Critérios para Avaliação da Segurança do Voto Eletrônico

Eng. Amílcar Brunazo Filho
Diretor Técnico da TD Tecnologia Digital Ltda.
Moderador do Fórum do Voto Eletrônico na Internet
amilcar@brunazo.eng.br

Resumo

Neste artigo se descreve os tipos de máquinas eleitorais, apresentando a nova geração que está sendo proposta no Brasil e nos EUA: as Máquinas de Apuração Conferível, nas quais os votos são apurados eletronicamente mas que oferecem uma forma de recontagem para efeito de auditoria. Também se faz uma análise da confiabilidade das urnas eletrônicas brasileiras segundo critério de avaliação de sistemas eleitorais sugerido por Peter Neumann. Ao final sugere-se que sistemas eleitorais automatizados sejam tratados como "Sistemas de Alto Risco de Fraudes".

1. Introdução

No ano de 2000 houve eleições no Brasil e nos Estados Unidos da América. Os problemas ocorridos na apuração das eleições americanas levaram muitos a alegarem a superioridade do sistema brasileiro.

Mas… **foi o nosso processo eleitoral informatizado avaliado sob critérios técnicos adequados**?

Em diversas cidades do Brasil houve dúvidas sobre processo eletrônico eleitoral, tendo ocorrido passeatas (Rio de Janeiro, RJ), depredações e incêndios (Barcarena, PA, e Bayeux, PB), greve de fome (Diadema, SP) e até atentados à vida (Umuarama, PR). Ocorreram também casos inquestionáveis de erros, como em Araçoiaba da Serra, SP, onde sete candidatos não tiveram suas fotos incluídas nas urnas e onde, por ordem do juiz, se violou e induziu a votação conforme relatado pelo jornalista Marcelo Soares da Folha de São Paulo (referência http6).

Mas nenhum recurso pedindo recontagem dos votos, conferência da apuração ou anulação do pleito foi aprovado por nossa Justiça Eleitoral, a qual detém poder executivo, legislativo e judiciário a um só tempo (Brunazo, 1999, item 3.2). O Tribunal Superior Eleitoral, TSE, **não ofereceu** aos partidos e eleitores **nenhuma forma de se conferir a apuração dos votos** e não foi julgado procedente nenhum recurso contra atos operacionais dos próprios juizes eleitorais regionais. O julgamento do caso de Araçoiaba da Serra - *acordão nº 138.441 do TRE/SP* - bem ilustra o espírito de corpo da justiça eleitoral com suas conseqüências danosas à credibilidade do sistema e foi comentado pelo jornalista Oswaldo Maneschy (Maneschy, 2001).

Para se determinar o grau de confiabilidade do voto informatizado no Brasil, apresenta-se na seção 2 deste artigo alguns **critérios para avaliação da segurança de sistemas eleitorais automatizados** e na seção 3 é apresentado uma classificação dos tipos de sistemas existentes. A seguir, nas seções 4 e 5, demonstra-se que o sistema eleitoral informatizado desenvolvido pelo TSE é um processo baseado no princípio da "**Segurança por Obscurantismo"** e se faz uma breve avaliação deste sistema segundo os critérios sugeridos.

Na seção 6 é apresentada a conclusão de que se deve classificar sistemas eleitorais como sendo "**Sistemas de Alto Risco de Fraude**", merecendo destarte um tratamento que contemple o princípio de **Segurança por Transparência** e utilize **canais de controle redundantes**. Na seção 7, ao final, se propõe a **impressão do voto** como canal de controle alternativo para possibilitar a **conferência da apuração** em máquinas eletrônicas.

2. Sistemas Eleitorais Automatizados – Critérios de Avaliação

Muitos analistas especializados em votação eletrônica, brasileiros e americanos, como Edgardo Gerck, Peter G. Neumann, Lorrie Cranor e Rebecca Mercuri, têm sugerido critérios para avaliação da segurança (security) e confiabilidade de sistemas eleitorais automatizados.

Ed Gerck iniciou um trabalho de coleta de recomendações de segurança que deveriam ser respeitadas por qualquer sistema eleitoral público, qualquer que seja a tecnologia utilizada. A última versão deste trabalho (Gerck, 2001), contém 16 requisitos considerados necessários, entre eles: inviolabilidade do voto garantida (até contra ordem judicial) por sistema totalmente livre de falhas; verificabilidade da integridade do sistema; auditoria e recontagem dos votos devem ser possíveis; e uso apenas de programas de código aberto, inclusive os dos sistemas de criptografia e assinatura digital (apenas as senhas privadas devem ser secretas).

Mercuri, em sua tese de doutorado (Mercuri, 2000), analisou os critérios de segurança ISO, basicamente a Norma Técnica ISO/IEC 15.408 de Dez/99 (http1), e concluiu que, ainda que muito rigorosas, estas normas são insuficientes para atender as necessidades de segurança e confiabilidade de uma eleição pública. Mercuri recomenda a adoção de critérios adicionais mais rigorosos para a avaliação de sistemas eletrônicos de votação.

Lorrie Cranor, em (Cranor, 1996), esboça um critério para de avaliação de sistemas eleitorais eletrônicos e propõe um elaborado sistema eleitoral criptográfico, chamado Sensus, que permite a conferência da apuração

pelo próprio eleitor. Mas ela mesmo reconhece que seu sistema não atende de forma ideal o item "*verificabilidade*" do seu critério de avaliação. Conclui que existe um natural conflito entre segurança e a necessidade de manter a inviolabilidade do voto e também afirma que sistemas eleitorais eletrônicos exigem características adicionais de segurança além daquelas concernentes a um sistema computacional seguro comum.

Antes disso, Peter Neumann já havia concluído que, mesmo sob um critério de avaliação simples, proposto em (Neumann, 1993), é muito difícil se construir um sistema eleitoral eletrônico que atenda todos os itens de tal critério e que *"alguns riscos (de segurança) são inevitáveis"*. O critério de avaliação da segurança de sistemas eleitorais eletrônicos proposto por Neumann é o seguinte:

- **Integridade do Sistema** – O sistema de computador deve ser à prova de modificação depois de validado e certificado por auditores externos.
- **Integridade e Confiabilidade dos dados** – Os votos devem se gravados corretamente e devem ser à prova de modificações.
- **Anonimato do Eleitor** – A associação entre o voto e a identidade do eleitor deve ser **impossível**.
- **Autenticação do Operador** – As pessoas autorizadas devem ter mecanismos de controle de acesso não triviais. Senhas fixas e "portas-do-fundo" para manutenção, por exemplo, não são recomendadas.
- **Auditabilidade do Sistema** – todas as operações internas do sistema devem ser monitoradas mas sem violar a confidencialidade dos votos. Toda alteração de programas e de dados de controle deve ser registrada. Deve ser impossível evitar este monitoramento ou modificar seus relatórios.
- **Transparência do Sistema** – Todos os programas, documentação, equipamentos, microcódigos e circuitos especiais devem ser abertos para inspeção a qualquer momento, a despeito de qualquer alegação de segredo dos fornecedores.
- **Disponibilidade do Sistema** – deve haver proteção contra ataques por saturação, também chamados de ataques DoS, e o sistema deve estar sempre disponível durante o periodo eleitoral.
- **Confiabilidade do Sistema** – o projeto deve minimizar os efeitos de erros e de códigos maliciosos.
- **Facilidade de Uso** – O uso do sistema deve ser ameno para eleitores e operadores. A interface com o usuário deve ser à prova de falhas e deve prever o mau uso acidental ou proposital.
- **Documentação e segurança** – Todo o projeto e implementação, inclusive a relativa a testes e segurança deve estar toda documentada consistentemente e sem ambigüidades.
- **Integridade do Pessoal** – O pessoal envolvido deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.

Este critério proposto por Neumann é bastante rigoroso apesar de simples e sucinto e demonstra o seu entendimento de que o voto eletrônico pede extremo zelo no trato da segurança. Poder-se-ia, ainda, acrescentar os seguintes itens aos critérios de Neumann:

- **Precisão** – eleições que podem ser decididas por apenas um voto não podem tolerar nenhuma margem estatística de erro durante a operação. Até o erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.
- **Resistência a falhas** – é desejável a existência de métodos de detecção de falhas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.
- **Resistência a fraudes** – a principal característica que **diferencia um sistema eleitoral** de outros sistemas de alto risco, é que ele é alvo freqüente de ataques mal intencionados. Medidas de defesa contra fraudes, inclusive as vindas do próprio corpo interno de projetistas, **devem ser rigorosas e redundantes**.

> ***Observação****: Michael Ian Shamos (Shamos, 1993) e Ed Gerck (Gerck, 2001), defensores do voto 100% eletrônico, comparam a confiabilidade de máquinas eleitorais com computadores de grandes aeronaves. Argumentam que mesmo não sendo possível se testar à exaustão um software de alto risco, ainda assim se confia e se voa num 747, o que justificaria se tolerar uma urna eletrônica mesmo que o sistema não tenha sido 100% testado. Esta comparação pode valer quando se trata de* ***falhas não intencionais*** *(safety) mas é inadequada quanto se trata de* ***fraudes propositais*** *(security). Pela experiência histórica, não se espera que o projetista de um sistema de controle de vôo o faça falhar propositadamente. Já com sistemas eleitorais informatizados, o projeto de segurança deve sempre prever que agentes internos possam atacar o sistema, como já ocorrido no Brasil no Caso Proconsult (Mineiro, 2000).*

3. Sistemas Eleitorais Automatizados - Tipos

Os sistemas tradicionais de votar podem ser classificados em **sistemas de apuração direta**, como as votações abertas ou por aclamação, e **sistemas de apuração posterior**, idealizados para assegurarem a inviolabilidade dos votos, nos quais o voto é materializado através de uma cédula eleitoral secreta.

Com sistemas automatizados de voto pode-se criar uma classificação semelhante:

- **Sistemas (máquinas) de Apuração Direta – MAD ou DRE** – São máquinas que possuem um contador ou acumulador de votos para cada candidato. O eleitor deve escolher seu candidato dentre aqueles apresentados pela máquina e registrar o seu voto, que será automaticamente adicionado ao acumulador do respectivo candidato. Estas máquinas podem ser mecânicas, com contadores de engrenagens e alavancas para votar, ou eletrônicas, com teclados e monitores. Máquinas mecânicas deste tipo garantiam o sigilo do voto mas já caíram em desuso. Recentemente surgiram as MAD eletrônicas que são chamadas de "*Direct Recording Electronic Voting System*" (DRE). O sigilo do voto numa MAD eletrônica só estará garantido se for possível demonstrar que nela não se grava os votos **abertos e ordenados** em separado, para posterior consulta. Além disso, uma MAD sempre será passível de fraudes por adulteração do seu programa. Assim, **a validação e certificação do seu software deve ser muito rigorosa**.
- **Sistemas (máquinas) de Apuração Posterior – MAP** – São sistemas que separam a votação da etapa de apuração dos votos. Para isto utilizam duas máquinas distintas, uma para o eleitor votar e outra para contar os votos. O eleitor vota numa máquina que **materializa o voto numa cédula,** por perfuração (*punchcard*) ou por impressão padronizada (*mark sense*). As cédulas são depositadas em urnas lacradas e depois são apuradas por máquinas contadoras. O sigilo do voto é garantido pelo uso de **cédulas sem identificação do eleitor** e de urna larga o suficiente para embaralhar os votos. As vantagens de uma MAP são a facilidade do eleitor comum entender como se garante a inviolabilidade e a possibilidade de recontagem dos votos a qualquer momento. Suas desvantagens são a fragilidade contra troca de cédulas e os erros de leitura.
- **Sistemas (máquinas) de Apuração Conferível – MAC –** são sistemas mistos, MAP e MAD, nos quais a apuração eletrônica é feita simultaneamente com a votação, mas é possível se conferir posteriormente a apuração por meio de uma recontagem dos votos. Para tanto, uma MAC deve prover uma forma de se guardar os votos de cada eleitor em separado mas, ainda assim, garantir a inviolabilidade do voto. Para isso pode-se recorrer à **materialização do voto** (voto em papel) ou a recursos matemáticos de proteção do voto virtual, como a *Assinatura Digital Cega* (Fujioka, 1993) ou a *Criptografia Homomórfica* (Neff, 2000).

Sistemas MAC com voto materializado têm a vantagem de aumentar as dificuldades para o fraudador, que teria que fraudar dois sistemas diferentes (o eletrônico e o impresso) para obter êxito num ataque dirigido, e assim diminui-se as exigências de qualificação de seu software. O tipo MAC pode ser entendido como uma **nova geração** de sistemas eleitorais automatizados, conforme sugerido por Mercuri em recente entrevista (http8) ao comentar sobre "os novos padrões que estão chegando".

Um exemplo de MAC são os **sistemas de eleição pela Internet** propostos pela SafeVote (http2) e VoteHere (http3). Mas, embora a idéia de voto pela Internet seja sedutora, existem críticos, (Philipps,1999) e (Hoffman, 2000), que a consideram prematura. De uma forma geral, ainda persistem problemas, como ataques por saturação, páginas falsas para roubo de senhas e, principalmente, a possibilidade de indução do voto, que no Brasil é chamado de voto-de-cabresto, se for permitido o voto em ambientes sem garantia de uma cabina indevassável ou se for permitido a posterior conferência do voto pelo próprio eleitor pela Internet.

4. Segurança por Obscurantismo

A urna eletrônica (UE) brasileira é uma MAD e sua confiabilidade depende de uma rigorosa validação e certificação do seus programas, já que nela não é possível se recontar os votos. Uma MAD pede absoluta transparência e auditabilidade em todos equipamentos e programas, como se vê em (Neumann, 1993), (Kitcat, 2000), (Schneier, 2000), (Gerck, 2001) e especialmente no relatório feito por Roy G. Saltman (Saltman, 1996), consultor do National Institute of Standards and Technology, NIST, contratado pelo TSE em out/96, onde diz:

> *"Para assegurar confiança pública nos resultados, é importante que os partidos políticos e outros grupos de interesse sejam parte do processo que garanta integridade do sistema. Isto requer que o* ***código-fonte*** *da UE seja disponibilizado para revisão de técnicos representantes dos partidos e outros interesses, e que esta revisão seja feita com generoso apoio e assistência do governo.* ***No processo de revisão precisa ser mostrado que o código-objeto realmente usado nas UE correspondem exatamente, num sentido lógico, ao código-fonte que foi examinado****... Para contribuir para este processo ajudaria muito se* ***a propriedade intelectual associada com o sistema pertencesse ao governo nacional****...".* - tradução do autor deste artigo

Mas o TSE adotou o princípio de ***Segurança por Obscurantismo*** contrariando as recomendações para máquinas MAD. Evidencia-se esta política adotada pelo TSE nos seguintes documentos oficiais:

- **Art. 13 da Resolução 19.877/97 do TSE** - Deixa explícito que "*O projeto da Urna Eletrônica … assenta-se no sigilo de seu funcionamento*".
- **Art. 2, Parag. único da Portaria 142/00 da Diretoria Geral do TSE** – declara que o sistema operacional da UE e sua biblioteca de segurança (criptografia) **não serão disponibilizados para análise do código** pelos técnicos dos partidos políticos. Esta portaria contraria o Art. 66 da Lei 9.504.

- **Resolução 20.714/00 do TSE** – nesta longa resolução, em resposta a uma impugnação dos programas das UE, o TSE afirma que os códigos-fonte do sistema operacional e da biblioteca de criptografia não podem ser apresentados para análise por motivos de segurança e de direitos autorais, já que **não é sua a propriedade intelectual**. O TSE também afirma que **não pode permitir aos fiscais dos partidos conferirem se o código-objeto carregado nas UE corresponde ao mostrado aos fiscais**, alegando motivo de segurança.
- **Decisão do Pedido de Liminar do Mandado de Segurança nº 2.914 –DF do TSE** – Um Pedido de Liminar contra a Portaria 142 e a Resolução 20.714, acima citadas, foi indeferido pelo TSE sob um argumento que é a própria explicitação do princípio do obscurantismo: "*… a restrição de acesso à segurança do sistema não denota falta de confiança nos integrantes das agremiações políticas, antes demonstra uma preocupação com a própria segurança, **pois é fato que menos pessoas tiverem acesso a tais informações, menor a possibilidade de vulneração e risco** à segurança das eleições*".

  Observação: O julgamento do mérito deste Mandado de Segurança contra a falta de transparência do TSE, que foi solicitado antes do primeiro turno das eleições de 2000, seria de fundamental importância para dar credibilidade ao processo eleitoral informatizado. Mas, pela peculiaridade do nosso sistema eleitoral, cabe ao próprio TSE julgar este recurso em que também é o réu. Numa atitude absolutamente obscurantista, até o momento em que já deu posse aos eleitos, o TSE protelou e não julgou o mérito da questão.

5. Avaliação da Urna Eletrônica Brasileira

Submetendo a UE aos critérios de avaliação da segurança propostos pelos diversos autores verifica-se que ela não se sai bem. Dos 16 requisitos em (Gerck, 2001), 3 não se aplicam à UE e ela é reprovada em 8 dos 13 restantes. Quanto aos critérios em (Neumann, 1993), vários itens são contrariados e nos demais a análise é inconclusiva, como se demonstra a seguir:

- **Integridade do Sistema** – REPROVADO - Conforme entrevistas concedidas ao Jornal do Brasil em 30/08/2000 e à Folha de São Paulo em 15/10/2000 (http7), pelo Eng. Oswaldo Catsumi Inamura, da Aeronáutica e do TSE, **os programas das UE foram modificados** depois de terem sidos apresentados aos auditores externos **e não foram reapresentados para análise** depois disso.
- **Integridade e Confiabilidade dos dados** – INCONCLUSIVO – são permitidos testes apenas em máquinas previamente preparadas para o teste e não em máquinas prontas para votar.
- **Anonimato do Eleitor** – SEM GARANTIAS – A associação entre o voto e a identidade do eleitor é uma hipótese não afastada, visto que o número do eleitor é fornecido à UE no mesmo momento em que ele digita seu voto e não se permite análise completa dos programas.
- **Autenticação do Operador** – REPROVADO – Em todos os terminais da rede do TSE, inclusive os que contem os códigos-fonte dos aplicativos e das bibliotecas padrão dos compiladores, está instalado um programa de manutenção remota, o PCAnyWhere, que possui "portas-do-fundo" para acesso remoto. O Sistema SiS, de controle de acesso, também possui portas para manutenção de emergência.
- **Auditabilidade do Sistema** – INCONCLUSIVO – Fiscais de partidos de Boa Vista, RO, relataram testes de dupla carga dos programas nas UE da 1ª Zona Eleitoral. Os arquivos de log destas urnas não revelam o fato, levando a crer que a carga dos programas na UE apaga o log existente anteriormente, perdendo registros úteis para auditoria que poderiam revelar uma fraude. Considera-se este tópico inconclusivo, pois não se obteve uma confirmação formal do teste feito na presença do juiz e do promotor público.
- **Transparência do Sistema** – REPROVADO – como demonstrado no item 4.
- **Disponibilidade do Sistema** – NÃO ANALISADO – o TSE, no entanto, afirma ter criado defesas contra ataques DoS na sua rede durante o período da totalização dos resultados.
- **Confiabilidade do Sistema** – APRESENTA FRAGILIDADES – nas UE os votos de cada candidato é constantemente mantido em memória temporária, RAM, sem dígito de verificação. A cada voto novo, o acumulado é regravado em memória permanente, Flash Card, sem verificação de integridade (novo valor = valor anterior + 1). Assim, uma eventual troca indevida em um bit na RAM, se propaga.
- **Facilidade de Uso** – APROVADO COM RESTRIÇÕES - para um eleitor acostumado a teclados e computadores a UE é fácil de usar, para outros nem tanto. Muitas reclamações de "*foto de candidato errado*", que surgiram em quase todos os municípios, foram devidas a dificuldades de uso da UE. O TSE não divulgou nenhuma estatística sobre a freqüência deste problema, que não foi pequena.
- **Documentação e segurança** – INCONCLUSIVO – os fiscais dos partidos não tiveram acesso à toda documentação, inclusive não foram apresentadas as alterações no código-fonte nem as justificativas destas alterações intempestivas feitas depois destes códigos terem sido apresentados aos fiscais.
- **Integridade do Pessoal** – NÃO AVALIADO – é difícil avaliar a "incorruptibilidade" de pessoas. Relate-se que houve muitas denúncias de falhas da segurança na guarda física das UE, com desvios e roubos.

6. Conclusões - Segurança por Transparência e Controles Redundantes

A reprovação da UE segundo os critérios de avaliação da segurança clama por correções no seu projeto e no seu processo de desenvolvimento e implantação. É evidente a necessidade de se adotar a política da **Segurança por Transparência**, como aparece nas obras citadas de Jason Kitcat, Roy G. Saltman, Peter G. Neumann e Rebecca Mercuri e como também é aceito por defensores do voto 100% eletrônico, como David Jefferson e Michael Shamos (http4) e Edgardo Gerck (Gerck, 2001).

Shamos até lançou um desafio público dizendo que poderia descobrir qualquer tentativa de fraude **numa** MAD/DRE, **desde que lhe seja dado acesso ao código da máquina** imediatamente antes e depois da votação/apuração. Destaque-se que o desafio de Shamos, lançado para provar a eficiência das técnicas de validação e certificação dos programas de uma MAD, é um teste que não se aplica ao voto pela Internet e se refere apenas a **uma única** MAD cujo programa de seu **total conhecimento**, não valendo para 320.000 MAD simultaneamente, como é o caso das eleições brasileiras.

Por outro lado, Ken Thompson, um dos idealizadores do sistema UNIX, deixa claro que não é suficiente se analisar e conhecer apenas os códigos-fonte do aplicativo principal e do sistema operacional de uma MAD. Num artigo (Thompson, 1984), citado freqüentemente em trabalhos que discorram sobre confiabilidade de sistemas, fica claro que um compilador maliciosamente modificado pode corromper códigos-fonte honestos.

O Eng. Márcio Teixeira, especializado em software básico e microprogramação, e este autor escreveram um artigo (Teixeira, 2001) onde se mostra que é possível introduzir vícios que fraudem a apuração com a UE e que passem despercebidos pela fiscalização permitida aos partidos políticos, **por exemplo**, adulterando-se o sistema operacional ou as bibliotecas padrão dos compiladores.

Todas estas possibilidades levaram à proposta (Brunazo, 2000, item 5) de que sistemas informatizados de votação sejam classificados como **Sistemas de Alto Risco de Fraude**, pois pode-se identificar aqui os conceitos de **Potencial de Dano** elevado e **Probabilidade de Fraude** não desprezível. Esta proposta está em consonância com as de Peter G. Neumann, Lorrie Cranor e Rebecca Mercuri (op.cit) sobre a necessidade de critérios de avaliação especiais e mais rigorosos para sistemas informatizados de votação.

Conclui-se que todas estas possibilidades de ataques por adulteração do código tornam extremamente complexa a tarefa de qualificação das mais de 320 mil urnas que são carregadas em mais de 5600 cidades simultaneamente e **nem a total transparência dos programas pode conferir plena confiabilidade** ao sistema, o que sugere que outros **canais redundantes e independentes de controle e auditoria sejam adotados**.

7. Proposta - Conferência da Apuração

Em recente mensagem colocada na lista de debate E-lection (http5), Peter Neumann diz que:

"Se votos serão gravados e contados eletronicamente, algum meio de auditoria indescartável, inalterável e inevitável deve existir para tornar adulterações eletrônicas e acidentes impraticáveis".

É dentro desta linha de pensamento que em (Requião, 1999), (Brunazo, 1999) e (Teixeira, 2000) recomenda-se evoluir as UE brasileiras de MAD para a nova geração MAC, ou seja, dar às UE a capacidade de **recontagem dos votos e conferência da apuração** por meio da **impressão do voto**, o qual seria mostrado ao eleitor antes de ser depositado em uma urna lacrada para posterior conferência quando e se requerido. Em (Teixeira, 2000) e (Brunazo, 2000) são contestados os argumentos apresentados contra a impressão do voto.

Esta idéia de transformar MAD em MAC por meio do voto impresso tem surgido, também, nos EUA como proposto por Bruce Schneier, inventor dos métodos Blowfish e TwoFish de criptografia, em (Schneier, 2000) e por Peter Neumann e Rebecca Mercuri numa recente reportagem (http8) sobre a modernização das máquinas do Estado da Filadélfia em que consideram as atuais MAD ultrapassadas e inseguras. Mercuri afirma:

"Um sistema (eleitoral) melhor deveria casar tecnologia de computadores com o papel, sugerindo uma MAD/DRE que grave eletronicamente a escolha do eleitor e também crie uma cédula impressa mecanicamente legível. O eleitor poderia ver a cédula através de uma janela na impressora e aprová-la antes de ser depositada numa urna lacrada." - tradução do autor deste artigo

Um protótipo que atende exatamente as propostas destes autores brasileiros e americanos já foi construído pela empresa brasileira Bematech e foi apresentado no simpósio SSI'2000, no ITA. É uma impressora especial conectada à porta paralela da UE, que imprime o voto e o mostra ao eleitor através de um visor de vidro. O eleitor pode, então, confirmar ou cancelar o voto. O voto impresso é depois depositado automaticamente numa urna lacrada, sem contado manual do eleitor.

Em (Gerck, 2001) se considera que, no caso de diferença entre a apuração eletrônica e a do voto impresso, seria erro considerar este mais seguro *a priori*, mas a proposta (Requião, 1999) impõe que esta decisão seja tomada *a posteriori*, uma vez que o voto impresso e o virtual exigem técnicas de fraude que deixam rastros diferentes, os quais poderiam ser detectados por uma sindicância, não gerando, assim, uma situação de impasse.

Propomos, então, que o voto impresso seja usado como uma via alternativa utilizada para controle redundante sobre a apuração eletrônica.

REFERÊNCIAS

BRUNAZO Filho, Amílcar, *A Segurança do Voto na Urna Eletrônica Brasileira*. In: Simpósio de Segurança em Informática, 1999, São José dos Campos. *Anais...* São José dos Campos, Brasil: Instituto Tecnológico da Aeronáutica, **1999**. P.19-28. - http://www.comp.ita.cta.br/ssi99/ssi99int.zip

BRUNAZO Filho, Amílcar, *Avaliação da Segurança da Urna Eletrônica Brasileira*. In: Simpósio de Segurança em Informática, 2000, São José dos Campos. *Anais...* São José dos Campos, Brasil: Instituto Tecnológico da Aeronáutica, **2000**. – http://www.votoseguro.org/textos/SSI2000.htm

CAMARÃO, Paulo César Bhering. *O Voto Informatizado: Legitimidade Democrática*. São Paulo, Brasil: Empresa das Artes, **1997**.

CRANOR, Lorrie Faith. *Electronic Voting*. ACM Crossroads Student Magazine, Association for Computing Machinery, New York, NY, USA: April, **1996**. - http://www.acm.org/crossroads/xrds2-4/voting.html

GERCK, Edgardo. *Voting System Requirements*. The Bell Newsletter, San Raphael, CA, USA: January, **2001**, Vol. 2, nº 1. - http://www.thebell.net/papers/vote-req.pdf

FUJIOKA, A., OKAMOTO, T., e OHTA, K. *A practical secret voting scheme for large scale elections*. In: Advances in Cryptology - AUSCRYPT '92, Springer-Verlag, Berlin: **1993**, pp. 244-251.

HOFFMAN, Lance J.. *Internet Voting: Will it Spur or Corrupt Democracy?*. In: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions, April 4 - 7, **2000**, Toronto, ON Canada: P.219-223. - https://www.acm.org/pubs/citations/proceedings/cas/332186/p219-hoffman/

KITCAT, Jason. *Why Electronic Voting Software Should Be Free Software.* The Bell Newsletter, San Raphael, CA, USA: september **2000. -** http://thecouch.org/free/docs/wfs.html

MANESCHY, Oswaldo. *Palm Beach Versus Araçoiaba da Serra*. Jus Navegandi, Teresina, PI, Brasil: janeiro de **2001**. - http://www.jus.com.br/doutrina/urnael19.html

MERCURI, Rebecca. *Electronic Vote Tabulation Checks & Balances*, Ph.D. Dissertation, Philadelphia, PA, USA: School of Engineering and Applied Science, University of Pennsylvania, **2000**. - http://www.notablesoftware.com/Papers/thesdef.html

MINEIRO, Procópio. *Proconsult – Um Caso Exemplar*. Cadernos do Terceiro Mundo, Rio de Janeiro: Editora Terceiro Milênio, n. 219, p. 17, Abril/Maio **2000**. - http://www.votoseguro.org/noticias/cad3mundo1.htm

NEFF, C. Andrew. *Conducting a Universally Verifiable Electronic Election Using Homomorphic Encryption*: VoteHere Inc, November **2000**. - http://votehere.net/vh-content-v2.0/homomorphicsystemdescription.pdf

NEUMANN, Peter G.. *Security Criteria for Electronic Voting*, In: 16th National Computer Security Conference Baltimore, Maryland, USA: September 20-23, **1993**. - http://www.csl.sri.com/neumann/ncs93.html

PHILLIPS, Deborah M.. *Are We Ready for Internet Voting?*. Arlington, VA, USA: The Voting Integrity Project, **1999**. - http://www.voting-integrity.org/projects/votingtechnology/internetvoting/ivp_title.shtml

REQUIÃO, Roberto. *PLS 194/99 – Projeto de Lei do Senado*. Brasília: Senado do Brasil, **1999**. - http://www.senado.gov.br/web/senador/requiao/pls99.htm

SALTMAN, Roy G.. *Assessment of Computerized Voting in Brazil with Recommendations for Nations of the Region*. Brasília, Brasil: Tribunal Superior Eleitoral, outubro **1996**.

SHAMOS, Michael Ian. *Electronic Voting – Evaluating the Threat*. In: Third Conference on Computers, Freedom and Privacy, March 93, Anais… Burlingame, CA, USA: Computer Professionals for Social Responsibility, **1993**, P. 3.18 – 3.25. - http://www.cpsr.org/conferences/cfp93/shamos.html

SCHNEIER, Bruce. *Voting and Tecnology*. Crypto-Gram Newsletter, San Jose, California, USA: Counterpane Internet Security, Inc., December **2000**. - http://www.counterpane.com/crypto-gram-0012.html

TEIXEIRA, Márcio C.. *Avaliação da Necessidade de Modificações na Urna Eletrônica Brasileira*. Brasília, Brasil: Comissão de Constituição, Justiça e Cidadania do Senado Federal, setembro **2000.** - http://www.votoseguro.org/textos/marcio2.htm

TEIXEIRA, Márcio C., BRUNAZO F., A *Reflexões sobre Confiabilidade de Sistemas Eleitorais*. Belo Horizonte, Brasil: Fórum do Voto Eletrônico, janeiro **2001**. - http://www.votoseguro.org/textos/reflexoes.htm

THOMPSON, Ken. *Reflections on Trusting Trust.* Communication of the ACM, Association for Computing Machinery, Inc., Vol. 27, nº 8, august **1984**. P. 761-763. - http://www.acm.org/classics/sep95/

(http1) International Standard ISO/IEC 15.408: http://csrc.nist.gov/cc/ccv20/ccv2list.htm

(http2) SafeVote Inc.: http://www.safevote.com/

(http3) VoteHere.net: http://votehere.net/VH-Content-v2.0/default.htm

(http4) Message in E-lection News Group: http://www.egroups.com/message/e-lection/246

(http5) Message in E-lection News Group: http://www.egroups.com/message/e-lection/245

(http6) Reportagem na Folha de São Paulo, 15/10/2000: http://www.votoseguro.org/noticias/folha2.htm

(http7) Reportagem na Folha de São Paulo, 15/10/2000: http://www.votoseguro.org/noticias/folha4.htm

(http8) Reportagem no The Philadelphia Inquirer, 15/01/2001: http://inq.philly.com/content/inquirer/2001/01/15/front_page/MACHINE15.htm