 dessa informação foram apresentados os seguintes argumentos:

- A petição dos fiscais representantes dos partidos seria **uma inoportuna e não justificada interferência de terceiros**.

- Os relatórios parciais eram referentes à **fase inicial, inconclusa dos testes preparatórios** (embora já estivessem provocando modificações no sistema).

- O solicitado envolvia **matéria atinente à segurança em tecnologia da informação**.

Esses argumentos discricionários e incoerentes **revelam autoritarismo**. E a decisão de manter dados secretos demonstra a adesão do administrador eleitoral ao **Princípio de Segurança por Obscurantismo**, radicalmente impróprio para esse caso onde deveria prevalecer o **Princípio da Publicidade (ou Transparência) do processo eleitoral** cristalizado no Art. 66 da lei 9.504/97 o qual, apesar de ter sido citado na Subseção 2.1.1 do *Relatório CMTSE* como salvaguarda do processo, não é integralmente cumprido pela autoridade eleitoral.

A integra da *Informação 002/2008/STI* é apresentada a seguir.

Obs.: Os erros na numeração dos parágrafos constam do documento original.
Os destaques em negrito foram colocados pelo CMind.

TRIBUNAL SUPERIOR ELEITORAL

Informação n.º 002/2008 - STI
Referência: Petição nº 1896
Assunto: Petições nºs 11.209/2008 e 19.603/2008

Senhor Diretor-Geral,

Tratam-se de Petições protocolizadas pelo Partido dos Trabalhadores – PT, pelo Partido Democrático Trabalhista - PDT e pelo Partido da Republica - PR (Prot. 11.209/2008 e 19.603/2008 - fls. 45/51) requerendo, em síntese:

- Alterações na proposta de minuta de resolução que disciplina os testes de vulnerabilidade quanto à segurança do sistema eletrônico de votação;
- Juntada, aos presentes autos, do contrato TSE nº 32/2008, firmado com a FACTI, com a anuência do CTI, que tem como objeto a prestação de serviços de consultoria para a elaboração, o acompanhamento da execução e a posterior análise dos testes de vulnerabilidade;
- Juntada, aos presentes autos, dos relatórios, atuais e futuros, decorrentes dos testes de vulnerabilidade, para conhecimento e consideração dos senhores Ministros dessa Corte, em seus julgamentos.

2. A proposta de minuta de resolução referida pelos requerentes, foi elaborada pelo grupo de trabalho, instituído pela Portaria 339/2007, com vistas à realização de estudos sobre a viabilidade técnica da efetivação dos testes de vulnerabilidade. O referido grupo de trabalho acatou o pedido de alteração da minuta no sentido de conceder prioridade aos partidos políticos na indicação de investigadores para os testes, bem como, a extensão da exigência de título de doutor a todos os membros da Comissão Avaliadora. Contudo, não mereceu acolhida, o pedido para que os representantes da Justiça Eleitoral não tivessem direito a voto na Comissão Avaliadora, **tendo em vista que os representantes da justiça eleitoral constituirão minoria no quorum deliberativo, pois, a comissão será composta por um representante de cada partido político que, em outubro de 2008, já totalizaram 27** (vinte e sete), por representantes dos institutos de pesquisa, pelo Ministério Público, pela Ordem dos Advogados do Brasil e por, no máximo, 04 (quatro) representantes da Justiça Eleitoral. A propósito, o grupo de trabalho apresenta nova proposta de minuta de resolução, com as devidas alterações.

2. Não há óbice ainda, ao deferimento do pedido de juntada, aos presentes autos, do Contrato TSE nº 32/2008, mesmo porque, a formalidade e a publicidade, são princípios ínsitos a todos os contratos administrativos. Inclusive, a publicação do contrato, na imprensa oficial, é condição para sua eficácia.

3. O Contrato TSR nº 32/2008, em sua cláusula segunda, dispõe sobre a execução da prestação dos serviços de consultoria para a elaboração, o acompanhamento da execução e a posterior análise dos testes de vulnerabilidade, especificando as atividades a serem realizadas pela empresa contratada (FACTI) .

4. O cronograma dessas atividades, nos termos contratualmente ajustados, é composto de duas fases: a fase interna, relativa à análise preparatória dos testes. E a fase externa, na qual serão realizadas os testes públicos, com a participação de todos os interessados.

5. A execução do referido contrato encontra-se em sua fase inicial, inconclusa, dos **testes preparatórios, de interesse exclusivo desse Tribunal, por envolver matéria atinente à segurança em tecnologia da informação, o que impossibilita o deferimento do pedido de juntada de relatórios parciais**. Desse modo, **a interferência de terceiros, alheios ao contrato, além de inoportuna, não se justifica**, pelo fato de que, ao final, quando da realização dos testes públicos, os interessados terão amplo acesso e participação. Acrescente-se que os relatórios dos testes parciais em curso encontram-se devidamente arquivados neste Tribunal, e inteiramente á disposição dos Ministros desta Corte, bastando que sejam requisitados a esta Secretaria.

5. Convém aclarar, que, devido à conjuntura eleitoral, estuda-se a possibilidade da realização dos testes públicos no segundo semestre do ano de 2009.

A sua consideração,

Brasília, 12 de novembro de 2008.

GIUSEPPE DUTRA JANINO
Secretaria de Tecnologia da Informação

ANEXO 2

2002 e 2008 - Assinaturas Digitais Divergentes

Comentários:

Neste anexo são apresentados o *fac-simile* de dois documentos produzidos pelo administrador durante o processo eleitoral de 2002 e de 2008 que comprovam a ocorrência de problemas na verificação das assinaturas digitais e resumos digitais criptográficos (*hash*) nas urnas eletrônicas.

São exemplos acabados de como a concentração de poderes cria as condições para abusos que acabam por comprometer a transparência do processo eleitoral.

O documento de 2002 – apresentado no Anexo 2.1 – é um memorando da Secretaria de Informática do TRE-PB aos supervisores dos polos de carga de urnas onde comunica a ocorrência de divergências nas assinaturas digitais nas urnas eletrônicas relativas aos valores publicados no portal do TSE.

Com o explícito objetivo de "*evitarmos problemas com os partidos"*, ou seja, **para esconder o problema dos fiscais externos (MP e Partidos)**, o servidor eleitoral graduado passa uma nova instrução a seus subordinados de que "*só devemos imprimir o hash se for solicitado*", contrariando orientação geral que existia então de sempre imprimi-los para serem incluídos nas atas das cerimônias.

O documento de 2008 – apresentado no Anexo 2.2 - é a primeira página da Tabela de Hash denominada *Chaves das Urnas*[95]*,* que foi calculada no dia 25 de setembro de 2008, **sem a presença dos representantes dos Partidos**, OAB ou MP, dez dias após o encerramento da Cerimônia Oficial de Lacração dos Sistemas que ocorrera em 15/09/2008.

95 *http://www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/chaves_ue.pdf*

ANEXO 2.1

Doc. 3

Adailton Ventura

De: "Adailton Ventura" <adailton@tre-
Para: "natus" <natu-todos@tre-pb.gov.br>
Enviada em: sexta-feira, 18 de outubro de 2002 16:40
Assunto: [natu-todos] assinatura digital

Srs. Supervisores,

Descobrimos que a assinatura digital de alguns arquivos da Urna Eletrônica não estão em concordância com o que está na página do TSE na internet, mas a assinatura na UE está correta.
Neste caso, se algum partido reclamar de alguma discrepância, deve-se informar que o TSE está corrigindo site e colocará as assinaturas corretas.
O problema ocorre nas assinaturas de arquivos com extensão *.VRT

Veja o exemplo abaixo:

http://intranet.tre-pb.gov.br/arquivos/natus/download/documentos/diretorioFI.jpg

A assinatura dos arquivos acima selecionados no site do TSE é:

Nome	Sha-1 Radix64	Sha-1 Hexadecimal
avaudio.vrt	- /5ibHE3aBhJWzVqTPoZn0o8inU=	3FFE626C7137681849583 56A4CFA199F4A3C8A75
VERSAOSB.VRT	- 4mzFmCzRoVAtIRngEDDNtFnyLT0=	E26CC5982CD1A1502D2119E01030CDB459F22D3D

O que está errado.
Sendo assim até o TSE consertar o site e para evitarmos problemas com partidos só devemos imprimir o hash se for solicitado. Informo que se algum fiscal de partido fizer questão deve ser impresso os hash dos arquivos da FI/FV, usando o disquete VPRE-VPOS.
As listagens impressas devem ser assinadas pelas autoridades presentes e fiscais de partidos e afixadas em local visivel (mural do NATU)
Os partidos não poderão receber cópia dos documentos, apenas conferi-los com a relação disponibilizada na Internet pelo TSE.

Boa sorte.
Adailton Ventura
Setor de Urnas Eletrônicas
TRE-PB / Secretaria de Informática
Fone: 0 XX 83 214 1328
0 XX 83 214 1244
E-mail: adailton@tre-pb.gov.br

PODER JUDICIÁRIO PROTOCOLO GERAL

ANEXO 2.2

Resumos Criptográficos "Chaves da Urna" - pág. 1 de 4

arquivo completo em:
http://www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/chaves_ue.pdf

Calculados no dia 25 de setembro de 2008,
sem a presença dos representantes dos Partidos, OAB ou MP,
10 dias após o encerramento da
Cerimônia Oficial de Lacração dos Sistemas ocorrida em 15/09/2008

Eleições 2008
Listagem de Hashs

Chaves da urna
09/25/08

Nome	Sha-1 Radix64
AC - /uenux/app/chave/avusrchave.vmt	X/JHffgaDsAyy28eNd/PJ/3UNcE=
AC - /uenux/app/chave/bu.pk1	uZNIuSYp+O51H9w4NXamoiVEk/E=
AC - /uenux/app/chave/ue.pri	bRhJiYyllnj04AocGaJnKFKRDC8=
AC - /uenux/app/chave/ue.pub	+q2Ue4QRYKz3R/wLw6vD2V1Z6D4=
AC - /uenux/app/chave/vd.pk1	6njU854m11W+AhMAzvVcGu8LTRM=
AL - /uenux/app/chave/avusrchave.vmt	M7kUznTmQdnoMUP4Gz6mUXMoI8U=
AL - /uenux/app/chave/bu.pk1	NvtCUCXyS2i8zeovsgNpnLhaY+o=
AL - /uenux/app/chave/ue.pri	wrGwbkvVJkHKWd+BvyPwUO+a/20=
AL - /uenux/app/chave/ue.pub	5mBl2ZK0Q/QM47z56D8duWWWZMY=
AL - /uenux/app/chave/vd.pk1	4euiC5/JCC/C5ODuqSNyMFFhahA=
AM - /uenux/app/chave/avusrchave.vmt	tVZPFTz878ZNZFbl0xv0mZwr5Tw=
AM - /uenux/app/chave/bu.pk1	8GT7wbooZcr1iowqxlBl0wqa78o=
AM - /uenux/app/chave/ue.pri	i4Jeh7E8Gu3GiPI4oFB6MQN6bTc=
AM - /uenux/app/chave/ue.pub	EN/9MshvttdWqQvicZTJu9T4r8o=
AM - /uenux/app/chave/vd.pk1	qeJR/8py1WpRuyytlXS4nKQ3Ci0=
AP - /uenux/app/chave/avusrchave.vmt	REjbmOWXgAQXe12mwGihX9XlSAQ=
AP - /uenux/app/chave/bu.pk1	MqFAKrvEjolciTTSNhIiJ+EL5fA=
AP - /uenux/app/chave/ue.pri	wukd9PHEr62XpBSVMU8pEzR7Qis=
AP - /uenux/app/chave/ue.pub	PgxAFK3o0C2WIdbf3lP84X4Y9C0=
AP - /uenux/app/chave/vd.pk1	V3Abqc1ymvfLKFZN36iR3G0SSLk=
BA - /uenux/app/chave/avusrchave.vmt	xhUOvQyoHL/jpHwyycBZ7CSUEaI=
BA - /uenux/app/chave/bu.pk1	onwFiA4Kfok/g9W6kxw0VC96kmw=
BA - /uenux/app/chave/ue.pri	WzBfnw/tGjzGbXTZAT5B6BO2zL0=
BA - /uenux/app/chave/ue.pub	CtoZe+EpAwVK+1j5dgDNSm8TZ5o=
BA - /uenux/app/chave/vd.pk1	e6JIBYYyY8AIkot51t87CKieAOI=
CE - /uenux/app/chave/avusrchave.vmt	eQ1LWj82ustyveEXBHxwJGb5hWI=
CE - /uenux/app/chave/bu.pk1	hZ253DgNcLlMprJtaapA3VfiWGM=
CE - /uenux/app/chave/ue.pri	8Xb74K0ppsUm708xhksWT5ir+Mw=
CE - /uenux/app/chave/ue.pub	PHxF2HdxfkQeAJiofMc/4gs7mBU=
CE - /uenux/app/chave/vd.pk1	UB8Ph3ZC0wFlD8C94pzicyIrBgs=
DF - /uenux/app/chave/avusrchave.vmt	i1cvmoJsIiNyeHDAD1VLvV9ON44=
DF - /uenux/app/chave/bu.pk1	h75ZdWHbc9i79nRxp1iuR+yWoQg=
DF - /uenux/app/chave/ue.pri	lU7kkEeB0sjwAcWcqZjG5ebQZT4=

ANEXO 3

Extratos das *Diretrizes VVSG*

- traduzidos pelo CMind -

Voluntary Voting System Guidelines. U.S. Election Assistance Commission, 31/08/2007
http://www.eac.gov/vvsg

Intro: 2.4 - ***Independência do Software***

Part 1: 2.7 - ***Independência do Software***

Todos os sistemas de votação precisam ser independentes do software para estar conformes com esta norma.

Testar [a integridade lógica de] software é tão difícil que auditorias da precisão de sistemas eleitorais não podem depender do próprio software estar correto. Assim, sistemas eleitorais devem ser 'software independent' para que auditorias não precisem confiar na correção do software do próprio sistema.

Os registros dos votos [para auditoria] devem ser produzidos de maneira que sua exatidão não dependa da integridade do software do sistema.

Um exemplo de sistema dependente do software são as ***máquinas DRE, que não estão conforme com estas normas****.*

Intro: 2.4.1 – ***Registros Independentes (do voto) Conferíveis pelo Eleitor*** *(RICE)*

Part 1: 2.7.1 - ***Obtendo a Independência do Software via RICE***

É requerido que, para ser independente do software, ***todo sistema eleitoral inclua um equipamento para registro independente do voto conferível pelo eleitor*** *(RICE). RICE podem ser auditados independentemente do software do sistema de votação.*

Voto Impresso Conferível pelo Eleitor *(VICE) é uma forma de RICE baseados em papel.*

Atualmente, os sistemas de votação que podem satisfazer a definição de independência do software usam o registros em papel conferível pelo eleitor como:

- *digitalizadores ópticos em conjunto com votos escritos ou VICE*
- *máquinas DRE* ***com*** *VICE*

Part 1: 1.1.6 Requisitos Principais - ...

Esclarece-se que registros redundantes do voto (RDV) gravados em máquinas DRE são para fins de recuperação e ***não devem ser confundidos com registros independentes do voto conferível pelo eleitor*** *(RICE) como especificado na Part 1: 4.4 Registros Independentes (do voto) Conferíveis pelo Eleitor*

Part 1: 4.4.1 Requisitos Gerais - ...

*registros conferíveis pelo eleitor existem para prover um registro da vontade do eleitor independente **(RICE) que possa ser usado para verificar a exatidão do registro eletrônico (RDV)** produzido pelo equipamento de votação.*

Part 1: 4.4.1-A.1 Verificação pelo eleitor

*Equipamentos de votação DEVEM criar um RICE **que o eleitor possa conferir sem auxílio de software**, excetuando-se os programas-assistentes para deficientes.*

Part 1: 4.4.1-A.2 Conferência do RICE pelos fiscais

*Equipamentos de votação DEVEM criar um RICE **que fiscais eleitorais e auditores possam conferir sem auxílio de software ou equipamentos programáveis**.*

Part 1: 4.4.1-A.8 Formato público do RICE

*Equipamentos de votação DEVEM criar um RICE **em formato público disponível e sem restrições, legíveis sem informações confidenciais, proprietárias e comerciais**.*

Part 1: 4.4.1-A.14 Permitido conteúdo não legível no RICE

*O RICE **PODE incluir código e outras informações ilegíveis sobre o voto dado**.*

Part 1: 6.6-B.2 Formato de troca dos Registros do Voto

*Máquinas DRE e escaneadores óticos DEVEM usar um **formato público disponível e sem restrições para exportar (para outros equipamentos) os Registros de Voto**.*

ANEXO 4

A verificação das assinaturas digitais nas urnas eletrônicas

O uso de **assinaturas digitais como salvaguarda para determinar a integridade dos arquivos digitais** usado no processo eleitoral, só tem eficácia se acompanhado de procedimentos seguros de verificação dessas assinaturas.

No momento de conferência das assinaturas digitais ou dos resumos digitais criptográficos, se eles forem calculados sem que o próprio software sob análise esteja "*rodando*", **são independentes do software e têm validade**. No entanto, se forem gerados sob controle do próprio software a ser verificado, podem ser apenas uma simulação. Como a memoria permanente da urna é do tipo que permite escrita e leitura dinâmica, **as assinaturas digitais ou os resumos digitais devem ser verificados ANTES de qualquer programa ser executado** (inclusive antes até do sistema de inicialização, BIOS) e não depois.

As regras da verificação das assinaturas são estabelecidas pelo próprio administrador eleitoral, que nesse caso também é o agente cujo trabalho estará sendo fiscalizado. Em outras palavras, **no processo eleitoral brasileiro é o fiscalizado que estabelece as regras e limites da fiscalização**, o que não é uma prática jurídico-administrativa recomendável.

Em 2008, as regras de verificação das assinaturas, citadas na Subseção 2.1.2 do *Relatório CMTSE,* decorrem da Resolução TSE 22.714/2008 e são as seguintes:

a) Auto-verificação pelos programas de computador do sistema eleitoral.
b) Impressão dos resumos digitais (*hash*) dos arquivos das urnas e computadores, pelo programa VPP ou VAD.
c) Verificação de assinaturas por meio de "*programas próprios*" dos partidos, MP e OAB.

Obs.: o uso de aspas na expressão "*programas próprios*" se justifica porque, **contrário do que foi dito na Subseção 2.1.2 do *Relatório CMTSE***, em 2008 **nenhuma entidade fiscalizadora** usou, de fato, programas próprios para verificação das assinaturas digitais. O PDT e o PR optaram por não usar esse recurso por causa da falta de confiabilidade descrita neste anexo, e o PT, MP e OAB receberam, *pro-forma*, programas desenvolvidos e compilados pelo próprio ente fiscalizado, o TSE, e não os usaram de forma sistemática.

Essas 3 formas de verificação de assinaturas, permitidas no processo eleitoral, **não atendem ao conceito de *Independência do Software*** (vide Seção 3.3 desta Réplica) pois é o próprio software cuja integridade se quer determinar que, **estando em execução**:

- Faz a auto-verificação.
- Imprime os resumos digitais.
- Lança e controla o ambiente de execução dos programas verificadores.

A **ineficácia dessas formas de verificação de assinaturas foi cabalmente demonstrada** com a ocorrência de erro na geração das tabelas de resumos digitais já no TSE (caso descrito com mais detalhes na Subseção 3.1.4 desta Réplica).

O Programa VPP, item (b) acima, **acusava erro na verificação** pois imprimia uma relação de resumos digitais diferente da tabela oficial. Mas os arquivos extras contidos na lista impressa, dizia o TSE, eram legítimos, revelando que **o procedimento de verificação dos resumos digitais impressos pelo VPP resultava num "*falso negativo*"**.

O erro nas assinaturas dos sistemas pelo TSE também se propagou para os **programas verificadores**, item (c) acima, desenvolvidos pelo próprio TSE para uso pelo MP e pela OAB. Ao serem executados, os programas verificadores **nem mesmo detectavam a presença dos arquivos sem assinaturas** e não os listavam na respectiva tela de resultados**, ou seja, seu resultado, ainda pior, era um "*falso positivo*"**.

Esses fatos demonstram que **não é confiável nenhuma das duas formas '*dependentes do software*' para a verificação das assinaturas e resumos digitais que são permitidas pela administração eleitoral** aos fiscais externos.

É exatamente por causa dessa dependência direta do próprio software para determinar a sua integridade, que as *Diretrizes VVSG*[96] afirmam, em sua Seção Intro: 2.4 (vide Anexo 3 desta Réplica), o seguinte:

> *"Testar [a integridade lógica de] software é tão difícil que auditorias da precisão de sistemas eleitorais não podem depender do próprio software estar correto. Assim, sistemas eleitorais devem ser 'independente do software' para que auditorias não precisem confiar na correção do software do próprio sistema.*
>
> *Um exemplo de sistema dependente do software são as máquinas DRE, que **não estão conforme** com estas normas."*

O uso permitido para os programas verificadores de assinaturas consiste em se **colocar um disquete na urna** e depois ligá-la para que o fiscal possa, de braços cruzados, observar a tela com o resultado de pretensa "*verificação*". Além de contrariar as *Diretrizes VVSG*, essa forma de verificação também está **em flagrante conflito** com o que foi proposto na Seção 5.5 do chamado *Relatório "Unicamp"* [97], que diz:

> *"Após a inseminação da urna **deve ser permitido aos representantes de partidos o acesso aos programas internos da urna** para cálculo e verificação da conformidade de seu resumo com aquele divulgado ao final do processo de compilação...*
> ***Como sugestões para a implementação da verificação da autenticidade dos programas**, podem ser consideradas as seguintes alternativas:*
> - ***utilização de um flash card externo** que contenha um programa verificador;*
> - ***verificação** do flash card interno **em computador independente**."*

Essas duas alternativas propostas no *Relatório "Unicamp"*, se atendidas, garantiriam total controle do ambiente computacional pelo fiscal externo, permitindo que a verificação de assinaturas fosse feita ANTES de ser executado os softwares da urna, pois:

---

96 *Voluntary Voting System Guidelines.* USA: U.S. Election Assistance Commission, 31/08/2007 -
página virtual em: http://www.eac.gov/vvsg
relatório completo em: http://www.eac.gov/files/vvsg/Final-TGDC-VVSG-08312007.pdf

97 **Tozzi, C.L. et al.** - *Avaliação do Sistema Informatizado de Eleições.* Campinas: TSE, maio de 2002 -
http://www.tse.gov.br/internet/eleicoes/relatorio_unicamp/rel_final.pdf

- as urnas eletrônicas têm sua inicialização (*boot*) preferencial pelo conector externo de cartões flash[98]. Assim, **o *flash-card* externo pode assumir, como *processo-pai,* o controle do ambiente digital da urnas** e verificar a integridade do que está gravado lá dentro de **forma totalmente independente**;
- num computador independente da urnas, obviamente, a verificação de assinaturas também seria **independente do software da urna**.

Isto mostra que esta sugestão no chamado *Relatório "Unicamp"* estava, precocemente, apontando para o conceito de *Independência do Software* na sua proposta de verificação das assinaturas digitais, antes mesmo desse conceito ter sido enunciado em 2006 pelo inventor da técnica de assinatura digital.

No entanto, no sistema brasileiro, **é o próprio software a ser auditado que controla a plataforma e o ambiente computacional** onde está instalado o programa de verificação de assinaturas. O programa verificador, gravado em disquete, é executado dentro deste ambiente e não tem nunca como assumir o seu controle. Estará sempre sob controle do próprio software a ser auditado.

Nada impede que um software maliciosamente adulterado instalado numa urna eletrônica, burle essas verificações e gere resultados falso-positivos da seguinte forma:

a) Não executa a auto-verificação e segue adiante.
b) Imprime os resumos digitais oficiais previamente conhecidos e publicados.
c) Controle a ação dos programas verificadores, camuflando os arquivos adulterados.

Por isso, todas essas formas permitidas de auto-verificação permitidas pela autoridade eleitoral não atendem ao conceito de independência do software e **não servem como salvaguardas de segurança contra a adulteração do próprio software**.

Dentro das regras em que pode atuar, o auditor ou fiscal do partido **nunca terá como saber se a urna eletrônica fiscalizada contém um software honesto ou um desonesto** que burla as verificações permitidas.

Porém, o mais surpreendente é que, no lugar de denunciar **a ineficácia da verificação de assinaturas como regulamentado pela autoridade eleitoral** e, ainda, que a proposta de verificação das assinaturas contidas na Seção 5.5 do chamado *Relatório "Unicamp"* **nunca foi atendida pelos procedimentos adotados pelo TSE,** o CMTSE diz, na Subseção 2.1.3 do seu relatório, o seguinte:

> *"Essa medida de auto-verificação foi implantada em atendimento à sugestão do Relatório da UNICAMP de 2002"*

Como a sugestão do citado, de verificação das assinaturas em **plataforma computacional independente**, nunca foi de fato atendida pela regulamentação do TSE em seus detalhes essenciais, revela-se aqui outra **evidente inversão de mérito** relativa ao conteúdo de obra citada no *Relatório CMTSE*.

Com esta atitude, **o CMTSE volta a praticar ato impróprio**, de natureza similar àquele descrito na Seção 4.4 desta Réplica, **que depõe contra a credibilidade do seu relatório e dos seus membros**.

98 A sequência de *boot* ou de inicialização das urnas eletrônicas é: 1) conector externo de cartões flash; e 2) flash-card interno. **Nunca o *boot* ocorre pelo disquete**, o que impede os programas verificadores gravados em disquete de funcionarem em um ambiente independente do próprio software das urnas eletrônicas.

ANEXO 5

Voto Eletrônico e Transações Financeiras Digitais

Com frequência, entre leigos em segurança de dados, costuma-se comparar a segurança e a confiança em sistemas de voto eletrônico com sistemas digitais de transações financeiras. O argumento básico e simples costuma ser:

> *"a tecnologia digital permite transmissão segura de valores enormes por computadores então também pode desenvolver sistemas seguros para a contagem de votos"*.

O CMTSE, na Subseção 3.2.1 de seu relatório, aparenta endossar este argumento ao citar como referência bibliográfica para reforçar suas posições, o seguinte artigo:

> ***Paper versus Electronic Voting Records - An Assessment.***
> *http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm (17 a 27) 2/14/2006 10:04:09 AM*

Esse artigo, escrito em 2004 por **Michael Ian Shamos**, professor da Carnegie Mellon University, defende que o voto impresso não resolve os problemas de segurança de *Máquinas DRE* e, na base do seu argumento, compara o nível da segurança em máquinas eletrônicas de votar com a eletrônica embarcada em aviões comerciais e com sistemas financeiros virtuais que "*executam transações financeiras de, pelo menos, $ 2 trilhões por dia*".

Shamos é uma voz quase solitária no meio universitário norte-americano quando defende essa posição. É bem maior o número de professores universitários e teóricos da computação que argumentam na posição contrária.

Citamos, a seguir, 3 autores americanos, todos detentores de grande reconhecimento no meio acadêmico internacional, que afirmam que a **dificuldade para se construir sistemas eleitorais seguros é incomparavelmente maior** do que outros sistemas, inclusive sistemas financeiros. Citamos também trabalho original de um dos coautores desta Réplica, que analisa os fundamentos e a natureza desta incomparabilidade.

Ronald Rivest, cuja importância fundamental na área de segurança de dados digitais e do voto eletrônico foi descrita na Seção 3.3 desta Réplica, no artigo "A *Modular Voting Architecture*"[99] publicado em 2001, apresentou a seguinte consideração:

> *"INTRODUÇÃO...*
>
> *A princípio, nós deveríamos estar aptos para construir sistemas eletrônicos de votação confiáveis. Na prática, isto é surpreendentemente difícil. Parece* ***muito mais difícil do que construir sistemas de comércio eletrônico confiáveis****.*
>
> *Uma razão que torna difícil construir sistemas digitais eleitorais confiáveis é que* ***deve ser impossível*** *para o eleitor provar para terceiros em quem votou... O voto digital, uma vez gravado, precisa ser simultaneamente anônimo e ilegível (criptografado).* ***Isto torna o voto eletrônico mais desafiador do que o comércio eletrônico****, onde existir recibos e* ***documentos de rastreamento detalhados*** *e completos é a norma."* *(tradução do CMind)*

---

99 **Rivest, R. et al.** - *A Modular Voting Architecture.* CalTech-MIT Voting Technology Project, EUA, 2001 - *http://people.csail.mit.edu/rivest/BruckJeffersonRivest-AModularVotingArchitecture.doc*

Já Bruce Schneier, premiado criptógrafo e autor dos maiores *best-sellers* sobre segurança digital, no seu artigo "*Internet Voting vs. Large-Value e-Commerce*"[100] diz:

> *"Há duas importantes diferenças entre grandes transações financeiras e votação que fazem as primeiras muito mais aptas para implementação em sistemas digitais: anonimato e recuperabilidade.*
>
> *… sistemas financeiros com identidade (cartões de crédito, ordens de pagamento, PayPal, etc.) são muito mais comuns que versões de 'dinheiro eletrônico' porque são mais fáceis de tornar seguros. Todas as transações financeiras de alto valor carregam nomes em anexo: quem recebe o dinheiro e quem paga. Votos carregam apenas o nome dos destinatários;* ***a principal característica do voto secreto é eliminar o nome do eleitor. É isto que torna muito mais difícil proteger o sistema de fraudes, muito mais difícil de detectar fraudes e muito mais difícil de identificar o fraudador e prendê-lo****.*
>
> *Outra diferença entre grandes transações financeiras e votação é que se pode reconstruir a trilha da transação financeira. Isto é importante. Se alguém manipula um roubo de um bilhão de dólares de um sistema financeiro, pode-se congelar a transação, tentar descobrir o que ocorreu e, possivelmente, recuperar o dinheiro.*
>
> *Se alguém ajeita para desviar um voto, não tem nada que se possa fazer (o eleitor não pode ser chamado para uma nova votação)... Nossos sistemas de votação não possuem a mesma capacidade de refazer transações que os sistemas financeiros possuem.*
>
> ***Construir um sistema de votação seguro em rede é um problema muito difícil, mais difícil que todos os outros problemas de segurança em computador*** *que enfrentamos e não solucionamos."* (tradução do CMind)

Peter G. Neumann, cientista chefe do Computer Science Laboratory da ONG SRI International, um dos pioneiros a propor em 1993 os critérios de segurança necessários para sistemas eleitorais digitais, em seu artigo *"Security Criteria for Electronic Voting"*[101], já comentava e previa as dificuldades de se implementar sistemas eleitorais:

> *"CONCLUSÕES...*
> *O requisito de inviolabilidade do voto e o requisito auditabilidade plena e garantida de ponta a ponta do voto são* ***conceitualmente contraditórios****. É essencialmente impossível contemplar ambos requisitos ao mesmo tempo [em sistemas eleitorais] sem recorrer a complicados mecanismos que, por sua vez, podem introduzir novas vulnerabilidades e oportunidades de subversão sofisticadas."*
> (tradução do CMind)

E por fim, Pedro Antônio Dourado de Rezende, coautor desta réplica e pioneiro no estudo de modelos semiológicos de confiança para segurança em informática, expõe no artigo "*Modelos de Confiança para Segurança em Informática*" [102], o seguinte:

---

100 Schneier, B. - *Internet Voting vs. Large-Value e-Commerce.* Em Crypto-Gram Newsletter, Counterpane Internet Security, Inc. - 15/02/2001 - *http://www.schneier.com/crypto-gram-0102.html#10*

101 Neumann, P.G. - *Security Criteria for Electronic Voting* - Computer Science Laboratory da SRI International; 1993 - *http://www.csl.sri.com/neumann/ncs93.html*

102 Rezende, P. A. D. - *Modelos de Confiança para Segurança em Informática.* Departamento de Ciência da Computação, UnB: 2009 - *http://www.cic.unb.br/~pedro/trabs/modelos_de_confianca.pdf*

> *"a utilidade das técnicas criptográficas [por exemplo, assinatura digital ou cifragem para sigilo] requer certas condições de confiabilidade no preparo do material que habilita ao uso dos mecanismos escolhidos, pelo que o uso adequado dos mesmos presume uma situação em que tais condições estejam atendidas. Ainda, o uso eficaz na situação presume, também, escolhas adequadas à natureza da proteção almejada. É fato – por demais ofuscado, mas paradigmático – que há contextos onde dos mesmos dados e ao mesmo tempo um interesse a proteger demanda sigilo enquanto outro, integridade apenas (transparência), e, desses dados, nenhum interessado é mais "dono".*
>
> *Por isso é útil, quando necessário, distinguir entre segurança da informação, segurança informacional (relativa a informação) e na informática (relativa a contextos informáticos). Confusões entre essas metas de proteção assumem postura ideológica ao reduzir todas à primeira, que é oblívia a conflitos entre interesse legítimos, trivializando as diferenças.* ***Tais confusões, intencionais ou não, sempre dificultam a distinção entre teatro e processo de segurança, principalmente onde houver conflitos de interesse****. Entre sigilo e transparência, por exemplo, o foco da proteção nos dados (e não nos interesses) ofusca conflitos e empoderamentos.*
> *…*
> *A possibilidade de conluio já se constitui, pois em vetor para refinamentos na análise de riscos e na gestão da Política de segurança.*
>
> *Na prática, um modelo de interesses unipolar serviria para representar, além de enredos trágicos em teatros de segurança, a semântica de riscos em sistemas cujos computadores foram desligados das tomadas e trancados em cofre cujo segredo foi perdido. ... A segurança em foco se resumiria a "safety". Trata-se, portanto, de um modelo inútil para processos reais de segurança não-triviais no estágio atual das tecno-imersões de práticas sociais, apesar de estar implícito em modelagens da Política de Segurança de* ***entidades complexas que desconsideram, às vezes deliberada ou casuisticamente, riscos de ataque originados internamente*** *("todos aqui são honestos, alguém duvida disso?!").*
>
> *Ainda, enredos trágicos são também encenados no processo da segurança de entidades complexas cuja abordagem a riscos corresponde à modelagens [de interesses] bipolar; isto é, por entidades cuja Política de Segurança mapeia interesses conforme uma lógica binária, "nós contra eles", reducionista demais para a situação em foco. Encenações desses enredos tendem a surgir em situações que envolvem sistemas sensíveis em rede aberta, ou sistemas em rede fechada que atendem a interesses conflitantes e oponíveis ao interesse superveniente (do dono do sistema).* ***Ao não contemplar refinamentos multipolares*** *[de interesses potencialmente conflitantes] em sua análise de riscos, por orientação precária ou por outra razão,* ***essas entidades se expõem****, junto com outras afetas à situação e talvez despreparadamente,* ***à condição de reféns****, a armadilhas de colusão envolvendo mediadores e terceiros, ou ambas."*

O que escapa à abordagem de Michael Shamos, é o fato de que **a modelagem bipolar de interesses é útil para a segurança digital de aplicações financeiras**, posto que o cliente e sua instituição financeira têm interesses que se alinham, **enquanto é perigosa para a segurança digital de sistemas de votação eletrônica**, posto que o eleitor interessado em eleição limpa e dois candidatos que concorrem a um pleito têm interesses potencialmente conflitantes entre si, pelo que **o risco de colusão - envolvendo operadores do sistema de votação - deve ser, neste caso, não apenas considerado, mas basilar para a eficácia do processo de segurança**.

ANEXO 6

Contradita à explicação do Caso Caxias-MA 2008

No esclarecimento ao Questionamento 7, contido no item I.1 do Anexo I do *Relatório CMTSE,* é apresentado **um esclarecimento impróprio** ao comentário feito pelo eng. Amilcar Brunazo Filho, membro do CMind, sobre o caso ocorrido na cidade de Caxias, MA, em 2008.

Uma reportagem da TV Bandeirantes, logo após as eleições, apresentava reclamações de eleitores e incluiu uma fala de 8 segundos de duração do eng. Amilcar Brunazo Filho.

Nessa fala, foi feito um comentário sobre o fato de existirem 16 arquivos "*extras*" nas urnas eletrônicas que não constavam da Tabela de Resumos Digitais (*hash*) originais, que haviam sido calculadas no dia 15 de setembro de 2008 durante a cerimônia oficial de lacração dos sistemas no TSE.

No Anexo 2.2 e na Subseção 3.1.4 desta Réplica está apresentada, respectivamente, a tabela dos hashs "*extras*" e a explicação sobre o erro da equipe técnica do TSE que resultou na geração dessa nova tabela somente no dia 25 de setembro, **FORA da cerimônia oficial e longe dos olhos dos fiscais representantes dos partidos**, entre os quais se incluía o eng. Brunazo.

Para uma entrevista sucinta para televisão aberta, não cabiam explicações detalhadas sobre criptografia, assinaturas digitais e integridade de software. O eng. Brunazo se expressou nos seguintes termos, nos 8 segundos que dispôs:

> *"Na hora que tem programa lá dentro [das urnas] que ninguém sabe de onde veio, eu não sei o que o programa faz. Pode fazer qualquer coisa. Pode desviar voto, pode identificar voto, pode fazer o que quiser."*

No Esclarecimento 7 a esta entrevista, o CMTSE, no lugar de explicar que ocorreu um erro da equipe técnica do TSE durante a geração das tabelas de *hashs* que impedia os fiscais saberem de onde provinham tais arquivos extras, **optou por esconder o erro dos seus assessores** e impropriamente afirmou:

> *"Questionamento 7: O engenheiro Amilcar Brunazo afirma que a urna possui arquivos que "ninguém sabe de onde veio".*
>
> *Esclarecimento 7:*
> ***Todos os sistemas da urna eletrônica são assinados digitalmente para garantia de autoria e procedência**. Se as assinaturas digitais não estiverem corretas a urna eletrônica não funciona."*

Para efeito de fiscalização, a **eventual garantia de autoria ou procedência de arquivos digitais só pode ser considerada válida se a assinatura digital desses arquivos ocorrer em condições assistidas e controladas pelos fiscais** e não a portas fechadas como ocorreu nesse caso.

O Eng. Amílcar Brunazo Filho mantém sua afirmação de que havia programas nas urnas eletrônicas em 2008 que *"ninguém [os fiscais] sabia de onde vinham"*.

ANEXO 7

O Registro Digital do Voto - RDV

O Registro Digital do Voto, *RDV*, foi criado em 2003 pela Lei 10.740/03, para substituir o Voto Impresso Conferível pelo Eleitor.

A aprovação dessa lei contou com forte apoio e pressão por parte do presidente do TSE de então, min. Sepúlveda Pertence, que interferiu ativamente tanto na votação da lei no Senado quanto na Câmara dos Deputados.

No Senado, o Min. Pertence telefonou para o relator na CCJ, **durante a sua votação**, para solicitar a aprovação sem modificações. Na Câmara, compareceu no último dia do prazo à reunião de lideres para solicitar a aprovação da lei em regime de urgência urgentíssima, no que foi atendido pelos parlamentares[103].

Nessas duas oportunidades, prometeu-se aos parlamentares que qualquer ajuste necessário na lei seria feito posteriormente por meio de resolução do TSE.

Embora a ideia do *RDV* viesse acompanhada de promessas de total transparência e acesso aos partidos[104], desde a sua criação em 2003, **o TSE nunca permitiu acesso livre dos partidos aos *arquivos RDV***.

2006 – RDV negados

Uma petição – PET TSE 2.722/2006 – **de dezembro de 2006**, onde um partido político **solicita acesso aos *RDV*** de cinco Estados (Brasília, São Paulo, Rio de Janeiro, Paraná, Alagoas, Bahia e Goiás), passados mais de 3 anos, **ainda não foi respondida**.

Sua apreciação vem sendo sistematicamente protelada no TSE, juntando-se pareceres e contra-pareceres de departamentos internos da administração eleitoral, onde foi posta até a alegação de que o acesso ao RDV permitiria a violação do voto.

Também no Caso Alagoas-2006 (vide Subseção 3.1.7 desta Réplica), **foi negado acesso aos *arquivos RDV*** para os assistentes técnicos da parte que questionou o resultado e demonstrou haver diferenças na quantidade de votos registrados entre os *arquivos LOG* e os *arquivos BU*.

A negativa de apresentação dos RDV de Alagoas partiu da Secretaria de Informática do TSE através da Informação nº 90/2006-ASPLAN/STI sob o argumento primeiro de ser *"questão de segurança"*.

Lembre-se, no entanto, que antes da adoção das urnas eletrônicas, **100% dos Registros do Voto** de então – as cédulas eleitorais – eram automaticamente abertas e mostradas para conhecimento dos fiscais dos partidos. Enfim, **o Registro do Voto, virtual ou material, deveria ser um documento de caráter essencialmente público, como impõe o Princípio da Publicidade**.

---

103 Ver noticia do TSE em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=12796*

104 Ver último parágrafo em: *http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=12801*

2008 – RDV "pré-processados"

O acesso aos *arquivos RDV* originais gerados pelas urnas eletrônicas **não foi possível nem mesmo em 2008, quando foi emitida a resolução TSE 22.770/08** que estabelece normas e procedimentos para a distribuição do *arquivo RDV* para fins de fiscalização, **conferência, auditoria**, estudo e estatística.

Essa resolução, **cuja redação foi proposta pelo coordenador do CMTSE**, estabelecia ainda que os *arquivos RDV* fossem criptografados e, para serem entregues aos solicitantes, deveriam antes serem "*decriptografados*" ou *"pré-processados"* por sua equipe técnica.

Mas, o §6º do Art. 59 da Lei 9.504/97, que trata deste assunto, estabelece apenas que **o arquivo RDV receba Assinatura Digital mas não prevê Criptografia**.

A diferença funcional entre estas técnicas são:

- **Assinatura Digital** – garante a **integridade** e a **autenticidade** de arquivos digitais mas **mantém a legibilidade** do documento. A conferência de uma assinatura digital é sempre feita através de uma CHAVE PÚBLICA sendo, portanto, perfeitamente compatível com o Princípio de Publicidade.

  Em outras palavras, a assinatura digital tem por função *"impedir a substituição de votos e a alteração dos registros",* como previsto no §6º do Art. 59 da Lei 9.504/97, mas **sem impedir que o conteúdo do arquivo possa ser visto, lido e conferido** por um eventual fiscal ou auditor que a ele tenha acesso, independente de interferência por terceiros;

- **Critpografia** – garante a **confidencialidade** de documentos digitais, **tornando-os ilegíveis**. O deciframento de dados criptografados é sempre feita por meio de uma CHAVE SECRETA, de forma que é um procedimento que enfrenta o Princípio da Publicidade.

  Essencialmente a criptografia, que literalmente significa "*escrita escondida*", modifica o conteúdo de um arquivo para que este se torne ilegível ou incompreensível para quem a ele tenha acesso. Para recuperar a legibilidade, para uso por um eventual fiscal ou auditor, o arquivo criptografado necessita antes ser decifrado (ou *"pré-processado"*) por aquele que detenha a chave secreta de deciframento.

Assim, o secretário da STI/TSE e coordenador do CMTSE, ao propor o texto da resolução que determina a criptografia do RDV e que seu deciframento seja centralizado sob seu próprio comando, basicamente, **usou o poder de legislar da autoridade eleitoral para criar um privilégio e um poder para si próprio**, ou seja, arvorou a si próprio a inédita tarefa de **conhecer e filtrar todos os Registros dos Votos de todas as urnas eletrônicas antes destes serem mostrados aos fiscais**.

E foi usando este poder discricionário, não previsto em lei, que se recusou a apresentar os RDV de Alagoas em 2006, como citado acima.

Criou, assim, um viés onde o atendimento ao Princípio da Publicidade do registro do voto deixa de ser automático e direito de todos candidatos, passando a ser tutelado pelos agentes com o privilegio de serem os únicos a poder ler e conhecer o conteúdo do RDV diretamente.

Certamente, este viés agride o caráter público inerente a todo registro do voto e **não está na direção de dar segurança ao cidadão**, pois está baseado em modelo de segurança bipolar (Vide Anexo 5 desta Réplica) onde **o risco de colusão - envolvendo operadores do sistema de votação – não está sendo considerado.**

No Esclarecimento 9 presente no Anexo I.2 do *Relatório CMTSE,* se afirma que o ***RDV* corresponde à cédula em papel**, mas na Subseção 4.1.1 desta Réplica, mostrou-se que há diferenças fundamentais entre o voto impresso e o voto virtual a ponto deste comprometer o Princípio da Publicidade no processo eleitoral, e a criptografia do RDV vem agravar essa impropriedade.

As *Diretrizes VVSG*, que o CMTSE citou como **referência relevante** a justificar as opções de segurança adotadas, estabelecem as regras para geração e guarda de documentos usados para conferência ou recontagem dos votos em máquinas de votar, em especial dos **registros dos votos**, nos seguintes termos:

> *Part 1: 4.4.1 Requisitos Gerais - ...*
>
> > *registros do voto conferíveis pelo eleitor existem para prover um registro da vontade do eleitor independente **que possa ser usado para verificar a exatidão do registro eletrônico** produzido pelo equipamento de votação.*
>
> *Part 1: 4.4.1-A.2 Conferência do RICE pelos fiscais*
>
> > *Equipamentos de votação DEVEM criar um registro independente do voto **que fiscais eleitorais e auditores possam conferir sem auxílio de software ou equipamentos programáveis**.*
>
> *Part 1: 4.4.1-A.8 Formato público do RICE*
>
> > *Equipamentos de votação DEVEM criar um registro independente do voto **em formato público disponível e sem restrições,** legíveis **sem informações confidenciais**, proprietárias e comerciais.*
>
> *Part 1: 6.6-B.2 Formato de troca dos Registros do Voto*
>
> > *Máquinas DRE e escaneadores óticos DEVEM usar um **formato público disponível e sem restrições para exportar [para outros equipamentos] os Registros de Voto**.*

Todas essas regras indicam que os registros do voto devem ser criados e mantidos pelas máquinas de votar em **formato aberto e legível** pelos fiscais.

Ou seja, dever-se-ia recorrer apenas às técnicas de assinatura digital (que mantém a legibilidade do texto), mas não de criptografia (que eliminam a legibilidade), para preservar a integridade e autenticidade do *RDV*.

Uma vez que a integridade e autenticidade do *RDV* já são garantidas por técnicas de assinatura digital, imposta por lei, o uso de criptografia nesse caso, imposta pela autoridade eleitoral, tem a única função de **manter o acesso ao *RDV* controlado exclusivamente pela equipe do coordenador do CMTSE**, o que contraria todas as regras de transparência e segurança sugeridas nas *Diretrizes VVSG.*

Todos os fiscais que solicitaram o *RDV* ao administrador eleitoral em 2008 receberam arquivos descriptografados e editados e **o mesmo irá ocorrer em 2010**, pois o TSE não aceitou sugestão de partido político para suprimir a criptografia do *RDV* nas urnas.

Nestas condições, contrariando as promessas da autoridade eleitoral aos parlamentares, **os *arquivos RDV* originais nunca puderam ser vistos pelo fiscais**, e continuam sendo mantidos inacessíveis desde sua criação em 2003.