



BELO
HORIZONTE

XIV SIMPÓSIO BRASILEIRO EM SEGURANÇA DE INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS

► ANAIS

SBC- SOCIEDADE BRASILEIRA DE COMPUTAÇÃO



SBSeg 2014 - Belo Horizonte, MG

XIV Simpósio Brasileiro em Segurança da Informação
e de Sistemas Computacionais

de 3 a 6 de Novembro de 2014 – Belo Horizonte, MG

ANAIIS

Editora

Sociedade Brasileira de Computação – SBC

Organizadores

Jeroen van de Graaf, UFMG
José Marcos Nogueira, UFMG
Leonardo Barbosa Oliveira, UFMG

Realização

Universidade Federal de Minas Gerais – UFMG

Promoção

Sociedade Brasileira de Computação – SBC

Copyright © 2014 Sociedade Brasileira de Computação
Todos os direitos reservados

Edição: Vitor Mendes Paisante

Dados Internacionais de Catalogação na Publicação

S612 Simpósio Brasileiro em Segurança da Informação e de
 Sistemas Computacionais (14. : 2014 : Belo
 Horizonte)
 Anais / XIV Simpósio Brasileiro de Segurança da
 Informação e de Sistemas Computacionais ; coordenação:
 Jeroen van de Graaf, José Marcos Nogueira, Leonardo
 Barbosa Oliveira — Porto Alegre: Sociedade Brasileira de
 Computação, 2014.
 xviii, 753 p. il. 23 cm.

ISSN: 2176-0063

1. Ciência da computação. 2. Informática. 3. Segurança
da informação. 4. Segurança de sistemas. I. Graaf,
Jeroen. II. Nogueira, José. III. Oliveira, Leonardo. IV.
Título.

CDU 004(063)

Modelo Brasileiro de Votação Mecatrônica Independente de Software ou Votação Mecatrônica

Ronaldo Moises Nadaf

nadaf@nadaf.net

Resumo. *O artigo sugere a criação do “Modelo Brasileiro de Votação Mecatrônica Independente de Software” ou “Votação Mecatrônica,” que propõe pesquisas e o desenvolvimento de novos equipamentos para um sistema automatizado de identificação do eleitor, coleta e apuração da votação, e de softwares capazes de gerar dois ou mais registros diferentes e auditáveis do voto digital e impresso.*

1.Introdução

Em 2009, o Congresso Nacional aprovou, e a Presidência da República sancionou, a lei 12.034 que previa, no art. 5º, a implantação do voto impresso e separação do terminal do eleitor da máquina de votar [1]. O objetivo era garantir a transparência, permitindo a auditoria dos votos e a implantação do conceito de sistema de votação independente de software[2], e também evitar que uma falha ou um erro viesse associar o voto coletado ao eleitor identificado no terminal.

Em 2011, o Ministério Público Federal moveu a ação de inconstitucionalidade nº 4543 contra o artigo 5º da lei e, em novembro de 2013, o Supremo Tribunal Federal acatou o pedido e declarou o artigo inconstitucional. A decisão, embasada num suposto reconhecimento mundial do sistema em uso, não levou em consideração pareceres técnicos e jurídicos emitidos por diferentes partes da ação [3].

A Suprema Corte também deixou de lado os resultados de um teste realizado pela própria autoridade eleitoral em 2012, quando uma equipe de cientistas revelou que o sistema brasileiro de votação é falho, defasado e carece de melhorias[4].

O objetivo desse artigo é apresentar uma proposta de evolução tecnológica do modelo atual de votação totalmente eletrônico para um modelo mecatrônico, ou seja, sugerir estudos para o desenvolvimento de dois novos equipamentos eletromecânicos que permitam a identificação biométrica do eleitor sem associa-lo à sua escolha, a impressão, a coleta, a apuração e armazenagem dos votos de maneira segura, operados por softwares distintos, capazes de gerar dois ou mais registros diferentes de voto, sendo um digital e outro impresso, e de realizar a auditoria do sufrágio sem que exista qualquer interferência humana no processo, onde apenas e tão o somente o eleitor tenha contato com o registro físico do voto.

Os modelos virtuais das máquinas aqui propostas, suas dimensões físicas e a cédula do voto, foi desenvolvida através de experiências realizadas em um ambiente

construído no software 3d Max Studio, onde os conceitos aqui descritos estão sendo colocados em prática em tamanho real e continuam em evolução.

2. Estrutura do Modelo de Votação Mecatrônica

No contexto tecnológico proposto, a primeira mudança antecede a votação, onde o próprio eleitor realiza a identificação biométrica das impressões digitais dos dedos e o reconhecimento da face. Em seguida vota em um teclado ou tela sensível ao toque, visualiza a foto do candidato e confirma o voto como já de costume.

A segunda mudança está na inclusão da “Mesa Receptora Independente”, que serve de suporte para a Urna Eletrônica (ou tablet) e os leitores biométricos, além de realizar a impressão, a coleta ou a trituração das cédulas de votação.



Figura 1 - À esquerda, Mesa Receptora Independente e à direita, Máquina Apuradora

A Mesa Receptora tem acopladas duas caixas, uma chamada de “Urna Independente de *Software*”, onde as cédulas válidas são armazenadas aleatoriamente; e outra, chamada de “Urna Ecológica”, onde as cédulas inválidas trituradas são armazenadas em forma de resíduo. Após o encerramento da votação, a Urna Independente é retirada da mesa e inserida na “Máquina Apuradora de votos”, um segundo equipamento que realiza o escrutínio e auditoria das cédulas, que confirmará o resultado apurado pela votação eletrônica.

Abaixo estão relacionados todos os equipamentos que compõem o modelo proposto:

1. Leitores biométricos das impressões digitais e de reconhecimento da face;
2. Cédula de Segurança em papel com três registros do voto do eleitor;
3. Dispositivo de registro digital do voto, que pode ser um tablet, notebook ou a Urna Eletrônica brasileira;
4. Mesa Receptora Independente, dispositivo que realiza a impressão, verificação, coleta ou fragmentação do voto em papel;
5. Máquina apuradora de votos para escrutínio e auditoria das cédulas de segurança.

2.1 Identificadores Biométricos do Eleitor

A Biometria já é testada desde 2010 pela Justiça Eleitoral brasileira. O Tribunal Superior Eleitoral vem promovendo o cadastramento biométrico do eleitorado em todo o Brasil, capturando suas características físicas, como a impressão digital dos dez dedos e a fotografia da face, possibilitando que essas informações sejam utilizadas pelos leitores biométricos instalados nos equipamentos de votação.



Figura 2 - Mesa Receptora e Leitores Biométricos

Na votação mecatrônica é desnecessária a figura do mesário, pois o modelo proposto é projetado para ser acionado pelo próprio eleitor e permitir o acesso à tela de votação somente após identificação do mesmo, realizada através de comparação dos dados coletados no cadastramento biométrico aos dados capturados por dois leitores, um no formato de mão (item II), para ler as impressões digitais de quatro dedos e outro, uma câmera que lê os traços da face (item I).

Com o único objetivo de automatizar o acesso ao sistema de votação, os equipamentos de votação são acoplados em um mesmo conjunto físico, cujo software de identificação biométrica, comunica o início e o término da operação ao software de votação, trocando apenas informações simples entre si, sem associar o eleitor ao voto.

Além disso, os sistemas de informática responsáveis pelo registro do voto e pela identificação do eleitor são programados separadamente e em código aberto (*Software Livre*), com total possibilidade de auditoria por equipes especializadas, reduzindo a possibilidade de fraudes, falhas ou registros que quebre o direito constitucional ao sigilo do voto e o associe ao eleitor.

A câmera digital do equipamento de votação (item I) será também utilizada com a finalidade de garantir a segurança do sigilo do voto e dificultar a retirada da cédula do ambiente de votação. Dessa forma, após realizar a identificação da face do eleitor, a câmera altera seu estado de funcionamento de um simples equipamento coletor de imagem e passa a funcionar como um sensor de presença.

O sensor de presença será responsável por garantir o sigilo da tela onde o eleitor lançará os dados dos seus candidatos, evitando que o programa de coleta de votos funcione quando for detectada a presença de mais de uma pessoa na cabina de votação.

O sensor evitará também que o eleitor deixe a cabine de votação após a impressão da cédula, ou seja, se o sistema perceber que o eleitor afastou-se da cabina de votação após a impressão da cédula, a mesa independente emitirá um sinal sonoro de alerta para que os fiscais das eleições verifiquem o motivo que levou o eleitor a interromper o procedimento do voto, garantindo o sigilo e evitando que o voto impresso saia do ambiente de votação.

2.2 Cédula de Segurança do Voto Independente

A cédula de Segurança é um papel oficial e padronizado medindo 22x9cm sensível à impressão térmica, especialmente desenvolvida para o eleitor manifestar a sua intenção de voto em eleições e/ou plebiscitos.

No Brasil, assim como as cédulas de dinheiro, ela pode conter elementos de segurança propostas pela Casa da Moeda que dificultem a adulteração ou reprodução da mesma.

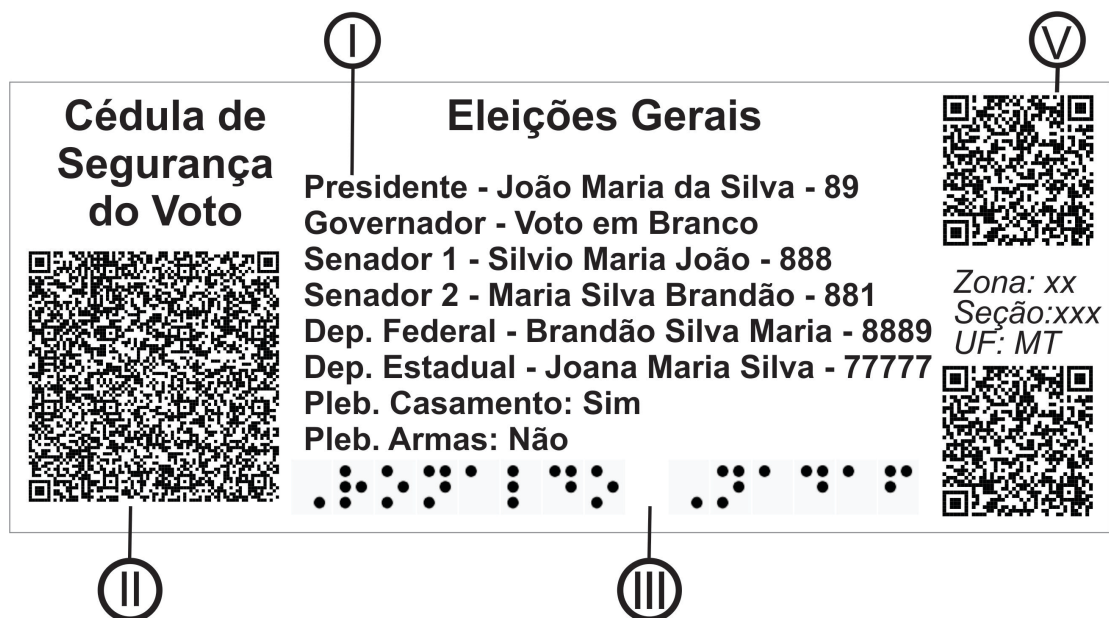


Figura 3 - Cédula de Segurança do Voto Mecatrônica

A cédula de segurança tem a característica de abrigar três registros impressos, sendo um em texto, outro em código de barras bidimensional e outro em código Braille.

Enquanto a norma norte-americana para o voto eletrônico naquele país sugere a necessidade de se gerar no mínimo dois registros [5], o modelo aqui proposto produz quatro registros do voto do eleitor, gerados por processos digitais distintos e auditáveis:

- I - Um registro textual contendo o cargo e o respectivo nome e o número do candidato, gerado pela urna eletrônica após a confirmação do eleitor;
- II - O segundo em código de barras bidimensional, invólucro gráfico com a dimensão de (5x5cm), localizado no canto direito da cédula, que armazena todas as informações do voto e de segurança do registro em formato XML, protegido

por assinaturas digitais de criptografia assimétricas geradas por chaves privadas institucionais instaladas nas “Mesas Receptoras Independentes”.

III - Um terceiro registro na linguagem Braile, gerado por outro sistema, impresso com tinta especial em alto relevo ou impressora Braile, que garante a acessibilidade ao eleitor deficiente visual,

IV - E o quarto registro utilizado atualmente, o totalmente digital, gerado pela urna eletrônica na conclusão da votação.

V – Registros de assinaturas digitais do voto em texto gerado tanto pela entidade administradora do processo eleitoral quanto por outras entidades fiscalizadoras (3x3cm).

Nesse modelo, o voto codificado em barras bidimensional pode ser auditado pelo eleitor apenas aproximando o maior código de barras impresso na Cédula de Segurança à câmera embutida em um *tablet*, que terão softwares que vão decodificar o código bidimensional e verificar a assinatura digital institucional através da chave pública de um ou mais participantes do processo de segurança criptográfica do voto, garantindo que, além do texto com os nomes dos candidatos, outro registro no papel comprove a integridade do registro de intenção de voto.

Em testes práticos, foi possível perceber que o código de barras maior tem a capacidade de armazenar, além das informações do voto em formato XML, múltiplas assinaturas digitais. Já os códigos de barras menores podem armazenar a mesma quantidade de informações que o maior, o que possibilita a existência de mais registros do voto assinados, e com impressão bidimensional, gerados por processos digitais distintos.

2.3 Dispositivo de Registro Digital do Voto – DRE

As máquinas de votar utilizadas em todo mundo são computadores adaptados para receber o voto. Nesse sentido, o modelo é idealizado para utilizar qualquer computador ou *tablet* oferecido pelo mercado, compatível com os softwares livres a serem desenvolvidos por um consórcio de universidades brasileiras de ciências da computação, e que preencha os requisitos técnicos para os procedimentos de identificação biométrica do eleitor, impressão e validação de cédulas de segurança do voto.



Figura 4 - À esquerda, Mesa Receptora com DRE Tablet e à direita, DRE Urna Eletrônica

Outro detalhe importante é a inclusão de tela sensível ao toque, que possibilita a utilização de um software que permite ao eleitor analfabeto posicionar o dedo indicador sobre a foto do candidato e confirmar o voto. Além do teclado reaproveitado da urna eletrônica, já adaptado com códigos Braille, mantendo a mesma sistemática de votação para os eleitores deficientes visuais.

Cabe salientar que a urna eletrônica brasileira hoje em uso possui interfaces USB que podem ser conectadas a mesa receptora, e adaptada para uma fase de teste em um processo de transição para o modelo aqui idealizado [7].

2.4 Mesa Receptora Independente

A “Mesa Receptora Independente” é um equipamento com três interfaces de interação que se comunicam via USB com os sistemas eleitorais instalados nos computadores que coletam o voto digital (DRE), transmitindo comandos eletrônicos quando concluídas as tarefas de impressão, coleta ou fragmentação do voto impresso. Ela ainda acopla os leitores biométricos, a urna independente e a urna ecológica.



Figura 5 - Interfaces da Mesa Receptora

I - Interface Impressora: É de onde sai a cédula de segurança já cortada, o “Comprovante de Comparecimento”, a “Zerésima” e o “Boletim de Urna”.

II - Interface Coletora: Confirma a procedência através das assinaturas digitais inseridas nos códigos de barras da cédula, que é “sugada” pelo dispositivo mecânico e armazenada aleatoriamente na “Urna Independente”. Concluída a operação, é emitido um sinal de autorização para a gravação e assinatura do voto digital lançado parcialmente no computador que coletou o voto.

Essa tecnologia é semelhante à utilizada nos terminais de cancelas eletrônicas para controle de bilhetes na saída de estacionamentos, que identificam o código de barras impresso do ticket entregue na entrada, comprovam a quitação, recolhem o bilhete de papel e liberam a cancela para saída.

III – Interface fragmentadora: Verifica a assinatura digital inclusa no código de barras da mesma forma que a interface coletora, confirmando a procedência, a cédula é sugada e triturada por dispositivo mecânico, e lançada em uma gaveta de armazenagem de resíduos de papel conectada a mesa receptora denominada “Urna

Ecológica”, evitando que o voto rejeitado venha contaminar o processo de escrutínio ou de auditoria da eleição. Concluída a operação, um sinal é enviado para que o software no computador que coletou o voto reinicie o processo de votação, cancelando o voto digital lançado parcialmente.



Figura 6 - Urna Independente retirada da Mesa Receptora

Para ampliar a segurança física das cédulas coletadas e armazenadas, existe uma mecânica que automatiza o lacre com tecnologia de radio frequência (RFID) da caixa coletora, acionado no final da votação, quando a “Urna Independente” será então sacada da mesa de votação e transportada para o ambiente de apuração e totalização dos votos, evitando o manuseio humano e mantendo a urna auditada contra tentativas de violação.

Importante ressaltar que, com a impressão do comprovante de comparecimento do eleitor pela própria máquina de votação, eliminam-se também os gastos atuais com a impressão e verificação dos cadernos de votação utilizados para o controle de acesso do eleitor à urna.

2.5 Máquina Apuradora

A máquina de escrutínio e auditoria é projetada para receber as cédulas de segurança resultantes da votação e armazenadas na “Urna Independente”. Sua primeira função é verificar a inviolabilidade do lacre rádio frequência da caixa coletora. Confirmada a auditoria física da armazenagem, os votos são recolhidos e encaminhados para o dispositivo de leitor ótico do voto, que captura as informações do registro em código de barras e as comparam com o voto em texto lido através de tecnologia OCR.

Se o lacre da urna apresentar indícios de violação, o equipamento emite um aviso sonoro e em texto no monitor e a urna é submetida à comissão apuradora, que decide sobre o prosseguimento de sua apuração.



Figura 7 – À esquerda, Máquina Apuradora, Nos detalhes, dispositivos embaladores e cédulas lacradas

Aprovado na auditoria, o voto da cédula é então contabilizado eletronicamente e esta é enviada para um espaço onde, junto com as demais cédulas, são armazenadas e, concluída a apuração total dos votos daquela seção eleitoral, serão lacradas com plástico formando um bloco de papel que recebe uma etiqueta de rádio frequência, concluindo assim o processo de apuração eletrônica das cédulas, produzindo como resultado relatórios de apuração da seção, impressos em texto e código de barras, ou relatórios de erros na auditoria das cédulas.

Já as cédulas provenientes da auditoria manual são apuradas em outra interface da máquina. O procedimento de escrutínio é sempre iniciado após identificada a relação entre a seção eleitoral e a etiqueta RFID, que resultam relatórios e um bloco de Cédulas de Segurança com um novo identificador RFID, ou seja, um ciclo de auditoria e contagem eletrônica que pode ser controlado por relatórios que vinculam a operação de escrutínio a uma identificação RFID.



Figura 8 - Cédulas Lacradas e Controladas por Tecnologia RFID

Para efeito de segurança, a máquina não possui nenhum dispositivo de entrada, além do disco que armazena os softwares livres que controlam os equipamentos de

interpretação, auditoria e contabilidade dos votos impressos, evitando assim qualquer interferência humana ao processo de auditoria.

O modelo deve ser amparado por leis que protejam o novo registro físico do voto. O ideal é que o acesso humano às cédulas de segurança lacradas, e a contagem manual cédula por cédula, só seja permitida após algumas recontagens eletrônicas, realizadas por máquinas apuradoras diferentes ou após a constatação de inconsistências nos registros do voto impresso e/ou decisão judicial.

Nesse sentido, evita-se uma nova forma de “voto de cabresto pós-moderno”, onde a correlação entre os candidatos escolhidos e expostos nas cédulas impressas serve como instrumento de coação utilizado por candidatos com má fé, pressionando eleitores com alegação de que este voto impresso poderá ser rastreado através de uma auditoria manual das cédulas de segurança.

Comprovada a necessidade através de decisão judicial de uma auditoria manual das cédulas impressas de uma seção, o primeiro escrutínio dos votos impressos será realizado por uma junta apuradora formada por deficientes visuais, que farão a leitura dos códigos Braile impressos na cédula, lançando-os em um sistema de tabulação próprio, chegando-se a totalização do resultado daquela seção.

Persistindo os pedidos para acesso às cédulas, uma segunda apuração manual, através de leitura do texto e/ou do código em barras, poderá ser realizada pelo autor do pedido sob a fiscalização do adversário, sendo obrigatório um terceiro escrutínio manual, a ser feito pelo adversário, sob a fiscalização do autor do pedido de auditoria manual dos votos.

3. Roteiro de Votação

O modelo de votação aqui concebido deve garantir a acessibilidade de todos os eleitores, inclusive os deficientes físicos, visuais e analfabetos. No caso dos deficientes físicos, anões ou pessoas mais baixas, a mesa é adaptada à altura do eleitor através de alavancas simples. No caso de deficientes visuais, os teclados que podem ser reaproveitados das urnas eletrônicas possuem linguagem Braile e a mesa uma impressora braile, tornando todos os métodos de lançamento e verificação do voto acessível.

Já no caso de eleitores analfabetos é possível visualizar a foto do candidato e escolher através da tela sensível ao toque, o que não altera é a possibilidade dele ler o nome do candidato. Vale ressaltar que todas as máquinas possuirão fones de ouvidos para possibilitar que qualquer eleitor ouça o voto, além de um leitor ótico na interface trituradora que reconhece os santinhos, que também ganham um código em barras bidimensional, lendo-os digitalmente e depois dando destino ecológico através da trituração.

No processo de votação observa-se a seguinte rotina, que pode ser orientada ao eleitor através de um fone de ouvido:

- a) A abertura da votação é autorizada por chaves criptográficas em código de barras bidimensional, inseridas na Mesa de Receptora pelos fiscais designados pela entidade administradora.
- b) O eleitor posiciona a mão no dispositivo de identificação biométrica e faz o reconhecimento das impressões digitais. A Mesa Receptora envia uma solicitação de autorização de voto assinada digitalmente para o sistema eletrônico de votação.
- c) O eleitor se posiciona em frente à câmera do computador e realiza o processo de reconhecimento biométrico da face.
- d) Em caso de falso-negativo, quando não há reconhecimento biométrico do eleitor, este deve solicitar a autorização aos fiscais, que verificam a identidade e autorizam a votação. Então é feita uma fotografia da face do eleitor, a coleta das impressões digitais dos dez dedos. Em seguida é liberada a tela de votação.
- e) Concluída a dupla identificação biométrica, o eleitor tem acesso à tela de votação onde visualiza os candidatos e utilizando um teclado para realizar o voto eletrônico parcial. Após confirmar os candidatos o eleitor autoriza a impressão da cédula de segurança.
- f) O eleitor retira a cédula de segurança da interface impressora e audita o voto em texto e em código de barras, através de um tablet externo.
- g) Confirmado o voto impresso, o eleitor insere a cédula de segurança na interface coletora, onde esta é sugada e posicionada aleatoriamente dentro da Urna Independente. Nesse momento o sistema eletrônico registra o voto digital, emitido um sinal sonoro e encerrando a possibilidade de uma nova votação para aquele eleitor.
- h) Caso o eleitor se arrependa e rejeite o voto impresso na cédula, ele deve eliminá-la inserindo-a na interface fragmentadora, que tritura o papel e automaticamente emite um sinal para o programa de computador cancelar a gravação do voto digital e reiniciar o processo de votação.

Todas e quaisquer operações que não comprometam o sigilo do voto serão registradas nos arquivos de “logs” do equipamento eletrônico de votação e da Mesa Receptora Independente, sempre assinado digitalmente com as chaves privadas das instituições participantes do processo.

4. Métodos de Segurança

A segurança do modelo proposto é baseada na técnica de criptografia de algoritmos de par de chaves assimétricas onde uma informação codificada utilizando a chave privada é decodificada somente por quem possua a chave pública, e vice-versa, garantindo a integridade, procedência e o sigilo das informações geradas, quando assim for necessário.

Na cédula, ela será usada para gerar as assinaturas digitais das informações do voto impresso em texto e em linguagem XML, inclusa no código bidimensional. No caso, uma primeira assinatura que comprovará a procedência institucional será criada com a chave privada da “Mesa Independente” e uma segunda assinatura, que reforça a primeira, sendo proveniente da chave privada de uma instituição auditora do processo.

Na prática, a segurança com criptografia assimétrica funcionará da seguinte forma:

- 1- Cada Mesa Independente possuirá dispositivos específicos (Smart Cards, Tokens ou outro chip criptográfico) responsável pela geração do par de chaves criptográficas.
- 2- O programa de computador responsável pela coleta de votos, após coletar todas as intenções do eleitor para os cargos em disputa e obter a confirmação para impressão da cédula, assinará com a chave privada da Mesa Independente o registro do voto em formato de texto e o registro do voto em formato XML. Todas as assinaturas serão impressas em formato de códigos de barras.
- 3- Uma segunda assinatura será gerada pelo programa de coleta de votos, mas com a chave privada de uma instituição independente do administrador eleitoral.
- 4- Após ler o texto da cédula e confirmar seu voto, o eleitor insere a cédula de segurança na interface validadora/coletora. Um programa de computador específico, em posse da chave pública, fará a conferência da assinatura digital embutida no código de barras, confirmando que a cédula foi gerada pelo mesmo equipamento que a coletará, bem como validando a integridade das informações contidas na cédula.
- 5- A assinatura digital gerada pela chave privada da instituição independente poderá ser utilizada pelo eleitor para uma segunda verificação de autenticidade do voto, que será realizada por um segundo equipamento eletrônico, onde estarão armazenadas as chaves públicas.

A conversão das informações em código bidimensional QR (Quick Response) também garante a segurança do processo já que impede o eleitor de memorizar informações, como as assinaturas digitais, que identificam a cédula e poderiam ser utilizadas como comprovação da venda de votos.

Para a segurança física das cédulas coletadas serão utilizados selos, ou lacres, com tecnologia radio frequência (RFID). Esse recurso permite identificar as urnas que receberão as cédulas válidas, construindo uma correlação para auditoria entre a caixa, a seção eleitoral, a máquina que apurou as cédulas e o bloco de cédulas apuradas.

A tecnologia serve também para garantir da integridade física da urna coletora contra eventuais tentativas de violação para inclusão ou exclusão fraudulentas de cédulas.

O RFID também será utilizado na Máquina de Apuração. O equipamento que faz a auditoria e a contagem dos votos coletados pela Mesa Independente só será acionado após a comprovação da identidade da urna coletora e de sua integridade física.

Após desempenhar as funções de auditar e contar votos, a Máquina Apuradora embala as cédulas e volta a utilizar um selo RFID que, além de garantir a segurança física do escrutínio, vai ser utilizado para facilitar o arquivamento do material coletado em cada eleição.

5.Conclusão

O modelo aqui proposto vai ao encontro do projeto inicial da urna eletrônica atualmente em uso no Brasil. Quando da sua concepção, ainda na década de 80, os estudos desenvolvidos pela autoridade eleitoral avaliaram vários modelos de urnas, sendo que todos os protótipos escolhidos como matrizes do projeto continham um dispositivo de impressão para garantir a integridade da eleição em caso de falha eletrônica [7].

Retirado duas vezes do processo eleitoral brasileiro (a primeira motivada pela hoje questionada credibilidade da urna e a segunda motivada por razões técnicas e políticas), o voto impresso proposto neste artigo ressurgiu movido pelas mesmas preocupações dos pioneiros que alavancaram o voto eletrônico no Brasil: a segurança do processo eleitoral em caso de falha eletrônica e a transparência do processo eleitoral.

Já as máquinas aqui propostas são um desafio para as ciências, tanto para a área da computação, que poderá criar ou aperfeiçoar *softwares* de votação em código aberto, quanto para área de engenharia mecatrônica, que passa ter um norte para a inclusão da robótica no processo de votação.

Referências bibliográficas

- [1] Presidência da República, Lei 12.034 disponível em http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/112034.htm
- [2] Rivest, R. L. (2008) “On the notion of “software independence” in voting systems”, Phil. Trans. R. Soc. A, vol. 366 no. 1881 pag 3759-3767, disponível em <http://rsta.royalsocietypublishing.org/content/366/1881/3759>
- [3] Supremo Tribunal Federal, Processo ADI/4543, disponível em <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4019347>
- [4] Agência Terra, Urna é a mais defasada, diz professor que violou sistema do TSE, disponível em <http://noticias.terra.com.br/brasil/politica/eleicoes/urna-e-a-mais-defasada-diz-professor-que-violou-sistema-do-tse,dbeadf0a2566b310VgnCLD200000bbccceb0aRCRD.html>
- [5] United States Election Assistance Commission, Seção 7.8, Apêndice C da “*Voluntary Voting System Guidelines*” (vol. 1) disponível em: http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx
- [6] Tribunal Superior Eleitoral, Concorrência 11.179/2010, Especificação UE 2011, Anexo II, pag 9, disponível em <http://www.tse.jus.br/transparencia/licitacoes-e-contratos/licitacoes/licitacoes-concluidas>
- [7] CAMARÃO, P. C. (1997), “O voto informatizado: Legitimidade Democrática”, Empresa das Artes, pag 76-81