ADI 4543/2011 – APRESENTAÇÃO DE RAZÕES – PDT

ANEXO 1

Sintonia entre a nova Lei e a Evolução da Tecnologia Eleitoral no Exterior

A tecnologia do voto eletrônico desenvolveu-se no anos 80 quando surgiram os primeiros artigos acadêmicos[1] sobre votação eletrônica, introduzindo o conceito de máquinas de votar DRE (de "*Direct Recording Electronic voting machines*"), que gravam o voto em meio digital – o ***Registro Digital do Voto***.

Máquinas DRE podem ser entendidas como a **1ª geração** de equipamentos eleitorais eletrônicos.

Em 1991, máquinas DRE começam a ser usadas em eleições na Índia, em 1992 na Holanda, em 1994 nos EUA e em 1996 no Brasil.

Em 2000, o Brasil torna-se o primeiro país a ter 100% do eleitorado votando com urnas eletrônicas DRE de 1ª geração.

Em máquinas DRE de 1ª geração, a confiabilidade da apuração eletrônica depende diretamente da qualidade do software utilizado para gravar o *Registro Digital do Voto* e, para verificar tal qualidade, recorre-se à **auditoria eletrônica do sistema,** como pontuado em nota do TSE de 18 de agosto de 2011, aqui acostada como ANEXO 8, que, relatando a debate dos ministros do TSE em torno da presente ADI 4543, conclui com a seguinte afirmação:

> *"... a **Justiça Eleitoral entende** que o uso da impressão do voto na perspectiva de se realizar uma auditoria não tem sentido, **porque todo o sistema pode ser auditado eletronicamente**."* *(destaque em negrito nosso)*

Porém, mesmo que se confirme que a cúpula dos administradores do processo eleitoral entenda não perceber vantagens numa auditoria do resultado eleitoral por uma via independente do software usado, a existência de uma forma alternativa de auditoria, **não tinge de inconstitucionalidade ao artigo de lei questionado na ADI 4543**.

1 a) Saltman R.G. *Accuracy, Integrity, and Security in Computerized Vote-Tallying*. NBS (now NIST) special publication, 1988.
b) Neumann P.G. *Risks in Computerized Elections (Inside Risks)*. Comm. ACM 33, 11, p. 170, November 1990.

O conceito de **auditoria eletrônica do sistema eleitoral** está fortemente ligado a procedimentos técnicos de **validação** do código-fonte e de **certificação** do software eleitoral por meio de **técnicas de assinatura digital**, como esclarece o portal *"Urna Eletrônica"* do TSE, onde é dito:

http://www.tse.gov.br/internet/urnaEletronica/index.html

*"O processo eletrônico de votação possui **mecanismos imprescindíveis para assegurar sua segurança: a assinatura digital** e o resumo digital.*

*A assinatura digital é uma técnica criptográfica para garantir que um conteúdo, no caso um arquivo digital, possa ser verificado principalmente no que se refere à sua integridade, isto é, **busca garantir que o programa de computador não foi modificado** de forma intencional ou não perdeu suas características originais por falha na gravação ou leitura. Isso significa que se a assinatura digital for válida, o arquivo não foi modificado.*

*Mas **a assinatura digital também é utilizada para assegurar a autenticidade do programa**, ou seja, confirmar que o programa tem origem oficial e foi gerado pelo Tribunal Superior Eleitoral. Neste caso, somente quem assinou digitalmente pode ter gerado aquela assinatura digital"* (destaques nossos)

Porém, **a eficácia da auditoria eletrônica e da assinatura digital** para garantir a confiabilidade técnica de sistemas eleitorais complexos **vem sendo fortemente contestada** no meio acadêmico e no âmbito jurídico internacional.

*Obs.: a expressão "confiabilidade técnica", aqui usada, se refere à confiança em sistemas informatizados que é estabelecida **por avaliações e critérios técnicos quantificados e normatizados**, e não à confiança pessoal ou intuitiva que alguém possa atribuir a terceiros. Por exemplo, o simples ato formal de assinatura digital por agentes que não participaram de processos de análise e validação de um sistema ou software complexo, não estabelece nem determina a confiabilidade técnica desse sistema*.

Apresenta-se, através do documento no ANEXO 9, as **especificações das urnas eletrônicas** modelo 2009 referentes ao *"Software Básico, Segurança e Criptografia",* cujo item (n) da seção 2.3 especifica que o dispositivo (*chip*) de segurança e autenticação **deverá utilizar a tecnologia denominada RSA** para a criptografia assimétrica, assinatura digital e verificação da assinatura.

A técnica RSA de assinatura digital, núcleo dito imprescindível da auditoria eletrônica utilizada pelo TSE, foi inventada em 1978, entre outros, pelo **Ph. D. Ronald Rivest**, como se pode ver no documento ANEXO 10, com a primeira página da enciclopédia virtual Wikipedia sobre o verbete *"RSA"*.

E **é o próprio cientista que inventou e patenteou a técnica de assinatura digital** utilizada na auditoria eletrônica pelo TSE que, em trabalhos publicados desde 2001 [2], **desqualifica a eficácia da assinatura digital** para assegurar a confiabilidade técnica de software eleitoral complexo.

Em trabalho conjunto do Massachusetts Institute of Technology e o NIST (órgão normativo) apresentado em 2006 [3], o prof. Rivest, afirma:

> *"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*** *dentro de restrições fiscais razoáveis* ***(testes exaustivos do software de sistemas eleitorais certamente teriam custo proibitivo)****. "*
> (tradução nossa)

Assim, questionada pelo próprio inventor por seu custo proibitivo, **uma auditoria eleitoral eletrônica que fosse eficaz tornou-se o fulcro do debate** sobre a segurança e a confiabilidade técnica de eleições informatizadas.

No Brasil, esse debate foi iniciado no meio acadêmico[4] durante as edições anuais do ***Simpósio sobre Segurança em Informática*** *(SSI)*, realizado no ITA entre 1999 e 2006 e culminou no meio legislativo na ***Subcomissão Especial de Segurança do Voto Eletrônico*** da CCJC da Câmara dos Deputados, que realizou sete audiências públicas entre 2007 e 2008.

Via de regra, a eficácia da auditoria eletrônica é defendida pelos operadores do sistema eleitoral e é contestada no meio acadêmico e pelo agentes externos de fiscalização eleitoral.

Respeitando o princípio do contraditório, os legisladores reuniram e ouviram, de um lado, representantes da administração eleitoral no Brasil, **defensores da auditoria eleitoral eletrônica** e, do outro lado, professores especialistas em Tecnologia da Informação e representantes e fiscais de partidos políticos e da OAB, **defensores de métodos alternativos para auditoria do resultado eleitoral**.

---

2 Rivest, R.R. et al. - *A Modular Voting Architecture.* CalTech-MIT Voting Technology Project, EUA, 2001 - http://people.csail.mit.edu/rivest/BruckJeffersonRivest-AModularVotingArchitecture.doc

3 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

4 Brunazo Filho, A. *A Segurança do Voto na Urna Eletrônica Brasileira* - In: SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA, 1999, São José dos Campos. *Anais...* São José dos Campos: ITA, 1999. P.19-28. http://www.votoseguro.org/arquivos/SSI99int.zip

Após ponderar as duas visões, **considerando o alto custo da fiscalização eletrônica**, a subcomissão da CCJC apresentou dois relatórios [5] e projetos de lei que reconheciam a ineficácia da auditorial eletrônica e aderiam ao *Princípio da Independência do Software em Sistemas Eleitorais*, adiante detalhado.

Ainda no âmbito legislativo, o debate continuou com a Justiça Eleitoral criando (Portaria TSE 192) um *Comitê Multidisciplinar*, coordenado pelo seu Secretário de Tecnologia de Informação (STI/TSE), que entregou um relatório aos membros da subcomissão dos deputados no dia 26 de maio de 2009 [6].

Em seu relatório, o ***Comitê Multidisciplinar do TSE*** defende a eficácia da auditoria puramente eletrônica do sistema eleitoral e, para apoiar seu ponto de vista, apresenta referências bibliográficas de seguinte forma:

> *"...**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) [7]

Para avaliar e obter um contraponto ao novo relatório do TSE, a *Subcomissão Especial de Segurança do Voto Eletrônico da Câmara dos Deputados* solicitou a mais especialistas e a todos os agentes externos (OAB e Partidos Políticos) já envolvidos na avaliação dos sistemas eleitorais.

Formou-se um grupo de especialistas que autodenominou-se ***Comitê Multidisciplinar Independente***, e que apresentou seu relatório [8] aos deputados da subcomissão em abril de 2010 [9], onde refutavam as teses e, em especial, demonstraram que **as referências bibliográficas citadas pelo Comitê Multidisciplinar do TSE não corroboravam seus argumentos**.

Pelo contrário, **os relevantes estudos citados pelos próprios representantes do TSE, apoiavam de forma clara a mesma posição dos relatórios da subcomissão dos deputados contra a eficácia da auditoria eletrônica em sistemas eleitorais**, como relata o seguinte trecho extraído da Seção 4.4 do relatório do comitê independente:

---

5 Relatórios dos Deputados disponíveis em: http://www.votoseguro.org/textos/sve2007-relatorio.pdf e em: http://www.votoseguro.org/textos/sve2008-relatorio.pdf

6 Nota relatando a entrega do relatório do Comitê Multidisciplinar do TSE aos deputados disponível em: http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1187457

7 Esta referência no relatório do TSE está mal formada e, de fato, quer remeter à dois relatórios, a saber:
a) **Relatório Brennan**: Norden L.D. et al. - *The Machinery of Democracy: protecting elections in an electronic world.* New York: Brennan Center of Justice, NYU, 2006 – Sumário em português em: http://www.votoseguro.org/textos/brennan-pt.pdf
b) **Diretrizes VVSG**: *Voluntary Voting System Guidelines.* USA: U.S. Election Assistance Commission, NIST, 31/08/2007 - http://www.eac.gov/vvsg

8 Sérvulo da Cunha, S. et all. *Relatório do Comitê Multidisciplinar Independente.* Brasília: edição dos autores, 2010. 105 p. - http://www.votoseguro.org/textos/RelatorioCMind.pdf

9 Ver em: http://www.votoseguro.org/textos/relatoriocmind-divulg.htm

"No sumário executivo 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...*

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 Comitê do TSE**, 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.*

*Portanto, **o conteúdo do Relatório Brennan NÃO CORROBORA O ARGUMENTO DO Comitê TSE** 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 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 Comitê TSE**, as Diretrizes VVSG **explicitamente descredenciam** o uso de máquinas DRE sem Voto Impresso Conferido pelo Eleitor.*

Em resumo, os dois relevantes estudos apontados pela referência ambígua do Comitê Multidisciplinar do TSE afirmam o oposto ao citado. Ou seja, dizem literalmente o contrário daquilo que os autores do TSE lhes imputam pelo contexto da referência." (destaques em negrito no original)

Falando em nome próprio, **todos os representantes da OAB e de partidos políticos (PT, PDT e PR)** que, desde 2004, se apresentaram para conhecer o sistema informatizado de eleições **nos termos do Art. 66 da lei 9.504/97** com a redação dada pela Lei 10.740/2003, foram unânimes em afirmar [10] :

*"... 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**."*

10 Sérvulo da Cunha, S. et all. *Relatório do Comitê Multidisciplinar Independente*. Brasília: edição dos autores, 2010. 105 p. - o trecho citado encontra-se na Seção 5.2 com as Conclusões Gerais, na página 85 - http://www.votoseguro.org/textos/RelatorioCMind.pdf

O representante da OAB assim descreveu as suas duas tentativas, em 2004 e 2006, de analisar e validar o software do sistema eleitoral [11]:

> *"Embora o TSE tenha desde logo divulgado 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.*
>
> *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.*
>
> *…*
>
> *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**" (destaque em negrito no original)*

11 Sérvulo da Cunha, S. et all. *Relatório do Comitê Multidisciplinar Independente.* Brasília: edição dos autores, 2010. 105 p. - o trecho citado encontra-se na Seção 3.2.1, na página 40

Para concluir, o representante da OAB informa que:

" 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...;*

*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**."*

No exterior, nos últimos oito anos, essas mesmas insuperáveis dificuldades práticas e limitações econômicas para uma eficaz validação e certificação do software de equipamentos eleitorais eletrônicos **levou à evolução da informatização eleitoral** no sentido de complementar a auditoria eletrônica do software eleitoral com outras formas de auditoria do resultado que não dependam da confiabilidade desse mesmo software.

Nesta direção, destacam-se os seguintes eventos:

- 2004 – Venezuela – 100% do eleitorado passa a votar em urnas eletrônicas modelo Smartmatic SAES3000, com **voto impresso conferido pelo eleitor**, para uso em **auditoria que independe do software** (por recontagem dos votos impressos de 1,5% das urnas).
- 2006 – o Ph. D. Ronald Rivest, que também é o inventor da técnica de assinatura digital usada pelo TSE, formaliza o ***Princípio da Independência do Software em Sistemas Eleitorais*** que passa a definir a **2ª geração de equipamentos eleitorais eletrônicos**, ou seja, aqueles nos quais é possível se desenvolver uma auditoria da apuração de forma independente do software utilizado, no lugar de se tentar estabelecer a confiabilidade no software por meio de uma cara e ineficaz análise do código e assinatura digital.
- 2007 – EUA – o *Princípio da Independência do Software em Sistemas Eleitorais* é adotado [12] pelas agência federais norte-americanas EAC (*Election Assistance Commission*) e NIST (*National Institute of Standards and Technology*), que declaram que os únicos modelos conforme com o novo padrão são as urnas eletrônicas com voto escaneado ou com voto impresso conferido pelo eleitor.

12 *"Voluntary Voting System Guidelines"*. USA: U.S. Election Assistance Commission, 31/08/2007 - *Página virtual em: http://www.eac.gov/vvsg* – ver adoção do princípio na seção *Introduction: 2.4*

- 2008 – Na Holanda, 16 anos após as primeiras experiências oficiais, passa a ser proibido o uso de urnas eletrônicas DRE de 1ª geração sem voto impresso por causa das dificuldades práticas de se determinar a confiabilidade técnica dos equipamentos.
- 2009 – Na Alemanha, **o Tribunal Constitucional Federal declara inconstitucional, por afronta ao Princípio da Publicidade, o uso de máquinas DRE de 1ª geração**, como melhor detalhado adiante.
- 2011 – Na Argentina, as urnas brasileiras de 1ª geração, testadas até 2006, foram abandonadas. Foi adotado urnas de 2ª geração nas Províncias de Salta e do Chaco, com previsão de atingir 100% do eleitorado em 2015. O documento ANEXO 11 contem reportagem publicada na Internet que assim descreve a urna argentina: "*... el elector va armando su voto hasta que queda definitivamente conformado y **se imprime en una "boleta"** que deberá plegar para introducirla luego en la urna*".

Após ponderar todas as posições a favor e contra a eficácia da auditoria eleitoral eletrônica, em mais de dois anos de debates na *Subcomissão Especial de Segurança do Voto Eletrônico*, **o legislador brasileiro acabou por aprovar o Artigo 5º da Lei 12.034/09,** aderindo ao *Princípio da Independência do Software em Sistemas Eleitorais* com os conceitos de *"voto impresso conferido pelo eleitor"* no seu *caput* e de *"auditoria (do resultado) independente do software"* no § 4º.

Ao acolher tal princípio, a nova lei cria condições concretas e objetivas, antes inexistentes, para:

- DETECTAR, por via automática e independente do software utilizado nas urnas, **eventual alteração desse software**, vinda de origem interna ou externa, que resulte em erro na apuração dos votos (§§ 1º ao 4º).
- IMPOSSIBILITAR, de forma absoluta, **eventual alteração do software** das urnas que possibilite uma identificação sistemática do voto (§ 5º).

A definição técnica formal [13], dada pelos responsáveis, para a *Independência do Software em Sistemas Eleitorais* é a seguinte:

> *"Um sistema eleitoral é independente do software se uma **modificação ou erro não detectado** no seu software não pode causar uma **modificação ou erro indetectável** no resultado da apuração" (tradução nossa)*

O *Princípio da Independência do Software*, em oposição à auditoria eletrônica, exige um **Registro do Voto Independente do Software** a uma **Auditoria Automática da Apuração**, com o objetivo de **viabilizar economicamente uma auditoria do resultado** e tornar o voto eletrônico protegido contra adulterações não detectadas do software. Assim, o **Artigo 5º da Lei 12.034/09** pode ser chamado por ***Lei do Voto Protegido*** (contra erros ou fraudes não detectadas no software).

13 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