O que é o voto eletrônico?

Beatriz Busaniche e Federico Heinz

Existem várias definições para o que é comumente chamado de “voto eletrônico”. Em um sentido amplo, o voto eletrônico é considerado como a incorporação de recursos computacionais em qualquer parte do processo eleitoral, seja no registro do cidadãos, na elaboração de mapas distritais, na logística eleitoral, no exercício do próprio voto, o escrutínio e a transmissão de resultados. No entanto, nesta introdução, consideraremos estritamente duas das áreas de sufrágio: a emissão do voto em si e a contagem de votos.

Em sentido estrito, chamaremos voto eletrônico aos mecanismos destinados a emitir e contar sufrágios em um único ato, através de um sistema de informática instalado e operando no mesmo local onde o eleitor atende para expressar sua vontade política. Então, entendemos por voto eletrônico cada sistema informatizado para o ato de emitir e contar os votos na mesa de voto, onde os cidadãos e as cidadãs entram em contato direito com os dispositivos eletrônicos. Consideramos o uso de computadores, urnas eletrônicas ou dispositivos similares para a emissão e contagem automatizado do sufrágio. Os mecanismos nos quais o computador não está diretamente envolvido no ato de votar, bem como aqueles que usam a informática exclusivamente para a automatização da contagem e a consolidação de resultados estão, portanto, expressamente fora de nosso foco.

Não existe uma maneira única de implementar o voto eletrônico, mas poderíamos dizer que há três tipos principais de sistemas a serem usados, que diferem não apenas em sua implementação, mas principalmente em seus riscos e benefícios. Os mecanismos mais freqüentemente identificados podem ser agrupados em três grandes grupos:

a) os sistemas de contagem automática de votos por meio de reconhecimento óptico das marcas feitas na cédula pelos cidadãos (sistemas que enfatizam o escrutínio eletrônico);

b) os sistemas de registro eletrônico direito (REDE, ou DRE, por sua sigla em inglês) comumente exemplificados com os chamados quiosques de votaçã ou urnas eletrônicas;

c) os sistemas de votação remota através da internet.[1]

Sistemas usados

a. Sistemas de contagem automática

Os primeiros sistemas desse tipo datam do século XIX, quando começaram a ser implementados na cidade de Nova York usando cartões perfurados. Atualmente, a maioria dos sistemas desse tipo baseia-se no reconhecimento ótico das marcas feitas pelo eleitor na cédula, seja diretamente ou através de uma máquina de marcação de cédulas. Entre 1994 e 2003, por exemplo, a Venezuela utilizou sistemas desse tipo, baseados em cédulas impressas em papel com um espaço preenchido pelo eleitor e, posteriormente contabilizadas por meio de um sistema de reconhecimento óptico de caracteres.

Em princípio, os sistemas de contagem automática resolvem o problema mais crítico da incorporação de tecnologia no voto: ao manter o princípio de que a vontade do eleitor é expressa em um pedaço de papel anônimo, ele dissocia o ato de votar (que deve ser não auditável) do ato de escrutínio (que deve ser auditável em todos os seus detalhes). Desta forma, é possível construir um sistema no qual todos os resultados em que a computação está envolvida podem ser auditados independentemente dos dispositivos usados e do próprio software, através do recurso simples de uma contagem manual.

Mesmo assim, a aplicabilidade desses mecanismos não pode ser tomada isoladamente, mas no contexto do sistema completo do qual fazem parte. É possível tomar muitas decisões em relação ao sistema como um todo que podem cancelar todas ou parte das vantagens do mecanismo.

Um elemento que não pode faltar na aplicação dos sistemas de contagem automática é a auditoria manual dos resultados gerados por uma parcela estatisticamente significativa das máquinas usadas, selecionadas aleatoriamente após o ato eleitoral. De outra forma, uma programação maliciosa do software de tabulação de votos poderia alterar os resultados sem ser detectada.

Estes sistemas perdem uma parte importante das suas vantagens quando a cédula não é marcada à mão pelo eleitor. As máquinas de marcação de cédulas re-introduzem muitos dos problemas associados com as máquinas de gravação direta no sistema. Enquanto elas permitem que o eleitor verifique se as marcas na cédula correspondem às suas escolhas, eles supõem um trabalho duplo para o eleitor (escolher, por um lado, controlar por outro), o que aumenta a probabilidade de que o eleitor não execute conscienciosamente o controle. Isso viabiliza o mesmo ataque que pode ser feito em máquinas de REDE: introduzir código que tente adulterar a intenção do eleitor, mas abandone a tentativa se o eleitor rejeita a cédula. Desta forma, os votos de todos os cidadãos que não sejam cuidadosos podem ser seqüestrados. O anonimato do voto também está em risco toda vez que a máquina de marcar cédulas poderia agregar, além das manchas legítimas, algumas que passam por “sujidade” mas que, na realidade, codificam informação que permite reconstruir a seqüência de emissão dos votos.

Um outro mecanismo que reduz a utilidade desses dispositivos é passar a cédula pelo scanner antes de introduzi-la na urna, em vez de fazerlo ao abri-la. Isso não só aumenta os custos –requer um scanner por mesa, enquanto o mesmo scanner pode ser usado para várias delas–, mas permite, potencialmente, registrar a seqüência na qual os votos foram expressos e, assim, reconstruir a relação de cada eleitor com seu voto.

Uma crítica comum a ese tipo de mecanismo aponta para a dificultade que ele apresenta no caso de eleições complexas, particularmente quando uma eleição é realizada para múltiplas posições nos níveis de distrito. Em uma eleição na qual, por exemplo, vereadores, prefeitos, legisladores provinciais,

legisladores nacionais, governadores e presidente devem ser eleitos, o tamanho da cédula torna difícil para o eleitor marcar todas as opções, assim como sua posterior leitura detalhada. No entanto, isso é mais uma crítica às eleições complexas do que ao próprio sistema de contagem automática: quanto mais complexa uma eleição, mais difícil votar e contar os votos. A "solução" para este problema, oferecida pelos sistemas REDE consiste, basicamente, em varrê-lo para baixo do tapete: como neles é impossível contar os votos à mão, disfarçam o vício de virtude, declarando que é uma tarefa "desnecessária".

Uma outra crítica comum a esses mecanismos, e igualmente imerecida, é a que desafia a facilidade com que o voto pode ser alterardo ou anulado pela adição de marcas por aqueles que realizam o escrutínio. Embora a viabilidade do ataque seja real, é exatamente igual a qualquer sistema baseado em papel, que por sua vez é melhor que o de qualquer sistema totalmente eletrônico: embora as cédulas podem ser alteradas, isso deve ser feito individualmente com cada cédula, e o impacto de uma pessoa corrupta é circunscrito às cédulas sob sua custódia. No sistema eletrônico, em contrapartida, uma única pessoa corrupta tem o potencial de infectar um grande número de máquinas, comprometendo até mesmo a integridade dos votos em massa, incluindo aqueles das seções eleitorais cujos promotores agem de boa fé.

b. Sistemas de registro eletrônico direto (REDE)

Os sistemas REDE ou DRE são os que mais correspondem ao imaginário popular das "urnas eletrônicas". Eles representam, além disso, o modelo preferido da maioria das empresas que participam desse mercado. As urnas eletrônicas usadas no Brasil, bem como em vários estados dos EUA ou nas últimas eleições na Venezuela, pertencem a esta classe.

Os sistemas REDE são caracterizados pelo registro simultâneo e a tabulação do voto através de um dispositivo informático, operado diretamente pelo eleitor através de un teclado, um comando especial ou uma ecrã. Ademais, alguns sistemas de REDE oferecem ajuda a pessoas com algum tipo de deficiência, por exemplo

através de uma interface de áudio para superar as dificuldades visuais. Ao contrário dos sistemas de contagem automática, em que o suporte fundamental da votação é a cédula marcada pelo cidadão, nas máquinas REDE o registro é feito diretamente na memória do dispositivo.

Muitos fornecedores de equipamento destacam o fato de permitir "separar" a eleção do papel como uma vantagem do sistema. Em geral, eles recomendam não usar a opção oferecida por alguns modelos de máquinas REDE para usar impressoras similares àquelas que trabalham dentro das caxas registradoras para gerar uma fita de auditoria, argumentando que "desnatura o voto eletrônico". Em qualquer caso, as máquinas REDE não usam o papel emitido para seus resultados, mas dependem enteiramente dos registros presentes em sua memória.

Os sistemas REDE podem ser configurados de tal forma que permitem ao usuário corrigir suas opções e até mesmo votar em branco, mas não permitem invalidar o voto ou cometer erros clássicos que resultam na anulação do voto.

Por outro lado, estes sistemas geralmente também são preferidos por aqueles que trabalham nas eleições, porque são os que mais trabalho economizam: não há cédulas para guardar, a contagem de votos é imediata e não há risco de uma nova contagem de votos jogam uma diferença com o anterior. A máquina sempre obterá o mesmo resultado, independentemente de se reflita a vontade de quem a usou para votar ou não.

Nessa preferência, torna-se evidente um ponto de tensão entre os interesses dos cidadãos (que precisam que o resultado reflete suas escolhas) e dos responsáveis por dirigi-lo (que querem terminar a tarefa o mais rápido e sem esforço possível, baixando o máximo de responsabilidade possível por eventuais erros ou atos de corrupção).

c. Sistemas de votação pela internet

Também conhecidos como sistemas de votação remota, estes são mecanismos para emitir o sufrágio desde um computador comum conectado à rede de redes, permitindo que os eleitores emitam sua

vontade de suas próprias casas, de pontos de acesso público, e até mesmo do estrangeiro. Existem variantes desses sistemas que permitem emitir o voto não apenas de um computador pessoal, mas eventualmente, também de um telefone celular ou de um sistema de televisão digital.

Um dos desafios mais sérios enfrentados por esse tipo de sistemas é a identificação do eleitor, essencial para assegurar várias propriedades importantes do mecanismo, como impedir alguém de votar mais de uma vez ou em nome de outra pessoa, ou pessoas que não estão habilitadas para fazer-lo. Este problema geralmente é resolvido por uma chave unívoca e pessoal, que pode incluir elementos de autenticação física, como a posse de uma cédula de identificação criptográfica ou um gerador de chaves pseudo-aleatórias.

Mesmo com os métodos de autenticação mais sofisticados, não é claro que seja possível conciliá-los com os requisitos de identificação exigidos por lei, que geralmente exigem a verificação de documentos de identidade pelas autoridades eleitorais. Um problema adicional associado à identificação é que estes sistemas exigem que a máquina que recebe o voto tenha conhecimento de quem lo está emitindo. Isso oferece um único ponto de ataque para aqueles que querem violar o segreto do voto: basta obter a informação armazenada no servidor do sistema de votação para descobrir como cada pessoa que o usou votou.

Os defensores desses sistemas destacam que eles se prestam a ser usados em lugares onde a participação em eleições não é obrigatória e a votação pelo correio é permitida. O argumento é sólido, no sentido de que é um sistema que pode ser usado em contextos em que a experiência mostra que o risco de fraude é baixo.

É interessante notar que existem experiências bem-sucedidas de usar a votação remota em certos âmbitos específicos, particularmente naqueles em que os participantes têm um alto grau de familiaridade e acesso a recursos informáticos e a exigência de anonimato está ausente. O projeto Debian, por

exemplo, um projeto de desenvolvimento de software comunitário composto por pessoas de todo o mundo que não têm a oportunidade de se reunir físicamente para votar, utiliza a votação remota como uma ferramenta cotidiana, com excelentes resultados. O sistema é robusto, justo e difícil de enganar, mas só funciona graças ao fato de que o voto não é segredo.

Principais problemas detectados em sistemas de votação eletrônica

Estes sistemas geralmente vêm com fortes afirmações sobre suas virtudes, como maior transparência do ato eleitoral, eliminação do clientelismo político, velocidade e infalibilidade da contagem, menor custo de cada eleição e maior participação do cidadão.

Lamentavelmente, essas declarações categóricas não são acompanhadas de dados sólidos para apoiá-las, e algumas empresas fornecedoras investem um esforço não negligenciável para evitar que sejam verificadas por terceiros independentes, como foi o caso da Sequoia Systems em 2008, que tentou impedir uma auditoria independente de segurança comissionada pelo Estado de New Jersey, argumentando que sua execução violaria os termos de uso do software que controla as urnas.

De fato, nenhuma dessas declarações suporta uma análise profunda e, embora algumas delas possam ser verdadeiras para alguns casos particulares, a experiência internacional mostra que, na realidade, elas estão longe de refletir o verdadeiro desempenho das urnas eletrônicas. Vamos parar, então, nessas afirmações categóricas em torno do voto eletrônico.

1. A transparência

A afirmação de que as urnas eletrônicas contribuem para a transparência da eleição é provavelmente a mais arriscada. É difícil entender como um processo opaco se tornaria mais transparente pelo recurso da adição de uma “caixa preta”. Longe de contribuir para a transparência, a urna eletrônica dificulta a capacidade da maioria dos cidadãos de supervisar a eleição.

Todas as pessoas sabem como verificar, só de olhar, que uma urna está vazia ou que um selo de segurança está intacto, e o sistema

educacional tem como objetivo garantir que todas as pessoas possam ler, escrever e contar. Mas essas habilidades são inúteis quando se trata de ver o que acontece “dentro” de uma urna eletrônica: a inspeção ocular não serve para ver se está vazia, mas é necessário usar um programa projetado para isso, que imprime um bilhete que diz “sim, estou vazia”. A questão é: podemos acreditar nele?

Quando a urna imprime os resultados, ela os obtém de operar em seus registros internos, armazenados em mídia magnética que os promotores não podem ler sozinhos. A única “comprovação” possível que a urna está efetivamente vazia, ou que os totais estejam corretos, é repetir a operação, que previsivelmente sempre dará o mesmo resultado. Mesmo se confiamos que o programa da urna está correto, o promotor médio não possui o conhecimento e as ferramentas necessários para verificar se o programa que está instalado na urna foi adulterado ou não.

Mesmo um promotor com amplo conhecimento de programação e eletrônica digital, equipado com ferramentas especializadas, provavelmente demoraria dias para verificar, com certo grau de confiança, que a urna estava efetivamente “no zero”, enquanto fazê-lo com o mesmo grau em que pode fazer-se inspecionando o interior de uma urna de papelão é efetivamente impraticável. É um problema da mesma complexidade que a construção de programas de computador livres de erros, algo que o estado da arte ainda não nos permite. Para pior, as ações que este hipotético auditor especializado deve realizar são muito mais invasivas que as necessárias para adulterar o funcionamento da urna, de modo que, supondo que ele nos diga que a urna está “limpa”, não só poderá provar isso alguém que não é especializado de forma semelhante, mas não temos como saber se o que ele fez, na verdade, foi verificar ou subvertê-lo.

Este é um problema fundamental das urnas eletrônicas: enquanto a verificação de sua confiabilidade depende exclusivamente de verificar se “funciona bem”, a tarefa de seu fiscalização está necessariamente nas mãos de uma elite tecnológica, para a qual o resto da população não tem outra hipótese senão acreditar nele.

Para corromper a fiscalização de uma eleição baseada em papel, é necessário ter promotores corruptos em um grande número de mesas, mas no caso das urnas eletrônicas é suficiente subornar ou extorquir um pequeno grupo de pessoas facilmente identificáveis.

Essas dificuldades são freqüentemente desconsideradas, argumentando que eleições controladas de testes podem ser feitas para ver como a urna se comporta, e salientando que essas urnas foram usadas em muitos lugares sem problemas. Infelizmente, esse argumento ignora o fato de que é muito fácil programar a máquina para que ela não se comporte da mesma forma durante os testes como durante a eleição, e que essa experiência mostra que na maioria das eleições, a necessidade de atualizar o software (seja o mesmo software da urna ou seu sistema operacional) leva ao programa que é executado durante a eleição pode não ser o mesmo que foi usado durante os testes.

Quanto ao resto, a afirmação de que essas urnas foram usadas sem problemas é muito arriscada: não sabemos se houve problemas ou não, precisamente porque a opacidade do mecanismo não nos permite verificá-lo adequadamente. É perfeitamente possível que nessas eleições tenham ocorrido enormes problemas, sem que ninguém tenha conseguido comprová-lo, e é precisamente esse o cenário que as urnas eletrônicas facilitam. De fato, há eleições como as dos Estados Unidos em 2004, em que as diferenças entre as sondagens e os finais sugerem fortemente que as urnas deram resultados incorretos.

2. O fim do clientelismo

O clientelismo político é um problema social, econômico e educativo que não é resolvido com a tecnologia. Para que a "compra de votos" funcione, é necessário ter um mecanismo que permita ao comprador um grau de confiança importante de que o eleitor votará efetivamente no candidato que ele prometeu votar. Nas eleições em papel, isso pode ser feito através do chamado "voto em cadeia", um mecanismo que alguns sistemas de votação eletrônica efetivamente impossibilitam.

No entanto, pensar que o voto em cadeia e o clientelismo são a mesmo coisa é um erro: o voto em cadeia é apenas um mecanismo para quebrar o segredo do voto. Não é o único, e as urnas eletrônicas oferecem mecanismos alternativos potencialmente muito mais eficazes. Isso se deve à natureza fundamentalmente diferente das urnas eletrônicas. Por exemplo, enquanto as urnas normais são contentores passivos de informação, os circuitos da urna eletrônica emitem radiação electromagnética. Experimentos realizados na Holanda mostraram que essas emissões tornaram possível detectar por quem uma pessoa votou a uma distância de 25 metros, usando apenas dispositivos comercialmente disponíveis.

Por exemplo, no estado de Ohio foi descoberto, dois anos depois de usá-las, uma séria falha nas urnas eletrônicas que permite violar el segredo do voto após as eleições: os relatórios emitidos pela urna no final da contagem permitem reconstruir a relação entre voto e eleitor. Este caso é particularmente grave porque ilustra um aspecto muitas vezes ignorado no cálculo do risco quando se usa uma urna eletrônica: o fato de não conhecermos vulnerabilidades nas urnas não significa que elas não existam, ou que ninguém as conheça. Qualquer um que estivesse ciente dessa vulnerabilidade poderia ter organizado uma compra ou extorsão massiva de votos que seria indetectável e exigiria um esforço logístico muito menor do que o voto em cadeia.

3. A velocidade na contagem

Uma das poucas vantagens promovidas que podem ser verificáveis é a velocidade na contagem. De fato, quando tudo corre bem, os resultados podem ser imediatos. O problema surge quando avaliamos o impacto potencial das diferentes coisas que podem dar errado. Enquanto na urna de papel, a influência de um inconveniente é geralmente proporcional à magnitude disto, nas urnas eletrônicas um problema muito pequeno pode ter conseqüências muito sérias. Isso leva ao fato de que, se os resultados da urna eletrônica não forem imediatos, geralmente não podem ser obtidos. Geralmente, não há meio termo.

Em 16 de dezembro de 2007, por exemplo, quatro urnas eletrônicas da firma Altec Sociedad del Estado (Río Negro) foram

utilizadas na cidade de Las Grutas, na Argentina. Após o dia da eleição, uma dessas urnas mostrou um resultado surpreendente: 0 votos. Felizmente neste caso, as urnas haviam sido gravadas no papel, porque o registro digital estava completamente perdido, mas mesmo assim o escrutínio levou horas, porque os votos impressos em uma tira de papel eram muito mais difíceis de identificar do que as cédulas originais. A única explicação da empresa fornecedora da urna foi que “alguém deve ter sacudido a urna”.

Do mesmo modo, há casos em que uma falha técnica em uma urna eletrônica fez com que a urna contasse milhares de votos em mesas nas quais só votaram centenas de pessoas, ou o caso de Nova Jersey, em que os resultados foram imediatos, mas o total de votos expressos não coincidia com a soma dos votos expressos por partido. Pode-se dizer que esse resultado é imediato quando na verdade é evidentemente incorreto?

A velocidade, sem confiança ou segurança, não serve muito em um processo eleitoral. Esta é um área em que a eficácia (fazê-lo bem) deve ter precedência sobre a eficiência (fazê-lo rápido).

4. A economia

A ideia de que usar urnas eletrônicas para economizar dinheiro nos comícios foi refutada por auditores independentes que a testaram. No estado de Maryland, por exemplo, entre 2002 e 2003, 19 mil máquinas com ecrã foram compradas à empresa Diebold. Para completar a compra, o Estado fez um empŕestimo de 67 milhões de dólares, 44 dos quais foram para os cofres da empresa para a compra e manutenção das urnas. Antes de incorporar esses dispositivos, Maryland usava um sistema de digitalização óptica.

De acordo com o relatório da organização *Save Our Votes*, publicado em fevereiro de 2008,[2] a mudança de tecnológica implicou um aumento médio de 179% no custo total por eleitor. Em um dos municípios, o aumento foi de 866%. A propósito, as máquinas Diebold ainda não foram pagas e já devem ser renovadas. O estado de Maryland está considerando retornar ao sistema de digitalização óptica.

5. A participação cidadã

Uma questão crítica ao avaliar a implementação do voto eletrônico é a participação cidadã. Nossas democracias modernas são atingidas pelo descrédito das classes dominantes e pela falta de confiança nos sistemas políticos. A aura de modernidade concedida pelo voto eletrônico parece ser a panacéia para entusiasmar os eleitores e encorajar a participação nas eleições.

No entanto, é importante ressaltar que a incorporação de urnas eletrônicas tem efeitos claramente contrários ao objetivo de melhorar a participação cidadã. Sem ir mais longe, as pessoas com pouca afinidade com os sistemas de computadores serão as primeiras excluídas: idosos ou pessoas de recursos limitados, pessoas com dificuldades visuais ou com muito baixo nível educativo que hoje não necessitam de mais preparação para escolher uma cédula, colocá-la em uma urna e emitir sua vontade política, serão confrontados com um sistema muito mais complexo para votar.

Mas este não é o único inconveniente. Talvez o maior problema seja que aqueles que auditam hoje as eleições em nosso nome (professores da escola, funcionários públicos, promotores de partidos políticos) não poderão auditar de maneira eficaz um sistema dessa natureza. Somente pessoas altamente qualificadas em engenharia de software, eletrônica e hardware poderão entender o funcionamento desses sistemas. Mesmo pessoal qualificado em segurança de sistemas de informação é incapaz de avaliar, validar e corroborar o correto funcionamento das urnas eletrônicas. Estes mesmos especialistas dificilmente ousam assinar uma certificação de segurança das urnas porque não existe um método formal de validação que os endosse.

Assim, uma participão real e tangível da cidadania será reduzida à confiança cega em um pequeno número de promotores informáticos que, mesmo tendo amplo conhecimento do assunto, não podem certificar a validade de um resultado em que todos os outros terão que confiar. Aqueles de nós que temos a vontade política de exercer nosso direito de auditoria nos veremos limitados devido à falta de conhecimento técnico, e teremos que

deixar a participação real para uma pequena elite de técnicos autorizados.

Embora não existem sistemas perfeitos, a diferença no impacto é substancial. Uma mesa de votação tradicional pode registrar inconveniências e ser cancelada. O impacto nos resultados geraies será mínimo. No entanto, um erro mínimo em um sistema de votação eletrônica pode alterar o resultado de uma eleição simultaneamente em um grande número de mesas.

6. Outros problemas gerais

Vale a pena agregar que, na grande maioria dos casos, os fornecedores de urnas eletrônicas são empresas privadas cuja composição acionária deveríamos conhecer detalhadamente antes de confiar-lhes um processo público e cidadão como a emissão do voto. Quais serão os mecanismos para auditar às empresas fornecedoras? Como saberemos quais são as suas conexões políticas e seus interesses em cada eleição? Estamos dispostos a privatizar um processo cidadão como o ato de votar?

Essas perguntas surgem à luz de escândalos nos EUA onde, por exemplo, um dos principais acionistas de uma das empresas fornecedoras de urnas (ES&S) se revelou um senador republicano com interesses óbvios e marcantes no resultado eleitoral.[3]

Não são poucos os inconvenientes que aparecem ao avaliar a automatização da emissão do voto. No entanto, há muito pouco que é discutido e certamente puco é o conhecimento sobre eles. O ato de votar é importante o suficiente para lidarmos com essa questão, e nos preocupamos com as incorporações acríticas de tecnologia que, longe de melhorar nossas democracias, são ameaças ao direito essencial da cidadania de votar em condições de sigilo, transparência e segurança.

Notas

[1] Tula, María Inés (coord.). “Voto Eletrônico. Entre votos e máquinas. As novas tecnologias nos processos eleitorais”, Buenos Aires, Ariel Ciencia Política - Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (cippec), 2005.

[2] “Cost Analysis of Maryland’s Electronic Voting System”, fevereiro de 2008. Disponível em http://www.saveourvotes.org/reports/2008/08-costs-mdvotingsys-tem.pdf

[3] Harris, Bev. “Senator Hagel Admits Owning Voting Machine Company”, Scoop, 31/01/2003. Disponível em: http://www.scoop.co.nz/stories/HL0301/S00166.htm