O mito da urna

desvendando a (in)segurança da urna eletrônica

Jeroen van de Graaf

Prelúdio:
"A urna é segura?" Todo cidadão responsável deve ter se perguntado isso pelo menos uma vez na vida. Talvez a dúvida volte a cada dois anos.

Pessoas com um viés mais técnico devem ter percebido o cabo de 5 metros que conecta o teclado onde o mesário digita seu título de eleitor à própria urna. Será que isso está seguro?

O Tribunal Superior Eleitoral garante que a urna é segura, mas quem vai buscar na internet encontra críticas severas. Mas no que deve-se acreditar? E ainda houve a contestação do PSDB em 2014, que menciona que grande parte da população desconfia da urna.

É uma situação confusa e insatisfatória, que este livro explica detalhadamente numa forma simples. Apresenta uma análise da segurança da urna eletrônica, fazendo uma comparação com uma eleição tradicional com cédulas em papel. O eleitor será capaz de formar a sua própria opinião.

Este livro também discute o mito ao redor da urna, que teria segurança perfeita e que seria a inveja do mundo. Claro que o país todo tem interesse em um sistema eleitoral confiável com credibilidade. Mas não existe um diálogo aberto e racional entre o TSE e a sociedade sobre a segurança do processo eleitoral. Decisões são tomadas sem base científica.

Einstein já disse que as coisas devem ser explicadas de forma mais simples possível, mas não mais simples do que isso. Com base nesta filosofia, este livro se dirige a não-especialistas: advogados, juízes, médicos, jornalistas, dentistas, arquitetos, etc. Ou seja, qualquer cidadão interessado e persistente, que realmente gostaria de entender se a urna é segura ou não.

Sobre o autor:
Jeroen van de Graaf (1960) é mestre em matemática pela Universidade de Amsterdam (1985) e doutor em informática pela Universidade de Montreal (1998). Faz pesquisa em criptografia já há mais que três décadas, sempre com foco em privacidade e transparência. Estuda sistemas e protocolos de votação já há mais que quinze anos. Hoje é professor do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, onde é um dos coordenadores do INSCRYPT, o Laboratory for Information Security, Cryptography, Privacy, and Transparency. Reside no país desde 1998 com visto permanente (Holanda não permite nacionalidade dupla); portanto nunca votou no Brasil.

Página web do livro: www.o-mito-da-urna.org

Versão 1.0 – 17/11/2017 : primeira versão
Versão 1.1 – 27/11/2017 : correções de ortografia

Do not harbor sinister designs.
Diligently pursue the path of "the two swords as one."
Cultivate a wide range of interests in the arts.
Be knowledgeable in a variety of occupations.
Be discrete regarding one's commercial dealings.
Nurture the ability to see the truth in all matters.
Perceive that which cannot be seen with the eye.
Do not be negligent, even in trifling matters.
Do not engage in useless activity.
Miyamoto Musashi

Dedicado a meu filho Alexandre,
que me ensinou o significado das palavras 'diabinho' e 'zombaria'.

Lista de siglas e termos

adversário Na área de criptografia e segurança de informação, **adversário** é o nome dado à entidade imaginária que tenta violar a segurança do sistema contemplado. É uma abstração neutra, sem conotação emocional, de palavras como *hacker*, *fraudador*, *inimigo* etc.

CESeg Comissão Especial de Segurança da SBC.

DRE Na terminologia estadunidense, a urna é um DRE, sigla para *Direct-recording electronic (DRE) voting machine* ou seja, um dispositivo que registra (armazena) os votos apenas na memória. Uma diferença é que nos DREs nos EUA, a identificação do eleitor **não** é integrada com o próprio DRE; ela é feita de forma independente.

log Cada sistema computacional tem um 'diário de bordo' que automaticamente registra todos os eventos importantes, chamado **arquivo log** ou simplesmente **log**.

RelSBC O relatório *Tecnologia Eleitoral e a Urna Eletrônica* escrito em 2002/2003, referência [10]. Veja pg. 14.

resumo criptográfico Uma função de hash criptográfica tem como entrada uma sequência de bits com tamanho qualquer, tendo como resultado uma sequência de 256 bits, o resumo criptográfico. O papel desta função é embaralhar todos os bits da entrada, de maneira que o resultado parece randômico, e que não é possível encontrar duas entradas diferentes com o mesmo resumo criptográfico. Portanto, o resumo criptográfico funciona com se fosse um identificador único da sequência de entrada, e por este motivo pode ser considerado o equivalente digital de uma impressão digital.

SBC Sociedade Brasileira de Computação.

STI Secretaria de Tecnologia da Informação do TSE (anteriormente chamada Secretaria de Informática)

TI tecnologia da informação

TRE Tribunal Regional Eleitoral

TSE Tribunal Superior Eleitoral

Sumário

Prefácio por Diego Aranha

No livro “O mito da urna”, o Prof. Jeroen ilumina o eterno debate em torno da (in)segurança da urna eletrônica com argumentos bastante acessíveis. Ao contrário de outros textos técnicos direcionados a especialistas, o livro procura responder às perguntas elementares que cidadãos brasileiros continuam a se perguntar, após mais de 20 anos da introdução de votação eletrônica no país. Alguns exemplos dessas perguntas, que aparecem de forma recorrente na Internet e na vida cotidiana, muitas vezes em longas discussões, são: ”Por que o Brasil utiliza urnas eletrônicas sem registro físico, ao contrário do resto do mundo?”, ”Esses equipamentos são realmente seguros?”, ”Os resultados são suficientemente transparentes e verificáveis?”, ”Aliás, o que é um sistema de votação seguro e transparente?”. A lista é extensa.

Em uma sequência de 9 capítulos, o livro começa sua visita ao tema do ponto de vista histórico. Posteriormente, enuncia nos Capítulos 2 e 3 os principais requisitos de segurança e transparência que um sistema de votação, em qualquer meio físico ou eletrônico imaginável, precisa simplesmente satisfazer para ser confiável. A urna eletrônica é então analisada sob a luz desse conjunto de requisitos nos Capítulos 4 e 5, com exemplos cuidadosamente descritos que contradizem os vários requisitos, tanto formalmente quanto experimentalmente. Os Capítulos 6 e 7 são mais construtivos e buscam soluções a longo prazo para aprimorar o estado geral das coisas. Os dois últimos Capítulos são de natureza mais política e resumem as posições oficiais do Tribunal Superior Eleitoral (TSE), manifestadas na tentativa de sustentar um mito insustentável por tantos anos, cujo preço todos nós (literalmente) pagamos. Uma tentativa sincera de tentar entender como chegamos até aqui é particularmente reveladora.

Como pesquisador dedicado e envolvido no debate em torno das urnas eletrônicas há 5 anos, sinto-me contente de finalmente encontrar um texto

acessível ao público geral, que com certeza se tornará referência no tema. A discussão focada na impossibilidade do sistema atual de provar a correção do resultado oficial retorna o debate ao ponto que verdadeiramente importa e corrige sua rota. A comunidade técnica, contando comigo inclusive, tem persistido no erro de se concentrar em torno de críticas à insegurança do software de votação, que termina sendo inacessível sem especialização, e reforça a posição do TSE de que o sistema atual pode ser incrementalmente corrigido. Precisávamos realmente de um pesquisador com mais de 20 anos de experiência em votação eletrônica e ao menos 15 anos de familiaridade com as urnas brasileiras para nos lembrar do que é relevante. Fico muito feliz de ter sido escrito por um amigo e colega de profissão e pesquisa.

Aproveitem a jornada!

Diego F. Aranha

Introdução

Cinco dias depois que Dilma Rousseff foi reeleita para presidente, o PSDB solicitou uma auditoria do resultado eleitoral, mencionando entre outros fatores a "desconfiança geral entre a população" sobre a tecnologia eleitoral utilizada. Isso ilustra um ponto importante, bem conhecido entre os pesquisadores eleitorais: um sistema eleitoral não deve apenas convencer a maioria da população sobre quem ganhou as eleições. Para acabar com todas as controvérsias, um sistema bem projetado deve **provar** para o perdedor que ele perdeu.

Infelizmente, a urna eletrônica atual nunca será capaz de dar uma prova desse tipo, porque nunca foi projetada para ser transparente. A segurança da urna baseia-se na filosofia de "segurança por obscuridade", de acordo com a qual os detalhes do projeto de um sistema devem ser mantidos secretos para evitar que a segurança seja comprometida. Esta filosofia de projeto certamente faz sentido em muitos casos, em contextos militares por exemplo. Mas não faz sentido no projeto do processo central de uma democracia: a eleição.

Para terem credibilidade, as eleições devem ser totalmente transparentes. O problema é que, no Brasil, para acreditar no resultado das eleições, é preciso ter fé cega nas autoridades eleitorais. Nenhuma confirmação independente da corretude do resultado da eleição é possível, pois não é possível recontar os votos. E esta é a forma como o sistema foi construído: é uma caixa preta, cujo funcionamento interno é conhecido apenas por um pequeno grupo de técnicos do TSE.

Essa falta de transparência tem sido alvo de severas críticas de muitas pessoas na academia desde que a urna foi projetada, dentro do Brasil e também no exterior. É também a razão que este mito, criado e cultivado pelo TSE, de que a urna é a inveja do mundo e que poderia ser um produto de exportação, simplesmente não é verdade. Por exemplo, em vários lugares como Holanda, Alemanha, Califórnia e Índia, o uso de tecnologias equivalentes à urna foi banido, exatamente por sua

falta de transparência. Em nível internacional, o projeto da urna é considerado irremediavelmente desatualizado.

Este livro aborda este ponto: a falta de transparência da urna eletrônica. Eu afirmo que o TSE tem dormido por mais de uma década. Se o TSE tivesse escolhido uma tecnologia de segurança diferente há quinze anos, o Brasil poderia ter um sistema eleitoral muito mais aberto e transparente. Na medida em que o TSE poderia ter **provado**, além de qualquer dúvida, se Aécio Neves, o candidato do PSDB, perdeu as eleições contra a Dilma ou não.

O que eu (não) estou dizendo

Não estou dizendo que a urna tenha sido uma má idéia. Pessoalmente, acredito que a urna trouxe a estabilidade necessária para o processo eleitoral no Brasil.

Não estou dizendo que devemos voltar às cédulas de papel. Ao contrário do meu país nativo, a Holanda, onde o equivalente da urna foi proibido e a votação atualmente ocorre com cédulas de papel, acredito que, para o Brasil, provavelmente seja mais seguro continuar usando a urna do que retornar às cédulas de papel.

Não estou dizendo que a urna já foi fraudada. Durante todos esses anos eu nunca vi provas convincentes deste tipo de fraude no Brasil, o que não quer dizer que não houve. Este é exatamente o problema: a urna sofre de uma falta de transparência muito séria. É tão mal concebida que a sua segurança não pode ser comprovada.

Em particular, não estou dizendo que a eleição presidencial de 2014 (Dilma-Aécio) declarou o vencedor errado. Mas a urna não é suficientemente transparente para provar ao candidato perdedor (neste caso Aécio) que perdeu.

O que estou dizendo é que a suposta segurança da urna foi exagerada, fora de proporção, pelo que considero uma lavagem cerebral. Grande parte da população brasileira são levadas a acreditar neste mito, que a urna é infalível, que é a inveja do mundo e que poderia ser um produto de exportação. Isso simplesmente não é verdade, é um conto de fadas.

Não estou dizendo que o TSE é malvado. O que estou dizendo é que o TSE tem sido complacente ao não buscar sistemas eleitorais mais transparentes. Sistemas melhores já começaram a aparecer em 2001 e 2002, então mais de 15 anos precio-

sos foram perdidos. Do TSE, tendo o papel de guardião do processo eleitoral, se esperaria mais.

Capítulo 1

Prólogo

Neste capítulo esboçamos o contexto histórico: como eram as votações antes da urna eletrônica, o advento da urna eletrônica, meu envolvimento como observador em 2002, e os quinze anos depois. Não tem a pretensão de ser completo. Seria possível escrever vários capítulos somente sobre toda a polêmica que a urna já criou, mas não contribuiria para encontrar uma solução.

Votar antes da urna

Antes da introdução da urna eletrônica no Brasil, se votava usando cédulas em papel: o eleitor anotava o nome ou número do candidato numa cédula e depositava na urna de lona.

Esse processo tem vários defeitos graves. Um defeito é a questão da ambiguidade do voto: O nome escrito é Fulano ou Beltrano? O número é um 1 ou um 7? Devido ao grande número de candidatos em algumas eleições (para vereador, por exemplo) não é possível imprimir uma cédula com todos os candidatos, na qual o eleitor marca (com um X por exemplo) o seu voto. Além disso não existe nenhum mecanismo para que o eleitor possa verificar se seu voto está correto.

Essa ambiguidade também é uma grande fonte de problemas no processo de apuração dos votos. Muitas vezes uma recontagem dava um resultado diferente, e uma segunda recontagem não confirmava um dos valores anteriores mas dava um novo, terceiro valor. E isso ocorria na madrugada ou no dia seguinte à eleição, com todos os participantes exaustos por estarem até aquele momento sem dormir.

A totalização dos votos, ou seja, a agregação dos resultados de cada urna por município ou estado, também dava problemas. O caso mais famoso é o das primeiras eleições de governador de Rio de Janeiro depois da ditadura, em 1982. O TRE terceirizou a totalização para a empresa Proconsult, dominada por pessoas vinculadas aos militares. Manipulando os votos brancos e nulos, eles tentaram impedir que Leonel Brizola ganhasse, já que apoiavam o candidato Moreira Franco.

A fraude foi descoberta e denunciada graças aos esforços do Jornal do Brasil, que montou um sistema de apuração paralela da contagem de votos, mostrando resultados bem diferentes. Após doze dias de confusão, a fraude foi reconhecida e o TRE declarou Brizola vencedor[(a)].

A urna eletrônica mudou tudo, o que sem dúvida é uma grande conquista, dada a grande estabilidade que deu ao processo eleitoral.

O advento da urna eletrônica

Nas eleições de 1996 a urna eletrônica foi usada pela primeira vez. O grande idealizador da urna eletrônica é Paulo César Bhering Camarão, Secretário de Informática do TSE à época. Para ele a urna eletrônica era *a chance of a lifetime*[(b)] para dar uma grande melhoria ao processo eleitoral brasileiro, documentado no seu livro *O Voto Informatizado: Legitimidade Democrática* [2].[(c)]

A urna eletrônica traz várias grandes vantagens:

- O eleitor tem um retorno ao ver a foto do candidato;
- A urna elimina a ambiguidade do voto;
- A urna acelera o processo de apuração;
- Usando redes e grandes servidores, é possível totalizar todos os resultados e determinar o vencedor na mesma noite.

No início a urna somente foi usada em cidades com mais que 200 mil habitantes. Em 2000 foi a primeira vez que a urna eletrônica foi usada no País todo.

Além dos desafios técnicos (o foco deste livro), a urna também enfrenta um grande desafio logístico. Entregar uma urna num município muito remoto, mantê-la funcionando sem problemas durante o dia da eleição, e enviar os resultados o quanto antes para o TRE não é uma coisa trivial. Nesses aspectos

a ‘urna’, não apenas como equipamento mas como um grande projeto nacional para informatizar o voto, foi um grande sucesso.

Do painel do Senado para a urna

Entre maio e junho de 2001 houve o escândalo do painel do Senado. Pelo regimento do Senado determinadas votações são confidenciais, mas a implementação do sistema foi simplória: quem tivesse acesso privilegiado ao sistema informatizado podia descobrir quem votou em quem. O senador José Roberto Arruda (PSDB à época) tinha obrigado a diretora do Prodasen (Centro de Processamento de Dados do Senado), Regina Borges, a fornecer a lista com o voto de cada senador na sessão secreta que cassou o então senador Luiz Estevão (PMDB-DF). [(d)]

Tendo chegado no Brasil em 1998, foi a primeira vez que realmente comecei a acompanhar a política brasileira. Projetar sistemas de votação com ajuda de protocolos criptográficos fazia parte dos meus interesses científicos. Eu sabia que para uma votação simples (sim/não com 81 votantes) era possível fazer um sistema auditável, mantendo o sigilo do voto.

Assim, eu comecei a me fazer perguntas sobre a segurança da urna, o que levou a um artigo, em coautoria com meu orientado Wilton Speziali Caldas, apresentado no Simpósio de Segurança da Informação de 2001 no Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos [9]. Apesar de algumas conversas informais[(e)], nenhuma das sugestões foi adotada pelo TSE.

O relatório da SBC – 2002

Em 2002, o TSE solicitou que representantes da Sociedade Brasileira de Computação acompanhassem as eleições daquele ano. Duas pessoas se candidataram: prof. Ricardo Felipe Custódio da UFSC, e eu. Nosso papel não era o de um fiscal de partido, mas o de testemunha e observador imparcial.

Nos meses antes das eleições, nós pudemos participar das sessões de avaliação do Sistema Informatizado de Eleições em três oportunidades: duas antes do primeiro turno e uma antes do segundo turno.[(f)] O trabalho consistia em participar

das sessões públicas no TSE (com passagens e diárias pagas pelo TSE), em que os partidos políticos têm o direito de analisar os sistemas a serem usados nas eleições: programas da urna, programas para configurar as urnas, programas para receber os resultados das urnas e totalizar os resultados, etc. Também acompanhamos o trabalho no TRE: a preparação das urnas e as atividades na véspera e no dia da eleições.

Uma coisa que me chamou atenção à época foi a falta total de interesse dos partidos políticos. Dos partidos, em particular dos grandes como o PSDB e PMDB, se espera que assumam o papel como testemunha num processo tão importante como uma eleição. Mas apenas encontrei representantes do PDT e do PT durante todos meus encontros no TSE (em 2002 e 2004). O que explica a ausência dos outros partidos? Desprezo pelo processo eleitoral?[g]

Nossos trabalhos resultaram num relatório publicado em maio de 2003 [10]. Usarei a sigla RELSBC para me referir a este relatório.

O relatório continha várias críticas e sugestões, mas o TSE não gostou. Não fomos convidados para dar explicações, e o TSE essencialmente engavetou o nosso relatório.

A última década

Durante muitos anos poucas notícias foram veiculadas sobre a urna ou a sua segurança. Isso até 2012, quando Diego Aranha, então na UnB (hoje na UNICAMP) participou dos Testes Públicos da Segurança do Sistema Eletrônico de Votação. Ele descobriu um erro muito grave, relatado na página 53.

Depois das experiências de Aranha, a Comissão Especial de Segurança da SBC, que reúne a maioria dos pesquisadores acadêmicos na área de segurança digital, decidiu criar um Workshop de Tecnologia Eleitoral como evento satélite do Simpósio Brasileira de Segurança (SBSeg), o maior evento nacional desta área. O primeiro Workshop ocorreu em 2014, mas depois decidiu-se fazer a cada dois anos, em anos ímpares, assim evitando anos eleitorais.

Em agosto de 2016, o TSE procurou colaboração com a SBC. Mas o escopo desta colaboração ainda não está muito claro. O convênio assinado tem que ser detalhado através de planos de trabalho para a execução de determinados projetos.

Um possível serviço é a participação de membros da CESeg ao Teste Público de Segurança, organizado pelo TSE, o que seria muito importante.

No entanto, vários pesquisadores acreditam que o serviço não deva ser meramente a auditoria a urna atual, baseada num projeto ultrapassado e sem salvação. Eles consideram importante discutir o futuro da urna; uma nova urna que seja realmente transparente. Porém, não está claro se o TSE está aberto a esta discussão. O fato é que o TSE pretende gastar 2 bilhões de reais nos próximos anos para implementar o voto impresso[(h)], um indício forte de que a resposta seja negativa.[(i)]

Anotações

[(a)]http://www.jb.com.br/pais/noticias/2012/11/27/ha-30-anos-jb-revelou-escandalo-do-proconsult-e-derrubou-fraude-na-eleicao

[(b)]"Paulo César Camarão teve *a chance of a lifetime* e se fez, com rara maestria e acuidade, o engenheiro, o gerente e o escriba – um Pero Vaz de Caminha, nessa expedição de sonho de liberdade sob o timão seguro, severo e amigo do Ministro Carlos Mário Velloso, a quem não escapou a oportunidade histórica de fazer acontecer o que todos os cidadãos autênticos desse País mais buscam nessa quadra da vida nacional em que, mais uma vez, e ainda uma vez, tentamos construir uma democracia: a certeza da verdade eleitoral. Este livro é o registro fiel de um sonho feito realidade." Texto na contra-capa do livro do Camarão[2] por Torquato Jardim, então Ministro do TSE, atualmente Ministro de Justiça.

[(c)]Já em 2002 ouvi críticas de que o TSE contratou várias empresas sem licitação. Não pretendo elaborar este aspecto da urna, mas acho interessante mencionar este trecho: "No ano de 2006, a Probank S/A foi contratada pelo então Secretário de Informática do Tribunal Superior Eleitoral, Paulo Camarão – que esteve no cargo por quase dez anos – para os serviços de urnas. No mesmo ano, Camarão tornou-se proprietário da Probank, criando, entre outros serviços o de totalização dos votos (E-VOTE), que chegou a ser vendido ao Equador também em 2006, depois de um acordo rompido, em que o TSE forneceria 2.200 urnas brasileiras às eleições do país." https://jornalggn.com.br/noticia/o-historico-de-favorecimento-e-irregularidades-nas-licitacoes-das-urnas-eletronicas

[(d)]http://www1.folha.uol.com.br/folha/brasil/ult96u53269.shtml

[(e)]Durante o simpósio conheci Dr. Catsumi, doutor em Engenharia Elêtrica pela Universidade de Tókio, pesquisador de CTA e o grande arquiteto técnico da urna.

[(f)]Foi quando eu conheci Dr. Camarão.

[(g)]Então, até 2014, o PSDB nunca se interessou para comparecer aos eventos organizados pelo TSE para conhecer ou auditar o sistema eleitoral. Mas em outubro daquele ano o partido, a perder uma eleição com uma quantidade significativa, em termos absolutos, de 3459963 votos, de repente

questionou o sistema eleitoral. Isso parece um comportamento oportunista que não se espera de um grande partido político numa democracia.

[(h)] As estimativas variam dependendo do prazo considerado e a cotação do dolar, e ficam entre 1,5 e 2.5 bilhões de reais Veja por exemplo http://politica.estadao.com.br/noticias/geral,impressao-de-voto-vai-custar-r-2-5-bi-diz-tse,70001900669 e http://www.tse.jus.br/imprensa/noticias-tse/2017/Junho/justica-eleitoral-trabalha-para-desenvolver-nova-urna-eletronica-que-tera-o-voto-impresso

[(i)] Para evitar qualquer dúvida ou constrangimento, quero deixar claro que a ideia de escrever este livro foi inteiramente minha. Nada disso foi discutido ou combinado com a SBC ou a CESeg, e portanto o livro apresenta a minha opinião pessoal.

Capítulo 2

Requisitos para eleições justas

Urna segura e eleição justa

"A urna é segura?"

Esta questão já me foi colocada dezenas de vezes. Mas antes de poder responder essa pergunta, é importante entender o que o termo "segurança" quer dizer exatamente.

Segurança é uma palavra que pode significar coisas diferentes para pessoas diferentes. Como especialista em segurança digital já me treinei a me perguntar, assim que escuto a palavra *seguro* ou *segurança*: o que o palestrante ou autor quer dizer exatamente? Quer dizer confiabilidade e robustez do processo? Sigilo do voto? Corretude do resultado? Então, primeiro é necessário definir o que "segurança" quer dizer no contexto de uma eleição.

Nós abordamos essa questão de uma forma simples e intuitiva. Primeiro apresentamos uma eleição convencional usando cédulas em papel. Segundo, faremos uma análise cuidadosa das propriedades de segurança às quais uma eleição deve satisfazer. Terceiro, formulamos uma lista de dez requisitos para uma eleição justa. Essa lista servirá como ponto de partida para discutir e analisar as propriedades da urna eletrônica nos outros capítulos deste livro.[(a)]

Uma eleição por cédulas em papel

Introduzimos a eleição por cédulas em papel por duas razões. Primeiro, quando se discute a tecnologia de eleição através de urnas eletrônicas, é bom ter uma referência. Especificamente, quando se discute a urna e se afirma que uma coisa é boa ou ruim, deve-se fazê-lo em relação a algo. Em segundo lugar, com uma eleição por cédulas em mente, podemos com mais facilidade apresentar os requisitos de segurança que uma votação deve obedecer.

Uma eleição convencional passa pelas seguintes etapas:

1. Estabelece uma lista com os nomes de todos os eleitores legítimos.
2. Antes de iniciar a eleição, todas as pessoas presentes testemunham que a urna está vazia.
3. Um eleitor legítimo que ainda não votou recebe uma cédula, entra na cabine de votação e preenche sua preferência.
4. O eleitor verifica a preferência preenchida na cédula.
5. O eleitor deposita sua cédula na urna. A partir desse momento, o voto é emitido, e ele não pode desfazer ou modificar seu voto.
6. Quando o tempo de votação expira, todos os presentes observam a abertura da urna e a apuração das cédulas contidas nela.
7. Aqueles que não concordam com a contagem podem solicitar uma recontagem. Os votos são recontados, sob a observação de todos os presentes, até que haja consenso.

Acreditamos que essas são as etapas típicas do processo de votação em muitos países, seja para eleições confidenciais nas câmaras de órgãos legislativos ou para eleições públicas em vários níveis de governo. As diferenças ocorrem, em geral, na formatação gráfica das cédulas e na forma como os eleitores marcam escolhas: uma cruz em um quadrado, conectando uma seta, preenchendo um círculo, escrevendo um número, escrevendo um nome, etc. Essas diferenças na sua maioria não alteram essencialmente os requisitos de segurança.

Votações com múltiplas urnas

Em grandes eleições e votações é geograficamente e logisticamente impossível que todo mundo vote na mesma urna. Então haverá múltiplas urnas, cujos resultados serão totalizados para se chegar ao resultado final.

Na página 13 já relatamos brevemente a tentativa de se fraudar o processo de totalização nas eleições para governador do Rio de Janeiro em 1982. Hoje tal fraude seria quase impossível. Dados os resultados da apuração de cada urna, qualquer pessoa com uma planilha consegue verificar a totalização dos votos. E esses dados passam por tantos técnicos do TRE que seria impossível abafar isso.

Então, um ponto crucial do processo é que os dados da apuração de cada urna sejam fielmente enviados ao TRE. Mais que isso, esse processo deveria ser verificável, mas durante muitos anos não era.

Já em 2001 eu propus que, após a eleição, a urna imprimisse um resumo criptográfico do Boletim da Urna, o relatório contendo todos os resultados.[(b)] Um observador somente precisaria anotar esse resumo. Posteriormente, quando o Boletim fosse publicado na internet, bastaria recalcular o resumo criptográfico e comparar com o valor anotado. Infelizmente essa sugestão não foi aceita.

Com a tecnologia avançando surgiu um outro caminho. Com uma câmera digital é possível tirar fotos do Boletim, mandar para um servidor, reconhecer o texto escrito no Boletim, e fazer a comparação com os dados oficiais publicados pelo TRE. Esse foi o projeto Você Fiscal, uma iniciativa de Diego Aranha que começou em 2014.[(c)]

Desta vez o TSE aceitou a sugestão. Desde 2016, a urna imprime o Boletim em dois formatos: primeiro normal, com letras e números; e uma cópia disso no formato de um QR Code. Isso simplifica em muito o processo, porque a parte árdua, o reconhecimento óptico de caracteres, é eliminada.[(d)]

Requisitos de uma votação justa

Sobre quem pode votar

REQUISITO A (APENAS ELEITORES VÁLIDOS)
Somente os eleitores legítimos, chamados de eleitores daqui por diante, podem depositar uma cédula nas urnas.
Explicação: Qualquer eleição tem um conjunto finito de pessoas que têm o direito de votar e apenas essas pessoas têm permissão para acessar o processo de votação.

REQUISITO B (*One man, one vote*)
Um eleitor pode votar no máximo uma vez.
Explicação: Não é permitido que a mesma pessoa vote duas vezes.

Sobre o ato de votar — a criação e transmissão de cédulas

REQUISITO C (SIGILO DO VOTO)
Preencher a cédula e colocá-la na urna é um ato confidencial e, em nenhuma circunstância, nem mesmo com a conivência do eleitor, deve ser possível deduzir qualquer informação sobre a opção votada pelo eleitor.
Explicação: é importante perceber que esse requisito tem dois aspectos. Primeiro, o eleitor deve ter a liberdade de expressar sua vontade sem o risco de repercussão. Para garantir isso, ninguém deve ser capaz de descobrir em quem ou no que ele votou ou deixou de votar.

Em segundo lugar, é necessário evitar a chamada 'influência imprópria' aos eleitores, que inclui a compra e venda de votos. Consequentemente, não deve ser possível, *mesmo com a cooperação ou conivência do eleitor*, a dedução do voto. Por esta razão, é de extrema importância que, durante a marcação e depósito da cédula, não seja criada nenhuma prova ou recibo que possa ser vinculada a um voto dentro da urna, uma vez que isso permitiria uma influência ou coação indevida sobre o eleitor.

Para garantir a confidencialidade do voto, existe um espaço privado, a cabine de votação, onde o eleitor pode preencher a cédula. Este requisito poderia ser reformulado afirmando que a única informação que pode sair da cabine de votação é o voto preenchido na cédula, nada mais.

REQUISITO D (VERIFICAÇÃO DA CÉDULA)
O eleitor pode verificar seu voto, se certificar se seu voto é válido, e pode rever seu voto antes de se comprometer.
Explicação: Depois de ter criado seu voto, mas antes de depositá-lo, o eleitor deve ter o direito de verificar se o seu voto está marcado como pretendido e que é válido. Ele deve ter a oportunidade de corrigir ou revisar sua cédula.

REQUISITO E (A CÉDULA SERÁ APURADA)
O eleitor pode se convencer de que seu voto está incluído no conjunto de votos apurados.
Explicação: Este requisito é o mais difícil de se concretizar. Gostaríamos de entregar uma prova/recibo ao eleitor, permitindo que ele verifique se seu voto está entre o conjunto de votos que serão apurados. A sabedoria convencional diz que esse requisito contradiz o requisito mais importante do sigilo do voto.

No caso das cédulas de papel, este requisito é conceitualmente alcançado da seguinte maneira: depois que o eleitor votou, depositando a cédula na urna, ele aguarda até o encerramento da eleição e quando a urna é aberta para a apuração, ele tem certeza de que sua cédula está no conjunto de votos que serão apurados, mesmo que não saiba qual voto particular corresponde ao que preencheu. Note-se que, essencialmente, a fé do eleitor se baseia na noção de senso comum de que um objeto colocado em algum lugar permanece lá e não desaparecerá por si só.

Existe uma tensão entre a exigência de verificabilidade, por um lado, e o sigilo do voto, por outro, o que torna o projeto dos sistemas eleitorais satisfatórios para ambos os requisitos sem usar cédulas ou outros objetos físicos extremamente complicado. Para proteger o anonimato do eleitor, toda eleição possui um procedimento implícito que mistura (embaralha) os votos, destruindo o vínculo entre a cédula e o eleitor. Este procedimento, trivial ao lidar com objetos físicos como cédulas ou cartas de baralho, é muito difícil de se simular no mundo virtual. O problema é difícil devido ao requisito de verificabilidade deste procedimento: deve ser possível garantir que o processo virtual de misturar não adicione, subtraia ou substitua nenhum dos itens originais. Voltaremos a este tópico ao discutir a comprovação física, na Seção 3.

Sobre a integridade do voto — de depositar a apurar

REQUISITO F (INTEGRIDADE DA CÉDULA E DA URNA)
Não deve ser possível que alguém modifique uma cédula, ou remova-a da urna, nem deve

ser possível adicionar cédulas não provenientes de eleitores legítimos.
Explicação: Os votos representam a vontade (anônima) dos eleitores, e qualquer modificação alteraria essa vontade.

Este requisito explica, por exemplo, por que se mostra a urna vazia antes de se iniciar a eleição; por que a urna deve permanecer em um lugar publicamente visível; e também por que, às vezes, urnas transparentes são usadas.

REQUISITO G (SIGILO ATÉ O FIM DA VOTAÇÃO)
Todos os votos permanecem secretos até o final da votação.
Explicação: Primeiro, revelar resultados parciais violaria o segredo da votação para aqueles que já votaram. Segundo, o conhecimento do resultado parcial pode influenciar o voto de alguém que vota mais tarde. Além disso, o acesso exclusivo a esta informação durante o período de votação pode proporcionar vantagem em termos de alocação de recursos eleitorais no dia da eleição ou mesmo desencadear a interrupção do processo de votação.

Sobre a apuração dos votos

REQUISITO H (CORRETUDE DA CONTAGEM)
Todas as cédulas válidas encontradas na urna, e somente aquelas, serão incluídas na contagem.
Explicação: os votos não escritos em uma cédula apropriada, por exemplo, não devem ser incluídos na apuração, pois podem representar múltiplos votos de um único eleitor. Além disso, os votos que são ambíguos não devem ser contados.

REQUISITO I (A APURAÇÃO É PÚBLICA)
A apuração dos votos acontece numa sessão pública e é verificável.
Explicação: Para maior credibilidade do resultado, é importante que representantes dos partidos e observadores neutros estejam presentes e possam verificar o processo.

REQUISITO J (DIREITO DE AUDITAR)
Deve ser possível auditar a contagem.
Explicação: nas eleições de papel convencional, um candidato ou partido pode contestar o resultado e solicitar uma recontagem dos votos, que também acontece em uma sessão pública. Em princípio, esse processo deve convergir para um resultado com o qual todos concordam.

Na prática, as coisas são mais complicadas: um perdedor pode preferir solicitar diversas recontagens em vez de admitir a derrota. Algumas regras geralmente são implementadas para limitar esse efeito. Outro problema é que a contagem manual é notoriamente pouco confiável: não é incomum que uma segunda recontagem dê um terceiro valor, em vez de confirmar um dos dois primeiros; portanto, nenhuma convergência ocorre.

De fato, recontar não é a propriedade crucial. Pode-se imaginar que uma sessão de contagem seja completamente filmada no vídeo de forma que qualquer disputa possa ser resolvida através das imagens gravadas, visualizando-a novamente, e não por outra recontagem. Então, o que está em jogo é o requisito de auditabilidade e não a recontagem, o que na verdade é apenas uma possível implementação da auditoria.

Simplificando os requisitos de segurança

É interessante observar que todos esses requisitos poderiam ser simplificados em apenas dois requisitos:

(I) Preencher a cédula deve ser um ato confidencial, o que significa que nenhuma informação vinculando um eleitor a uma cédula pode ser vazada.

(II) Tudo o que não contradiz Requisito (I) deve ser transparente.

Isso é muito sucinto, provavelmente sucinto demais para ser útil na prática. Porém, é uma observação interessante, uma vez que indica o que é essencial do ponto de vista da segurança; às vezes serve como um princípio orientador na grande variedade de requisitos para eleições justas.

Conclusão

Neste capítulo estabelecemos uma lista de dez Requisitos aos quais uma eleição justa deve atender. No próximo capítulo discutimos como as mudanças nas tecnologias eleitorais têm impacto na questão de transparência e verificabilidade.

Anotações

[a] A abordagem e estrutura deste capítulo é parecida com as utilizadas no [10] e [3], e alguns trechos foram copiadas literalmente.

[b] Veja [9].

[c] Para detalhes veja https://www.researchgate.net/publication/299424370_Crowdsourced_integrity_verification_of_election_results_An_experience_from_Brazilian_elections; http://www.vocefiscal.org

[d] http://www.tse.jus.br/eleicoes/eleicoes-2016/qr-code-no-boletim-de-urna-manual-para-a-criacao-de-aplicativos-de-leitura

Capítulo 3

Transparência no processo eleitoral

O que é transparência

À mulher de César não basta ser honesta, tem de parecer honesta.

A um sistema eleitoral não basta ser correto, tem-se que provar que é correto e auditável. Ou, conforme abordamos na Introdução, um sistema eleitoral não deve apenas convencer a maioria da população de quem ganhou, mas **provar** aos candidatos perdedores que perderam.

Para explicar a noção de transparência, damos primeiro um exemplo num contexto diferente. Quem paga em dinheiro vivo pode simplesmente contar o dinheiro, depois entregar à outra parte, que conta o dinheiro e concorda ou não. Porém, quando se trata de uma quantia elevada, é melhor que uma das partes pegue o dinheiro e o coloque na mesa ou balcão de maneira que o outro possa facilmente conferir se a quantia está certa, por exemplo agrupando as notas em grupos que somam 100 reais. Assim, disputas podem ser resolvidas facilmente, porque é mais fácil descobrir e apontar onde está o erro. Na realidade, quem age de forma transparente está dizendo o seguinte: você não precisa confiar em mim, use seus próprios olhos e ouvidos e convença-se de que estou sendo honesto com você.

Consideramos a segunda maneira de executar a transação mais *transparente*, porque *a parte passiva é capaz de acompanhar o processo com facilidade e pode se convencer de que ele é executado de maneira honesta*. Adotaremos isto como nossa definição de transparência.

Uma eleição serve para determinar a vontade do povo, assim dando a legitimidade aos candidatos eleitos para assumirem seus cargos. Ou seja, para uma democracia é de suma importância que as eleições tenham credibilidade em todos os seus aspectos. Portanto, é desejável executar as eleições de uma forma transparente, porque aumenta sua credibilidade.

Em eleições com cédulas convencionais já existem costumes e cerimônias associados à transparência:

- Antes do início, se mostra que a urna está vazia;
- Observadores podem assegurar a integridade da urna durante a eleição;
- A apuração dos votos acontece em sessão pública;
- As cédulas são mostradas para que todos possam ver.

Também é costume registrar minuciosamente o que acontece, para que no caso de um recurso, tal como um pedido de recontagem, seja possível reconstruir o que aconteceu. Dizemos que um processo é *publicamente auditável* quando vários registros de eventos são guardados, garantindo que posteriormente seja possível verificar se o processo funcionou corretamente, ou se houve um erro.

Comprovação física do voto

Numa eleição tradicional com cédulas em papel, o que convence o eleitor que sua cédula está contida no conjunto de cédulas serem apuradas é a noção de senso comum de que um objeto (a cédula) depositado num lugar (a urna) continua lá e não desaparece sozinho. O eleitor pode depositar sua cédula, aguardar o encerramento da votação e testemunhar a apuração dos votos. Então a lisura da apuração depende dessa propriedade física.

Usando papel, um risco quando pessoas escrevem o nome do candidato é a de ambiguidade. Por esse motivo foram inventados cédulas padronizadas, em que o eleitor precisa marcar um quadradinho em frente do nome do candidato para votar. Este tipo de cédula é conhecido como a cédula australiana.[(a)]

A humanidade nem sempre usou papel para esta comprovação física. Por exemplo, os gregos tiveram um processo para expelir um cidadão de Atenas por dez

anos, no qual se usava fragmentos de cerâmica, disponível em abundância, para anotar o voto. A palavra grega para estes fragmentos é *ostrakon*, o que deu origem ao verbo inglês *to ostracize* (expelir).[(b)]

Tecnologias eleitorais não são iguais nas suas capacidades de capturar e guardar a vontade do eleitor. Em algumas tecnologias, a vontade do eleitor é 'gravada' e guardada numa forma física que é impossível de reverter. Por exemplo, os cacos de cerâmica (ostrakon); as marcas de um lápis numa cédula convencional; uma perfuração no papel, ou a tinta num papel. Isto é chamado *comprovação física do voto*, e a sua existência possibilita uma recontagem. Ela torna o processo auditável.

Em outras tecnologias esta comprovação física do voto não existe. O voto do eleitor já é contabilizado imediatamente no momento da votação, ou seja, o voto é adicionado ao registro (mecânico ou eletrônico) do candidato correspondente, mas não há um registro independente do voto.

No caso de eleições usando máquinas mecânicas, não existe uma cédula. O eleitor aperta alguns botões que representam seu voto. Depois, aciona uma alavanca para confirmar seu voto, e mecanicamente o voto é totalizado. Por exemplo porque uma roda dentada, agindo como contador, avança uma posição. Esta tecnologia não fornece transparência: não é possível verificar se alguém mal-intencionado é capaz de modificar um voto, convencer-se que o voto pertence ao conjunto, ou recontar os votos. O eleitor deve ter fé na tecnologia empregada, e confiar que ela forneça estes requisitos.

Sistemas de votação eletrônicas, como a urna brasileira, já foram chamados 'a versão eletrônica de máquinas de alavanca'.[(c)] Tampouco há uma cédula, e eles têm as mesmas propriedades de segurança que os sistemas mecânicos. Na verdade, pior. Com máquinas de alavanca é preciso acesso a todas as máquinas para fraudar; num sistema eletrônico apenas acesso ao código fonte é suficiente. Veja pg. 35.

Conclusão

Em muitos sistemas de votação tradicionais sempre existia uma comprovação física da vontade do eleitor. Novas tecnologias facilitam a confiabilidade e rapidez de uma eleição, mas ao mesmo tempo eliminam essa comprovação física, levando a sistemas que não são auditáveis.

Anotações

[a] https://www.britannica.com/topic/Australian-ballot

[b] https://en.wikipedia.org/wiki/Ostracism

[c] Américo Monteiro, Natércia Soares, Rosa Maria Oliveira e Pedro Antunes, *Sistemas Electônicos de Votação*, Relatório Técnico TR-01-9, Departamento de Informática, Universidade de Lisboa, 2001

Capítulo 4

O sigilo do voto violado

A identificação do eleitor

Um ingrediente essencial de qualquer eleição é a identificação do eleitor antes de permiti-lo a depositar o voto. Isso corresponde aos Requisitos 1 e 2, que rezam que apenas pessoas autorizadas, chamadas eleitores, podem votar, e apenas uma única vez.

Tradicionalmente o eleitor se identifica perante a mesa mostrando o seu título de eleitor. Antes, a mesa tinha uma lista impressa com todos os eleitores daquela seção. Hoje, além da lista impressa, a urna tem uma cópia desta lista armazenada na sua memória. Um mesário digita o número do título e a urna é liberada para votar, desde que este número conste na lista interna.

Aqui, a preocupação principal é a fraude eleitoral cometida ou facilitada pelos mesários. Por exemplo, imagine uma seção eleitoral pequena no meio do sertão, onde a maioria dos eleitores já votou na parte de manhã. Durante 30 minutos na parte da tarde não há nenhum eleitor aparecendo na seção eleitoral. Mesários criativos poderiam aproveitar deste período de seguinte maneira: eles apostam que vovô, de 77 anos, não vai comparecer para votar, ainda porque o voto acima de 65 não é obrigatório. Então eles vão liberar a urna e votar no lugar dele, usando sua identidade. E assim por diante, votando em nome de eleitores na lista que ainda não votaram e provavelmente não vão aparecer. E se, porventura, vovô aparece, os mesários usam a identidade de um outro eleitor que ainda não votou para liberar a urna.

É por este motivo que o TSE introduziu a biometria, liberando a urna apenas quando há uma identificação positiva de um eleitor.

Na verdade, a biometria nunca é perfeita e existe uma chance de aproximadamente 2% de um eleitor legítimo não ser reconhecido pela urna.[a] Para estes casos o presidente da mesa tem o poder de desativar a biometria e liberar a urna para que o eleitor possa votar.

Este procedimento poderia ser utilizado como forma de fraudar também, mas é evidente que quando nos arquivos log da urna existem 6 desativações da biometria, entre 15h30 e 16h00 no dia de votação, que isso é extremamente suspeito e há um indício forte de que está havendo fraude. No mínimo seria prudente trocar os mesários para a eleição seguinte.[b][c] No entanto, o TSE informou que existem poucos casos deste tipo de fraude.[d]

Em resumo, considerada isoladamente a biometria melhora a identificação do eleitor. Então, em comparação com uma eleição com cédula em papel, a urna atende melhor aos Requisitos 1 e 2.

Porém, a dificuldade é que a identificação do eleitor está fisicamente integrada com o processo de votar, já que ambos usam o mesmo dispositivo. Isso é problemático, como veremos na próxima seção.

O sigilo do voto violado

A maior falha de segurança da urna é tão óbvia que nem é necessário muito esforço para explicar.

O problema é que o equipamento que o eleitor usa para votar é o mesmo usado para identificar o eleitor. Mais especificamente, a urna é um equipamento internamente equivalente a um PC, mas com dois monitores e dois teclados de padrão diferente. Um teclado é aquele onde o eleitor digita seu voto; o outro teclado é conectado à urna através de um cabo de 5 metros, usado pelo mesário para liberar a urna para o próximo eleitor, digitando o seu número de título de eleitor.

Um agente malicioso poderia facilmente modificar o software da urna de forma que os dados de identificação do eleitor serão vinculados ao voto digitado. Um programa com essa funcionalidade poderia ser colocado em várias camadas de software diferentes. Por exemplo, um *key logger* é um programa que armazena

cada tecla digitada no teclado. Tendo dois *key loggers*, um para o teclado de identificação e um para o teclado de votação, seria possível pegar os dois arquivos log gerados e cruzar os dados, descobrindo quem votou em quem. Repare que isso também seria possível se autenticação e votação fossem em dois equipamentos diferentes. Incluir um sistema de identificação na urna que impossibilita este cruzamento é delicado.

Em termos de segurança isso é um pecado mortal. Não estamos alegando que este tipo de cruzamento está acontecendo, mas o projeto da urna nem deveria permitir este tipo de ataque, em hipótese alguma.

Não existe sistema eleitoral algum no mundo que tem essa característica, pois seria declarado inconstitucional. O sensato é separar a identificação do eleitor completamente do ato de votar, em sistemas convencionais com cédula de papel: o eleitor se identifica, e depois tem, de forma anônima, acesso a um sistema diferente para emitir seu voto.

Ao integrar essas duas funcionalidades num único dispositivo jogou-se fora o voto secreto. E o mero fato da urna permitir, em hipótese, a existência de software que vincule votos a eleitores desqualifica o projeto da urna completamente.

Quando eu relato essa característica da urna brasileira a um especialista em tecnologia eleitoral no exterior ele reage chocado, ou começa a rir em descrença.

Essa falha de segurança já foi comunicada ao TSE em 2002. O texto da Seção 3.3 (pg. 20) do RelSBC é:

> **3.3 Vincular o Voto ao Eleitor**
>
> O presidente da mesa digita o título do eleitor num equipamento chamado *micro-terminal* fisicamente conectado à urna. Com isto é muito simples relacionar eleitores aos votos. É só registrar, em separado, as teclas do micro-terminal e da urna. Contudo, trata-se somente de uma possibilidade. Em nossas investigações não foi encontrado qualquer vestígio desta possibilidade ter sido implementada. No entanto, este é um desconforto que o eleitor não precisaria ter.

E na seção Considerações Finais do mesmo documento consta o seguinte trecho:

> **(3) O projeto da urna não elimina a possibilidade de que a identidade do eleitor seja vinculada a seu voto.**
>
> Como foi explicado em 3.3, para registrar quem votou, o título do eleitor é digitado num equipamento que está eletronicamente ligado à urna. Já que o eleitor usa a urna para votar, uma mudança simples de software permitiria vincular a identidade do eleitor a seu voto, o que fere o sigilo do voto. Não foi encontrado qualquer vestígio desta vinculação ter sido implementada. No entanto, acreditamos que o registro de quem votou deva ser implementado de uma forma diferente.

Conclusão

A urna brasileira não elimina rigorosamente a possibilidade de que um voto seja vinculado a um eleitor, e neste sentido viola o Requisito C: o sigilo do voto. Também viola Artigo 14 da Constituição.[e]

Anotações

[a] Entender a taxa de erro de sistemas biométricos não é algo simples. Existe a *false acceptance rate* e *false rejection rate* que têm uma relação adversarial: diminuir uma aumenta a outra. Este fenômeno não é um problema de engenharia, mas consequência das leis de probabilidade conhecido como a *base rate fallacy*, que faz que diminuir a taxa de erro abaixo de 2% é quase impossível. Veja por exemplo *Performance evaluation of fingerprint verification systems* http://ieeexplore.ieee.org/document/1542027/

[b] http://politica.estadao.com.br/noticias/geral,tse-pede-a-pf-e-procuradoria-investigacao-sobre-falha-em-40-mil-votos-de-2014,10000056311

[c] http://www.brunazo.eng.br/voto-e/textos/urnas-b2.htm

[d] Comunicação pessoal, 6 de novembro 2017

[e] https://www.senado.gov.br/atividade/const/con1988/con1988_08.09.2016/art_14_.asp

Capítulo 5

A corretude do software – a discussão errada

Numa votação com papel, quando um eleitor atento deposita sua cédula preenchida na urna, ao soltá-la ele pode pensar: "O que acontece agora com minha cédula?" Se a urna fosse feita de material transparente ele poderia vê-la. E talvez o eleitor possa ficar até o fim da eleição no local da votação, vigiando a integridade da urna e assistir à apuração dos votos. Dessa forma ele teria certeza absoluta que seu voto foi incluído.

E numa votação eletrônica? O eleitor aperta CONFIRMA e aparece a palavra "FIM". Mas como ele sabe se sua cédula foi incluída na apuração e que seu voto realmente conta? Pior: numa votação eletrônica não existe uma cédula.

Esta é a sensação da caixa preta: o eleitor não sabe como seu voto é processado. O sistema é fechado, e o eleitor tem que confiar cegamente no sistema eleitoral. Em particular, o eleitor depende da corretude do software da urna.

Portanto, muitas vezes a pergunta se a urna é segura se reduz à questão dos softwares da urna serem corretos ou não. Esta questão é como areia movediça, quanto mais você estuda, mais complicado se torna o assunto. Quem tiver interesse pode consultar Capítulo 3 do RELSBC; aqui eu vou dar apenas um resumo, por dois motivos.

Primeiro, é uma discussão muito técnica, apenas interessante para especialistas. Portanto está fora do escopo deste livro. Segundo porque, no final, eu acho a questão da corretude do software irrelevante. Porque ela tira o foco de uma

questão mais importante: a falta de transparência da urna. Este é o ponto principal deste capítulo e deste livro.

Fraude de varejo vs. fraude de atacado

Anteriormente, se alguém quisesse fraudar as eleições teria que modificar muitos equipamentos. Quando se faz as eleições usando um computador, é somente modificar o software. Nas palavras do Prof. Avi Rubin (veja [7], pg. 37; tradução nossa):

> Com tecnologias de votação mais tradicionais, como máquinas de alavanca ou máquinas que escaneiam a cédula[(a)] ou cédulas de cartão de perfuração, alguém que queira fraudar uma eleição deve comprometer cada máquina individualmente. Chamamos isto *fraude de varejo*. Exige um considerável acesso físico e esforço, e o risco de ser capturado aumenta com cada instância de adulteração. Em contrapartida, a capacidade de corromper várias máquinas em vários locais ou influenciar os resultados agregados de várias máquinas com uma única ação, constitui o que chamamos de *fraude de atacado*, onde o menor esforço causa o maior dano. A votação sem papel baseada em software torna a fraude de atacado possível.

Não existe segurança através de software

Se você tem uma plataforma computacional a qual o adversário tem acesso, não é possível garantir a integridade do software; sempre será possível que o dispositivo seja hackeado.

Por exemplo, num sistema com cédula em papel o presidente da mesa mostra que a urna está vazia. Da mesma forma é necessário mostrar que o equipamento que conta os votos está no seu estado inicial. Num sistema de votação mecânica, verifica-se que todos os contadores estão na posição que representa não haver votos. Num sistema de votação eletrônica os valores armazenados nos registros que representam o número de votos por candidato são impressos. No Brasil este relatório é chamado de *zerésima*.

No entanto, num sistema de votação eletrônico, quem garante que o relatório impresso representa o verdadeiro estado daqueles registros? Se alguém quisesse fraudar, não seria um dos primeiros passos criar um arquivo falso, de zerésima, garantindo sua impressão quando fosse solicitado, independente do verdadeiro estado da máquina?

É claro que nesse tipo de fraude há mudanças de alguns arquivos: foi colocado um arquivo a mais (contendo a zerésima pré-construída), e foi mudado o programa atendendo à solicitação de impressão da zerésima.

Então, para dificultar esse ataque, podemos escrever um meta-programa, que tem como tarefa verificar a integridade de todos os arquivos, por exemplo comparando os resumos criptográficos calculados com os valores armazenados no equipamento. Teoricamente esse esquema descobre qualquer modificação em um dos arquivos, dificultando a modificação dos programas.

Mas e se alguém consegue modificar esse meta-programa? Modificações, por exemplo, podem fazer com que o meta-programa nunca reclame sobre discrepâncias entre os resumos criptográficos ou mesmo emita um resumo criptográfico padrão para um determinado arquivo. Na realidade, para quem já sabe como modificar programas executáveis, não é muito difícil achar a função responsável pela comparação dos resumos criptográficos calculados com os valores armazenados. Tampouco é complicado descobrir o comando onde se faz essa comparação; deve ser algo parecido com:

```
SE (res_calculado==res_armazenado) continuar;
SENÃO abortar;
```

e tampouco é complicado modificar nela a condição para sempre ser verdade:

```
SE (TRUE) continuar;
SENÃO abortar;
```

Não será na linguagem de programação *C*, claro. É preciso conhecimento de *assembly*, a linguagem de mais baixo nível com instruções de processador.

Podemos até pensar em técnicas criptográficas mais avançadas, mas o problema é que não é claro que elas resolvem todos os possíveis ataques no nível mais baixo de software: firmware, BIOS, sistema operacional, drivers, etc. O tamanho dos softwares da urna é vasto, estima-se que existam mais que 13 milhões linhas de código fonte na urna.[(b)(c)]

A conclusão é que essas técnicas apenas dificultam ataques e aumentam a integridade, mas nunca os impossibilitam completamente. Para qualquer providência em software contra fraude, é sempre possível conceber um contra-ataque que o burle. Por isso, basear a segurança de um sistema eleitoral apenas no software é um caminho inviável. Abrir o código-fonte não resolveria o problema, porque com uma quantidade enorme do código-fonte fica impossível *provar* que o executável corresponde ao código-fonte, e que não há um software malicioso no equipamento que gera e soma os votos. Pelo mesmo motivo, usar software livre ou aberto não resolve esta questão, mas ajudaria para melhorar a qualidade do software e daria credibilidade ao processo eleitoral.

A impossibilidade de detectar erros e fraude

A seção anterior foi em grande parte tirada do RELSBC, escrito em 2002. Em 2006, pesquisadores do *National Institute of Standards and Techology* dos EUA relataram os problemas assim[(d)] (tradução nossa):

> **Incapacidade de testar sistemas complexos para erros e fraudes**
>
> A necessidade de independência de software [explicada na próxima seção] em sistemas de votação baseia-se na incapacidade, num sentido prático, de testar sistemas complexos para erros e fraudes intencionalmente introduzidas. Os especialistas em desenvolvimento de software rejeitam a eficácia de um processo de desenvolvimento mesmo bastante rigoroso, com revisões e testes para encontrar ou prevenir erros e códigos intencionalmente maliciosos nos sistemas de votação de hoje. Os sistemas de votação estão aumentando em complexidade à medida que são adicionados mais recursos, por exemplo, funções de acessibilidade. Além disso, os sistemas de votação geralmente utilizam produtos COTS [Common Off-the-shelf] que são muito complexos, como Microsoft Windows CE e Embedded XP. Testar sistemas de votação atuais e futuros para um alto grau de segurança seria extremamente caro e provavelmente não seria econômico para um fornecedor.

O parágrafo seguinte apresenta uma medida de segurança interessante: quantas pessoas precisam conspirar para fraudar uma eleição. Usa pela primeira vez o termo *DRE*, sigla para *Direct-Recording Electronic (DRE) voting machine*, ou seja,

um dispositivo que registra (armazena) os votos apenas na memória. Repare que, em geral, os *DREs* **não** realizam a identificação do eleitor (como é o caso no Brasil; pg. 31); ela é feita de forma independente, e o eleitor tem acesso ao *DRE* anonimamente.

> No entanto, persistem os argumentos de que a maioria dos erros são capturados pelo teste e que a fraude intencional nunca foi nem será uma questão importante na segurança do sistema de votação. Análises de segurança propuseram que uma medida útil da segurança de um sistema de votação é o tamanho da conspiração necessária para 'burlar' uma grande eleição, ou seja, quanto maior a conspiração necessária, mais seguro será o sistema. Uma abordagem dependente do software, como o DRE, não oferece capacidade alguma independente para detectar se a fraude causou ou não erros nos registros. Em princípio, um único programador inteligente e desonesto que trabalha em uma empresa de máquinas de votação poderia burlar uma eleição em todo um estado, se esse estado usar principalmente um único tipo de sistema (apenas 4 vendedores de sistemas de votação têm uma participação de mercado significativa nos EUA).

E continua, refutando argumentos muito similares àqueles usados pelo TSE:

> Os argumentos para refutar essa tese se concentram geralmente nas seguintes afirmações:
>
> 1. Não há evidências de códigos maliciosos intencionalmente introduzidos ou fraude nos sistemas de votação,
>
> 2. Os procedimentos eleitorais são eficazes para manter os sistemas de votação livres de fraude introduzida intencionalmente, e
>
> 3. O teste atual dos sistemas de votação é adequado para descobrir código malicioso.
>
> As afirmações 1 e 2 não se sustentam diante da enorme evidência de fraude de computador que ocorre em outras áreas da TI [tecnologia da informação] e que já ocorre ou provavelmente ocorrerá em sistemas de votação, dados os bilhões de gastos em eleições, bem como a rica história de fraude eleitoral. Se um sistema de votação dependente do software, como o DRE, não pode ser testado para determinar se o código malicioso existe ou se uma fraude ocorreu, então não se pode argumentar que não ocorreu e que os procedimentos eleitorais são efetivos para impedir isso. O que resta

> [como método] são estimativas sobre se a fraude ocorreu, como as pesquisas pré e pós-eleitorais em comparação com os resultados das eleições. Mas e se os resultados forem diferentes? Se não houver apelação exceto recontar os registros eletrônicos do DRE, simplesmente não há apelação. No entanto, as eleições não deveriam depender de estimativas como estas.
>
> No que diz respeito à afirmação 3, foram feitas muitas evidências de que os sistemas de votação em geral não são desenvolvidos de acordo com modelos rigorosos de desenvolvimento de código seguro nem testados com o rigor de outras aplicações críticas para a segurança. Os especialistas rejeitam que mesmo essas medidas seriam suficientes para detectar de forma confiável todos os erros ou códigos maliciosos ocultos em sistemas de votação. Vários estados [dos EUA] expandiram seu escrutínio e teste de sistemas de votação.

(In)dependência do software

Para destacar ainda mais a questão de falta de transparência em sistemas eleitorais parecidos com a urna, os pesquisadores Rivest (do MIT) e Wack (do NIST) introduziram, em 2006, a noção de independência do software (*software independence*)[(e)], que essencialmente diz que o resultado de uma eleição não pode depender unicamente da corretude do software.

Mais especificamente, a definição apresentada pelos autores é assim: "Um sistema de votação é independente do software se uma mudança ou erro não detectado em seu software não pode causar uma mudança ou erro indetectável em um resultado eleitoral. Um sistema de votação que não é independente de software é dito dependente de software, ou seja, em certo sentido, é vulnerável a erros de programação, códigos maliciosos ou manipulação de software não detectados, portanto, a corretude dos resultados das eleições depende da corretude do software". Portanto, a urna é dependente de software.

Em seguida, os autores explicam a motivação por trás desta definição:

> Para ilustrar o raciocínio da independência do software, podemos executar alguns 'experimentos mentais'. Posicione-se no lugar de um adversário e imagine que você tenha o poder de substituir em segredo qualquer software existente usado pelos sistemas de votação por software do qual você

> detenha o controle da construção (você pode assumir que você tem o código-fonte para o software existente).
>
> Com tal habilidade, você (como o adversário) pode mudar um resultado eleitoral ou 'burlar uma eleição' sem risco de detecção?
>
> Se assim for, o sistema depende do software – o software é um 'calcanhar de Aquiles' do sistema de votação. Corromper o software dá a um adversário o poder de fraudar secretamente e silenciosamente uma eleição.
>
> Caso contrário, o sistema é independente de software – o sistema de votação como um todo (incluindo os componentes não-software) tem redundância suficiente e potencial para verificação cruzada de que a má conduta do software pode ser detectada. A detecção pode ser feita pelo eleitor, por um funcionário eleitoral ou técnico, por um auditor pós-eleitoral, por um observador ou por algum membro do público. (Na verdade, qualquer um, exceto o adversário.)
>
> Nessas 'experiências mentais', estamos considerando o adversário como um agente maligno que poderia carregar software fraudulento em sistemas de votação. De forma mais realista, podemos considerar este adversário como uma abstração das limitações do processo de desenvolvimento de software e do processo de teste. (Como tal, para determinar se um sistema é independente do software, deve-se presumir que os erros do software estavam presentes quando o software foi escrito e não foram capturados pelos processos de controle de desenvolvimento de software ou pelo processo de certificação.)

Outra forma de visualizar esta situação é imaginar que há um diabinho dentro do sistema que gosta de fazer zombarias com o desenvolvedor do sistema. Um sistema que não deixa nenhuma liberdade ao diabinho para corromper seu funcionamento correto é independente de software.

Hardware seguro

Para sair deste dilema, o TSE optou por usar um hardware seguro a partir de 2010. A ideia é que na urna haja um componente que executa determinados programas apenas quando eles são assinados digitalmente. Este tipo de tecnologia já existia, e foi aprimorada através de uma colaboração entre três pesquisadores da UNICAMP, um da empresa Kryptus, e dois do TSE para desenvolver tal componente

especificamente para DREs [4].

Conheço pessoalmente todas as pessoas de Campinas porque nós trabalhamos junto num projeto no passado(f), considero duas delas meus amigos, e tenho confiança total nelas.

Mesmo assim, eu não concordo com esta abordagem. Aquele componente usa técnicas de engenharia elétrica que são fora da minha área de competência. Então, apesar de ser especialista em votação e certificação digital, eu sozinho não consigo entender aspectos cruciais do artigo que descreve esta tecnologia.

Portanto, a minha confiança nesta tecnologia seria 'por associação'; seria porque eu conheço pessoalmente essas pessoas e confio nelas. Mas não seria por convicção própria. Como isso fica para um cidadão comum, sinceramente preocupado com seu voto?

E no que este componente adianta? Como um eleitor tem certeza que, no dia da eleição, a urna na sua frente contém este componente e que está cumprindo seu papel?

Ou seja, mesmo que o hardware seguro resolvesse o problema e garantisse a corretude dos programas, eu seria contra esta abordagem por motivos filosóficos. Esta abordagem não permite ao eleitor convencer-se que seu voto será incluído e apurado. Portanto, ela não resolve a questão da percepção da caixa preta, e nunca leva a um sistema mais transparente.

A próxima seção aprofunda este argumento, enquanto mais tarde neste capítulo relatamos que supremo tribunal constitucional de Alemanha rejeitou o princípio de 'confiança por associação' no caso de eleições.

A discussão errada

Desde o início da urna, a questão da corretude do software foi criticada. (Estou falando da urna sem voto impresso, que será discutido no próximo capítulo.) Estas críticas levaram a uma série de melhorias:

1. Verificação das assinaturas digitais dos códigos na urna (2002; veja pg. 36);

2. Registro Digital de Voto (2004; veja pg. 53);

3. Hardware seguro (2010; veja a seção anterior)

4. QR-Codes (2016; veja pg. 20).

Simplificando um pouco, pode se dizer que começou um jogo de gato e rato, onde o rato sempre consegue burlar as medidas de segurança implementadas pelo gato. Simplificando ainda mais, surgiu o seguinte diálogo entre o TSE e uma parte da sociedade:

- TSE: "A urna é segura."
- Sociedade: "Não é verdade."
- TSE: "Então prova o que você disse."

Este é um diálogo que o TSE não tem como perder, porque ele detém todas as informações sobre os detalhes técnicos, e ele sempre pode alegar que, por motivos de segurança ou para proteger a propriedade intelectual, determinados detalhes não podem ser revelados. É um jogo assimétrico, já que todas as cartas estão nas mãos do TSE.

Mas na minha opinião, esta discussão está completamente equivocada.

Não cabe à sociedade descobrir o que está errado com a urna. Cabe ao TSE demonstrar que a urna implementa eleições justas, seguindo os critérios elaborados no capítulo 2 na página 21. O ônus da prova está com o TSE, não o contrário.

Não adianta o TSE ser capaz de convencer a si mesmo que a urna é segura, mesmo que utilize ajuda de especialistas na área. A percepção da população é que a urna é uma caixa preta; a psicologia está errada. Se o TSE deseja credibilidade da urna, ele deve oferecer uma urna transparente, publicamente auditável e verificável.

Porém, o grande problema da urna atual é que ela não é transparente; ela nunca foi projetada para ser. Ela foi projetada a partir de uma filosofia militar, onde a segurança é garantida mantendo aspectos cruciais em sigilo, no ramo conhecida como "segurança por obscuridade"o que não é considerado uma boa prática. Para uma eleição, o processo primordial de uma democracia, obscuridade não é aceitável. E o fracasso desta filosofia foi dramaticamente mostrado diante da impotência do TSE em provar ao PSDB, em 2014, que seu candidato, Aécio Neves, perdeu as eleições. Houve uma auditoria, mas sem possibilidade de recontar os votos ela se torna uma farsa.

A transparência atual é insuficiente

O TSE alega que a transparência da urna atual é suficiente. Eu discordei em 2002, e continuo discordando. No fundo, o argumento pode ser resumido muito simples: o holandês prof. Edsgar Dijkstra, eminente pesquisador em computação, já argumentou que testes apenas podem provar a presença de erros, mas nunca sua ausência.[g]

Repito aqui, integralmente, o quarto item das Considerações Finais do RelSBC:

> **(4) A transparência e a auditabilidade da urna deixam a desejar.**
>
> No inicio, a segurança da urna se baseou em técnicas clássicas, principalmente separando as funcionalidades dos subsistemas, e as responsabilidades dos funcionários envolvidos.
>
> Para nós é óbvio que ultimamente o TSE está mais aberto, que ele realmente quer convencer terceiros de que o sistema eleitoral brasileiro é seguro. Observe-se que o TSE tem esta obrigação para com os partidos políticos e a sociedade em geral. Infelizmente, achamos que os mecanismos oferecidos não são suficientemente convincentes.
>
> Os principais mecanismos de auditoria à disposição dos partidos políticos são:
>
> **(a)** sessões abertas, em que o TSE mostra seus programas, tanto os da urna, quanto os da totalização;
>
> **(b)** um sistema de resumos criptográficos e assinaturas digitais, para demonstrar que os arquivos mostrados na sessão correspondem aos usados no dia de eleição;
>
> **(c)** a impressão da zerésima (um relatório que mostra que todos os candidatos têm zero votos) da urna e do sistema de totalização no início da votação;
>
> **(d)** a impressão do boletim da urna, quando esta for encerrada;
>
> **(e)** a divulgação por CD de todos os dados (votos por candidato, etc.) de todas as urnas pelos TREs;
>
> **(f)** a votação paralela (Um dia antes da eleição, em todos os Estados, duas urnas são sorteadas, lacradas e transportadas ao TRE. No dia da eleição, numa sessão aberta e gravada por vídeo, simula-se uma votação nelas em que todos os votos são escolhidos pelos fiscais e testemunhas e são

abertos. Depois, confere-se o resultado emitido pela urna, que deve corresponder à contagem manual.);

(g) a impressão do voto.

Com exceção do último item (a impressão do voto), nenhum destes mecanismos vão convencer um cético uma vez que:

(a) (sessões abertas): Primeiro, a quantidade de software da urna é enorme– tão grande que é impossível estudar tudo durante uma semana. Segundo, o sistema operacional não foi mostrado. Infelizmente, como foi explicado em 3.6 [do mesmo relatório], ataques no nível de sistema operacional apresentam uma ameaça real. Terceiro, mesmo se tudo fosse mostrado, seria muito difícil excluir com certeza a possibilidade de que houvesse um programa malicioso escondido em algum lugar. Um pequeno arquivo de alguns kilobytes seria suficiente para quebrar a integridade da urna;

(b) (resumos criptográficos dos arquivos) Primeiro, como ter certeza de que o programa que calcula os resumos faz realmente o que foi especificado, em particular durante a verificação dos resumos na urna? Segundo, como foi mencionado em 3.5.2 [do mesmo relatório], o trabalho de verificação é lento e trabalhoso, e a amostragem é apenas uma fração mínima do total. Aliás, durante o segundo turno, os resumos publicados na página do TSE foram mudados, dificultando o trabalho dos partidos. Terceiro, mesmo que todos os arquivos fonte do ambiente de desenvolvimento sejam iguais aos mesmos da urna, como ter certeza que eles serão realmente executados no dia de eleição?

Ressaltamos que o que estamos colocando aqui são ataques hipotéticos que, ainda por cima, muitas vezes implicam a conivência de um ou vários funcionários da Justiça Eleitoral. Não estamos dizendo que estes ataques existem de verdade, ou que já foram realizados alguma vez. O que queremos dizer é que não existem mecanismos efetivos que permitam aos partidos políticos verificarem que a eleição ocorreu de uma maneira honesta. Existe uma zona cinza em que, no final das contas, todo partido político (e todo cidadão) precisa ter fé na Justiça Eleitoral e em seus funcionários. Apesar de termos toda confiança neles, temos a opinião de que a existência desta zona, em princípio, é errada.

(c), (d), (e) (zerésima e boletim da urna) A combinação de (c), (d) e (e) dá uma grande confiabilidade ao processo de totalização: os partidos

políticos podem obter um grande número de boletins da urna. Além disso, os partidos podem verificar que os dados, tal como divulgados pelo TRE, correspondem aos dados em todos os boletins obtidos, e que os totais foram calculados de forma certa. Obviamente, cada diferença seria uma indicação de um problema grave. Na prática, esta parte já funciona razoavelmente bem. Contudo, propusemos em 3.5.5 [do mesmo relatório] uma mudança simples que facilitará muito o trabalho de fiscalização pelos partidos;

(f) (votação paralela): A votação paralela perde um pouco em credibilidade, porque o sorteio acontece no dia anterior ao da eleição. Teoricamente, pessoas maliciosas podem esperar até sábado de manhã antes de começar a adulterar a urna. Porém, confiscar uma urna e executar uma votação paralela no dia de eleição é logisticamente muito difícil em estados muito grandes. Os ataques em que a urna sabe distinguir entre uma votação de verdade e uma simulação, como explicado [num email do Prof. Stolfi; referência no texto original], não são nossa primeira preocupação.

A urna na Alemanha

Na Alemanha aconteceu algo muito interessante. Um cidadão comum[(h)] contestou o uso da tecnologia similar à urna, por ser uma tecnologia que nem todo cidadão consegue entender. Perdeu em primeira instância, mas ganhou no supremo tribunal constitucional (*Bundesverfassungsgericht*). Incluímos aqui um breve relato tirado de [6], pg. 53 (tradução nossa):

A Natureza Pública de Eleições

A votação eletrônica; na verdade, qualquer tipo de ferramenta eleitoral eletrônica, envolve obscuridade para um leigo, e abordar essa barreira tornou-se um desafio para uma consolidação definitiva das tecnologias eleitorais. Se comparado a ferramentas baseadas em papel, evidências fornecidas de forma eletrônica podem ser sem sentido para um leigo, devido à sua complexidade técnica inerente. Enquanto uma recontagem de [cédulas em] papel pode ser entendida e monitorada por qualquer pessoa, uma recontagem informatizada pode fornecer figuras finais corretas, mas o procedimento só pode ser entendido por especialistas técnicos. *Essa opacidade inerente às fer-*

> *ramentas habilitadas de certo modo contradiz os pilares básicos das eleições, que sempre dependem da transparência e da supervisão pelos cidadãos [grifo nosso].*E é por isso que o uso de novas tecnologias para fins eleitorais provavelmente tem que abordar preocupações particulares que não estão presentes em outras áreas. Uma decisão do Tribunal Constitucional alemão em 2009 é considerada um marco. Teve um impacto direto nos subsequentes desenvolvimentos legais e nas implementações de votação eletrônica como a norueguesa, a estoniana e a suíça, que pretendem fornecer ferramentas melhores para verificar a eleição.
>
> Em março de 2009, o Tribunal Constitucional alemão proibiu as máquinas de votação que estavam em uso para as eleições federais. Foram máquinas fornecidas por Nedap, um fornecedor holandês cujos dispositivos também foram implantados na Holanda e na França. Além de outros processos anteriores que tiveram resultados diferentes [referência no texto original], este processo foi iniciado por Ulrich Wiesner e seu pai contra o governo federal nas eleições de 2005. Apesar do fato de que não houve grandes problemas durante o atual implementação de máquinas de votação, o processo destinou-se a desafiar a votação eletrônica como tal. Rejeitado pela Câmara [*Bundestag*] como "obviamente sem causa" [referência no texto original], o processo terminou com uma decisão notável da Tribunal Constitucional Alemão baseado na natureza pública das eleições. O Tribunal destacou que as máquinas de votação tinham uma falha inerente que não era vinculada com o desempenho real. Mesmo uma implementação bem sucedida de uma perspectiva técnica, esta não seria legalmente aceitável devido ao fato de que tais dispositivos não cumprem os principais princípios democráticos, a saber, aquele que prevê a supervisão dos procedimentos eleitorais por diferentes partes interessadas, sem conhecimento especializado necessário. Foi o que o tribunal alemão chamou de *natureza pública* de eleições: *"todo cidadão deve ter a capacidade de monitorar e entender, sem conhecimento técnico específico, os estágios centrais de uma eleição* (§109; Ver também §119, 148 e 149). Os especialistas em TI normalmente assumem estas tarefas importantes no papel de representantes [da sociedade], mas o Tribunal não aceitou procedimentos de confiança indireta.

Ou seja, a corte mais alta de Alemanha estabeleceu explicitamente a transparência do processo eleitoral e o direito de supervisão pelo cidadão. A tecnologia usada deve ser compreensível por um cidadão comum; delegar para um pequeno grupo de especialistas em TI não é aceitável. É surpreendente que o judiciário brasileiro,

que tanto preza a tradição jurídica alemã, em lugar nenhum leve este argumento em consideração.

A urna em outros países

Estados Unidos Tecnologia eleitoral nos EUA é o caos total, porque cada condado (município) tem autonomia sobre este assunto, naquela filosofia estadunidense na qual os estados desconfiam do governo federal. Ainda, cada estado tem leis diferentes e eleições diferentes. Por exemplo, além do presidente e governador, elege-se juiz, procurador, e vota-se pró ou contra o uso de maconha para motivos médicos.

Obviamente os condados não tem condições para desenvolver equipamento para votar, portanto eles são obrigados a comprar este tipo de equipamento no mercado. Consequentemente, a variedade de tecnologias empregadas no EUA deve ser maior do que no resto do mundo junto.

Um efeito colateral negativo é que os condados mais pobres tendem a ter uma tecnologia de qualidade inferior, causando filas maiores e mais falhas nas urnas no dia de votação. Isso faz que o voto do cidadão pobre, já sub-representado porque o voto não é obrigatório, e menos ouvido que o do cidadão que vota num condado rico. Comparando este aspecto, a experiência brasileira, com um sistema eleitoral único para o país todo, se sai muito vantajosa.

Em 2002 houve um escândalo porque uma equipe liderado por Prof. Avi Rubin de *John Hopkins University* mostrou que o software das máquinas da empresa Diebold era de baixíssima qualidade, e era muito fácil de modificá-lo e manipular os resultados [7]. Um resultado disso é que os DREs, ou seja máquinas de votação cuja segurança é unicamente baseado no software e sem comprovação física, foram proibidos em vários estados, como a Califórnia.

Índia O equivalente da urna indiana era um dispositivo extremamente simplório, e sua insegurança foi demonstrada por Hari Prasad, J. Alex Halderman e Rop Gonggrijp.

Holanda Na Holanda aconteceu algo parecido. O *stem-computer* (computador de votação) era a versão holandesa de um DRE. Não foi possível provar que o software estava correto, não houve comprovação física do voto. O juiz proibiu o

uso desta tecnologia e a Holanda voltou a usar cédulas em papel.[(i)]

Argentina Neste momento, há uma grande controvérsia em torno da votação eletrônica na Argentina.[(j)]

Em 2015, a Cidade de Buenos Aires implementou um novo sistema de votação em que as cédulas foram impressas em papel com um chip RFID embutido. Foram mostradas falhas de segurança neste sistema[(k)]levando a uma reação contra à votação eletrônica. Em 2016, após árduas discussões legislativas, o Congresso Nacional rejeitou a proposta do executivo nacional de implementar um único sistema de cédulas eletrônicas. Recentemente, um grande grupo de especialistas em informática das universidades nacionais falou contra a votação eletrônica[(l)] e convidaram a assinar na web uma adesão a tal rejeição.

Nas eleições de agosto de 2017, o sistema manual gerou muitas controvérsias, porque no maior estado argentino, a província de Buenos Aires, o partido oficial celebrou na televisão às 22 horas uma vitória em mais de sete pontos[(m)], mas no escrutínio definitivo finalizado duas semanas depois, o vencedor foi um partido da oposição.[(n)]

Neste momento, a votação eletrônica só se aplica a algumas eleições locais em certas cidades e contextos acadêmicos, por exemplo, algumas faculdades universitárias públicas.

Eleições hackeadas

O termo *election hacking* pode significar várias coisas, mas em geral se refere a qualquer interferência externa a uma eleição.

Recentemente saiu a notícia que vários DREs americanos foram hackeado no DefCon, o maior encontro mundial de hackers.[(o)] Isso não foi uma grande surpresa: a segurança destes equipamentos não é muito forte, mas demonstrar esse fato foi sempre protegido pela lei americana (o *Digital Millennium Copyright Act*) que proíbe a engenharia reversa. No final de 2016 foi criada uma exceção a esta lei para equipamentos de votação, então somente recentemente foi possível acessar e hackear estas máquinas de votação. A urna brasileira se encaixa na mesma categoria, e suspeito que ela também não seja resistente a este tipo de penetração.[(p)] Como deve ser claro agora, com sistemas transparentes não existem riscos de fal-

sificar o resultado de uma votação.

De outra natureza são as notícias que a Rússia tentou interferir na eleição presidencial de 2016, em favor de Trump. Há provas que hackers russos tentaram invadir os registros estaduais dos eleitores (que nos EUA são armazenados de forma descentralizada).[(q)] Em pelo menos um caso conseguiram invadir uma urna, aquela produzida pela empresa VR Systems.[(r)(s)]

Também suspeita-se que a Rússia tentou sabotar a campanha eleitoral de Hillary Clinton, invadindo o servidor de email do Partido Democrata e repassando 19 mil emails para Julian Assange de Wikileaks, que os publicou[(t)], ou repassando-os diretamente para o filho de Trump[(u)].

Uma outra tendência são as tentativas de influenciar as eleições através das redes sociais. *Sites* falsos com notícias falsas criadas por pessoas falsas já são técnicas comuns.[(v)] Bem mais sofisticada é a aplicação de *Big Data*. A empresa americana Cambridge Analytica [(w)] se especializa em manter dados pessoais de todos os eleitores americanos. Estes dados são cruzados com os dados do Facebook, inclusive os *likes*, permitindo um retrato bastante nítido das preferências políticas de cada eleitor. Em seguida a campanha paga Facebook para mandar propagandas direcionadas para determinados eleitores em regiões específicas, que poderiam virar uma eleição.

Existem pessoas afirmando que essa estratégia deu uma vantagem decisiva ao candidato Trump em 2016, permitindo-lhe virar o pleito em estados que estavam equilibrados.[(x)] Também suspeita-se que na votação do Brexit esta estratégia resultou num resultado decisivo para sair da Comunidade Europeia.[(y)] Existem outras pessoas afirmando que não é verdade, que a Cambridge Analytica exagerou seu papel por motivos comerciais. Mas o cenário parece bastante plausível, e muito preocupante.

Conclusão

Mesmo que o software da urna fosse perfeito, o sistema resultante não é publicamente verificável ou auditável. O projeto atual da urna acaba com a comprovação física da vontade do eleitor, então os Requisitos E, F, I e J não são atendidas. Portanto discutir a corretude do software da urna é um desperdício de tempo, porque

isto não resolve a falta de transparência; a percepção de que a urna é uma caixa preta.

Anotações

[a] *optical-scan machines* no texto original.

[b] http://gps.serpro.gov.br/pub/serpro/?numero=222

[c] Nunca entendi porque uma máquina relativamente simples como a urna precisa de tanto software. Ao invés de criar um equipamento simples e enxuto, foi criado um monstro. Enquanto se sabe que a complexidade é o enimigo de segurança.

[d] https://web.archive.org/web/20091128025506/http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf

[e] http://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[f] Um projeto da RNP para a construção de um HSM.

[g] "Program testing can be used to show the presence of bugs, but never to show their absence!" https://en.wikiquote.org/wiki/Edsger_W._Dijkstra

[h] Imagine isso no Brasil.

[i] http://wijvertrouwenstemcomputersniet.nl/English

[j] Texto elaborado junto com Pablo Marcelo García.

[k] http://ivan.barreraoro.com.ar/vot-ar-una-mala-eleccion/

[l] http://www.cronista.com/economiapolitica/Expertos-universitarios-lanzaron-una-campana-contra-elto-voto-electronico-20161101 -0113.html

[m] https://www.minutouno.com/notas/1565761-vidal-y-bullrich-hablaron-como-ganadores-las-paso-provincia

[n] https://es.wikipedia.org/wiki/Elecciones_primarias_de_Argentina_de_2017

[o] https://www.wired.com/story/voting-machine-hacks-defcon

[p] A lei brasileira proíbe a engenharia reversa da urna de seguinte maneira: a mera posse de um cartão de flash ou um pendrive da urna por alguém que não é da justiça eleitoral já é crime.

[q] http://time.com/4828306/russian-hacking-election-widespread-private-data

[r] https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html

[s] https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election

[t]https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election

[u]https://www.theguardian.com/us-news/2017/oct/07/trump-russia-steele-dossier-moscow

[v]http://www.valor.com.br/opiniao/5094250/eleicoes-sob-ataques-digitais

[w]https://cambridgeanalytica.org

[x]https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

[y]https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Capítulo 6

A impressão do voto

Estudando os documentos sobre a concepção, projeto e desenvolvimento do sistema eleitoral informatizado no Brasil, observa-se que um tipo de comprovação do voto era previsto desde o início:

> b) Deverá ser resguardado o direito à fiscalização da votação e da apuração, bem como garantir a conferência do resultado de cada Seção por meio de auditagem ou recontagem; ([2], pg. 72.)

> 4 – A comprovação física do voto deverá conter pelo menos o número do candidato e será impressa ou grafada, de forma que seja possível a leitura de seu conteúdo sem a necessidade de qualquer tipo de equipamento eletro-eletrônico ou mecânico; ([2], pg. 75.)

A primeira eleição com a urna, a de 1996, foi efetuada com a impressão do voto. Porém, a impressão deu tantos problemas que foi abolida. Nas eleições de 2002 a impressão foi re-introduzida como um teste em aproximadamente 25.000 urnas (3% das urnas). A impressão do voto empregada nas eleições de 2002 foi assim: depois de ter apertado a tecla CONFIRMA pela última vez, confirmando o voto para presidente, a urna imprime os números e nomes dos candidatos escolhidos numa unidade de impressora separada da urna. A impressão acontece numa caixa de plástico com um visor transparente. Desta forma, o eleitor poderia ver o papel com seus candidatos através de uma lente, sem poder tocá-lo.

Vendo os candidatos escolhidos, o eleitor aperta na tecla CONFIRMA ou CORRIGE. No primeiro caso, a palavra VÁLIDO é impressa no papel, o papel é cortado e

cai numa sacola de plástico preta, que funciona como uma urna convencional e o procedimento de votar encerra-se. No segundo caso, a palavra CANCELADO é impressa no papel, o papel é cortado e cai na sacola de plástico, e o eleitor pode votar novamente. Se o eleitor cancela duas vezes, ele é conduzido para votar numa cédula convencional de papel.

Desconhecemos a natureza exata dos problemas que ocorreram com a impressão do voto. Mas é óbvio (1) que o processo de votação é mais demorado: o eleitor pode conferir seu voto, e refazer se quiser. (2) Muitos eleitores não se esforçam para conferir seu voto. (3) A impressora é mais um equipamento que pode causar falhas técnicas. (4) Ela aumenta o custo de cada urna. Veja também a página do TSE.[a]

Eduardo Azeredo e a abolição do voto impresso

Pelos motivos supracitados, o TSE queria se livrar do voto impresso. O meu entendimento é que o então presidente do TSE, Nelson Jobim, pediu a Eduardo Azeredo (PSDB), deputado federal àquela época, para preparar uma nova lei implementando estas mudanças. O Projeto Lei 1503/2003 virou a Lei 10740/2003[b] que efetivamente aboliu o voto impresso.

Agora avance para o fim de outubro de 2014.

O PSDB alegou que houve fraude nas eleições presidenciais e exige uma auditoria. No entanto, sem uma comprovação física do voto uma recontagem é impossível e uma auditoria não faz sentido. E quem foi responsável por este fato foi Eduardo Azeredo, membro do mesmo partido.

A farsa do registro digital do voto

Para dourar a pílula, o TSE inventou o seguinte esquema: Além de incrementar o registro do candidato votado pelo eleitor, a urna ia armazenar uma cópia de cada voto numa tabela. Para impossibilitar fazer a ligação entre eleitor e voto (já que a urna mantém estes dois dados num mesmo equipamento, como já discutido no Capítulo 4) esta tabela seria preenchida numa ordem aleatória.

O problema desse esquema é que não convence ninguém que tem um mínimo

de conhecimento de informática. O argumento é muito simples: supondo que um fraudador seja capaz de modificar a parte do programa que incrementa os registros dos candidatos, ele também será capaz de modificar a parte do programa que deposita votos – cédulas digitais naquela tabela. A dificuldade adicional é a mesma, então supondo que o fraudador consiga a primeira modificação, ele também consegue a segunda. O registro digital de voto agrega absolutamente nada em termos de segurança.

Para não deixar nenhuma dúvida vou reformular este ponto: apesar da propaganda do TSE afirmando o contrário, **o registro digital do voto não é, e não substitui, uma comprovação física do voto.** Se trata simplesmente de uma segunda cópia digital, que um fraudador competente consegue modificar a vontade, sem deixar rastros.

A burocracia brasileira está repleta de parafernália de comprovação física, como assinaturas, rubricas, carimbos de tinta, chancelas, timbres, selos, sinetes, lacres, cera, marcas d'água, monogramas em baixo-relevo, e notas fiscais enumeradas a serem emitidas em quatro vias com papel carbono (também para cima!) e com comprovante de entrega. Mas no processo de votação todo isso foi abandonado, contra o bom senso, essencialmente por decreto do TSE quando a urna eletrônica foi introduzida.

Não está claro para mim se trata de uma tentativa da Secretaria de Tecnologia de Informação do TSE para enganar os ministros, ou se o STI e os ministros junto tentaram enganar a população brasileira, ou se houve um grande problema de comunicação entre eles (veja Seção 8). Mas o resultado é o mesmo: a urna carece de transparência; a população brasileira não dispõe de um mecanismo efetivo para verificar o resultado de uma eleição. É um direito inalienável de um povo numa democracia. Não está na Constituição Brasileira, mas, na minha opinião, deveria estar. Veja o caso de Alemanha, já mencionado (pg. 45).

A implementação falha do registro digital do voto

Naquela época, depois das eleições de 2002, fiquei um pouco preocupado com a implementação desta tabela. Em particular a questão da ordem aleatória. Gerar bits aleatórios num equipamento não é simples e é um processo sutil, onde programadores inexperientes facilmente cometem erros. Um caso famoso, que todo

mundo da área conhece e que conto cada vez que dou aula sobre este assunto, é o de Netscape.[c]Para abrir uma conexão segura e criptografada, o Netscape precisa gerar uma chave aleatória. É uma sequência aleatória de 80 bits, correspondendo a $2^{80} = 1208925819614629174706176 \approx 1.2 \times 10^{24}$ possíveis valores, suficiente para impossibilitar uma busca exaustiva. Porém, o método em que o Netscape gerava esta chave tinha um vício, um erro grave. A entrada 'aleatória' para gerar a chave era o *process id*, um número único que o sistema operacional aloca a cada processo que é executado. O problema é que a quantidade de processos num computador é limitado. Mesmo considerando 10000 processos como limite superior, fica evidente que o espaço de possibilidades fica muito limitado: 10000 é muito menor que 10^{24}. Enquanto uma busca exaustiva num espaço de 10^{24} possíveis valores é completamente inviável, este erro reduzia o espaço efetivo para 10000 possibilidades, onde uma busca exaustiva pode ser feito num segundo com um notebook comum.

Avance para 2012.

Não fiquei nem um pouco surpreso quando Diego Aranha descobriu que o TSE cometeu o mesmo erro na urna.[d] O semente a partir do qual a ordem na tabela foi definida foi baseado no horário, como definido pelo relógio interno da urna. Ainda, já que essa semente seja definids durante o processo de inicialização da urna, a hora exata aparece no relatório inicial da urna, a zerésima, facilitando ainda mais o trabalho de um adversário eventual. Ou seja, o registro digital do voto não só não resolveu o problema, mas foi implementado de forma mal-feita.

O argumento equivocado do retrocesso

Já em 2002 eu ouvi o argumento que reintroduzir o voto impresso seria um retrocesso. Tinha a impressão que isso era a opinião do(s) ministro(s), não dos técnicos da Secretaria de Informática. Quinze anos depois ainda escutamos esse mesmo argumento.

Para quem acredita no mito da segurança da urna, pode parecer que acrescentar uma impressora é um retrocesso. Infelizmente o argumento é equivocado.

A introdução da urna eletrônica foi um avanço em muitos aspectos, mas foi um retrocesso quanto à questão de auditabilidade do processo eleitoral. Como ex-

plicamos na Seção 3, para ser auditável é necessário ter uma comprovação física da vontade do eleitor. Sem esta comprovação não se tem auditabilidade real, e portanto não há credibilidade.

A (in)constitucionalidade do voto impresso

Nos últimos anos tivemos a discussão no TSE e STF se o voto impresso é constitucional ou não. [(e)] Até o termo usado para este assunto é confuso. Me parece óbvio que a impressão do voto é constitucional, desde que o sigilo do voto seja preservado. O que poderia ser inconstitucional é a lei que a implementa. Neste ponto está exatamente a dificuldade jurídica.

O voto impresso foi implementado pela segunda vez na minirreforma eleitoral de 2009. O Artigo 5^o da Lei 12034[(f)]estipula o seguinte: *Após a confirmação final do voto pelo eleitor, a urna eletrônica imprimirá um número único de identificação do voto associado à sua própria assinatura digital.*

A ambiguidade está na palavra *sua*: ela se refere à urna, ou ao eleitor? De ponto de visto de bom senso não há nenhuma dúvida: o eleitor não tem como criar nenhuma assinatura digital na urna, então *sua* se refere à assinatura digital criada pela urna. No entanto, o STF interpretou diferente: que o dispositivo poderia se referir a uma assinatura digital do *eleitor*.

O fato que o STF não optou por meramente interpretar a lei assim, mas optou por derrubar esta lei inteiramente leva à hipótese que a questão não é somente jurídica mas também política. Tenho a impressão que os ministros do TSE e STF não gostam do voto impresso, e derrubar esta lei foi uma estratégia para atrasar a impressão do voto, contrariando toda pesquisa acadêmica no mundo e todos as tecnologias eleitorais adotadas em outro países. como vimos no capítulo anterior.

Deve se lembrar que esta discussão aconteceu antes da eleição presidencial de 2014, em que o candidato Aécio Neves contestou o resultado deste pleito.

A situação atual

Foi, então, preparada uma minirreforma das leis eleitorais que não previa a impressão do voto, o que foi mudado pelo Senado. A situação atual está bem des-

crita no site do TSEhttp://www.tse.jus.br/imprensa/noticias-tse/2017/Fevereiro/serie-voto-impresso-impressao-do-voto-ja-foi-questionada-no-stf:

> O ministro [Gilmar Mendes] ressalvou, no entanto, que a questão da volta do voto impresso está sendo rediscutida com o Congresso Nacional. "Como sabem, eu continuo defendendo a ideia de continuidade do voto simplesmente eletrônico, com a ampliação do controle do sistema de auditagem", afirmou Gilmar Mendes.

Citamos aqui tambem em integro a parte final desta página web do TSE sobre este assunto:

> A Comissão de Reforma Política do Senado Federal chegou a retirar do texto do Projeto de Lei Complementar 75/2015, que originou a Lei n° 13.165, a obrigação do voto impresso ao atender a um apelo do Tribunal Superior Eleitoral (TSE).
>
> Na ocasião, o TSE salientou que a exigência do voto impresso é contraproducente, pois o sistema eletrônico de votação já permite ampla auditagem por agentes públicos, privados e partidários. Além disso, a Corte Eleitoral destacou, ainda, que a impressão do voto poderia ser muito onerosa aos cofres públicos.
>
> Ao examinar o PLC 75/2015 no quarto trimestre de 2015, o Plenário do Senado restabeleceu a obrigatoriedade do voto impresso na votação do projeto. Emenda ao texto, apresentada pelo senador Aécio Neves (PSDB-MG) e aprovada pela maioria dos senadores, retomou a impressão do voto para a próxima eleição presidencial.
>
> Ao derrubar em dezembro de 2015 o veto da presidente Dilma Rousseff à obrigatoriedade do voto impresso, com o voto de 368 deputados e de 56 senadores, o Congresso Nacional restabeleceu a exigência no texto da lei. Diante disso, já para as próximas eleições, a urna eletrônica terá de imprimir o voto dado pelo eleitor, que será depositado em local lacrado, sem qualquer contato por parte de quem vota.

A novela continua.

Conclusão

Como explicamos no final do Capítulo 2, para um sistema eleitoral ser transparente é necessário uma comprovação física da vontade do eleitor, senão não há verificabilidade. O voto impresso é um mecanismo para conseguir isso, mas é um paliativo.

Como veremos no capítulo seguinte, hoje existem sistemas eleitorais que oferecem muito mais auditabilidade que meramente imprimir o voto. Ao invés de gastar 2.5 bilhões de reais para o voto impresso nos próximos dez anos[g], não seria mais apropriado fazer primeiro um estudo das possibilidades? Um porcento desta quantia é 25 milhões, uma quantia com a qual se poderia financiar vários projetos de pesquisa.

Anotações

[a] https://web.archive.org/web/20170203233556/http://www.tse.jus.br/imprensa/noticias-tse/2017/Fevereiro/serie-voto-impresso-primeira-experiencia-com-impressao-do-voto-foi-nas-eleicoes-de-2002

[b] http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=124899

[c] https://en.wikipedia.org/wiki/Random_number_generator_attack#Predictable_Netscape_seed

[d] https://sites.google.com/site/dfaranha/projects/relatorio-urna.pdf

[e] Veja por exemplo https://tse.jusbrasil.com.br/noticias/2545215/lei-que-preve-voto-impresso-para-as-eleicoes-de-2014-e-contestada-pela-pgr.

[f] Veja http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12034.htm

[g] http://politica.estadao.com.br/noticias/geral,impressao-de-voto-vai-custar-r-2-5-bi-diz-tse,70001900669

Capítulo 7

Sistemas com transparência total

Um equívoco comum, mas compreensível, é o seguinte raciocínio: "Já que a votação por computador nunca pode oferecer sigilo e corretude, portanto é necessário voltar a sistemas tradicionais com cédulas em papel." Porém, existe uma terceira opção; existem sistemas de votação híbridos, que combinam as propriedades de papel e do computador, resultando em sistemas confiáveis e transparentes. Este capítulo fornece um vislumbre do que é de fato uma grande área de pesquisa.

Os sistemas de votação eletrônicos geralmente são divididos em duas categorias: votação em cabines e votação remota. Os dois são substancialmente diferentes: na votação em cabines as autoridades eleitorais presumidamente têm controle total sobre o software e o hardware usados para votar, enquanto que na votação remota as autoridades devem lidar com a possibilidade de que as cédulas enviadas sejam mal formatadas, por erro ou por maldade.

Outra diferença importante é que uma cabine oferece privacidade ao eleitor, o que pode não ser o caso na votação remota em que a coação pode ser um risco. Por exemplo, 'votação familiar' é o termo para coação de membros da família para votar de uma certa maneira. É por esta razão que a maioria dos pesquisadores, incluindo a mim, não defende a votação na internet para eleições nacionais importantes: simplesmente não se sabe se alguém está ao lado do eleitor e que tipos de pressão sutil estariam sendo usados. Por estas razões a votação na internet está tecnicamente fora do escopo deste livro, mas ainda é um tópico muito interessante. Portanto, a discussão é relegada para o Apêndice A e nos concentramos aqui na votação de cabine.

Sistemas de votação transparentes

Muitos sistemas de votação eletrônica são percebidos como uma caixa preta: o eleitor deposita sua cédula, e espera-se que esta seja gravada corretamente em algum formato digital, por exemplo como uma entrada em um banco de dados. Em seguida, o procedimento de contagem de votos é executado, mas, novamente, o eleitor não tem como testemunhar esse processo.

Dizendo em outras palavras, quem vota não é o eleitor; é uma máquina. Portanto sistemas de votação mais transparentes são altamente desejáveis.

Mas há um paradoxo aqui. Por um lado, para fornecer auditabilidade se gostaria que o sistema emitisse um recibo ao eleitor, mas por outro lado este recibo não deve revelar a escolha do eleitor; isso violaria a privacidade da cédula. Então a questão é: como emitir um recibo que convence o eleitor sem divulgar a sua preferência de voto? Como resolver o dilema entre auditabilidade e privacidade?

A idéia é oferecer sistemas de votação verificáveis de fim-a-fim, nos quais o eleitor pode estar convencido de que seu voto é contabilizado corretamente na contagem.[(a)]

Em quase todas as propostas, a verificabilidade de fim-a-fim é dividida em dois passos. **Verificabilidade individual** permite ao eleitor estar convencido de que seu voto está incluído no conjunto de objetos digitais que em conjunto determinam o resultado da eleição. **Verificabilidade universal** permite a qualquer pessoa, seja eleitor ou uma pessoa de fora, verificar se o resultado da eleição foi calculado corretamente a partir deste conjunto. Discutimos as duas propriedades detalhadamente abaixo, depois de apresentar um exemplo.

Um exemplo de um sistema de votação transparente

Descrevemos agora um sistema de votação simplificado que fornece segurança de fim-a-fim, isto é, verificabilidade individual e universal.

Suponhamos que o eleitor se identifique aos mesários, que verificam se ele é elegível para votar usando um método diferente do método atual usado pela urna. Em outras palavras, o eleitor acessa a máquina anonimamente; o procedimento é o seguinte:

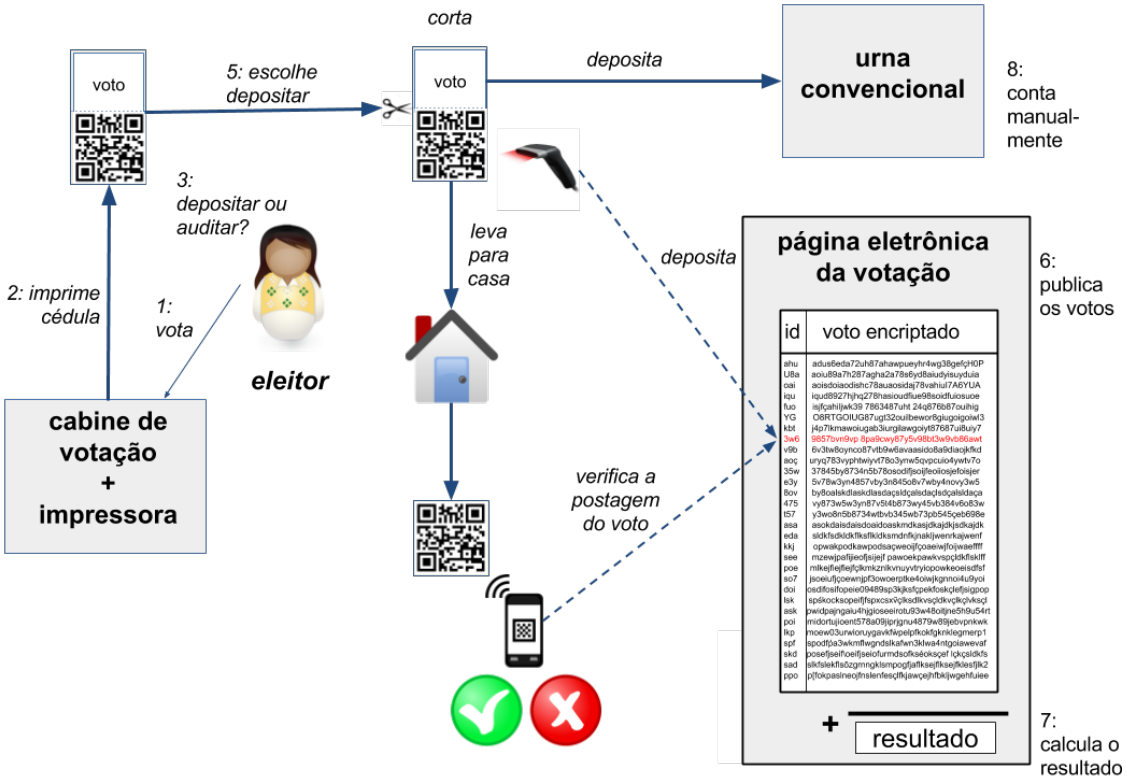

Figura 7.1: Exemplo de um sistema de votação verificável. Os números correspondem com os passos no texto.

Esquema de votação transparente simplificado

1. O eleitor entra com sua escolha na máquina de votação. Por simplicidade assumimos que é uma escolha entre duas opções, codificadas respectivamente como 0 e 1.

2. A máquina de votação imprime uma cédula composta por duas partes: v, o voto do eleitor em texto simples; e e, o mesmo voto em forma cifrada, representado no formato de código de barras. O algoritmo de ciframento usado possui uma propriedade muito especial explicada abaixo, e requer uma sequência de bits aleatórios adicional, chamada r, como entrada. Então, temos $e = E(v, r)$, onde v é o voto e r é uma sequência aleatória adicional gerada pela máquina.

3. O eleitor escolhe entre *auditar* esta cédula ou *depositá-la*.

4. Se o eleitor optar por *auditar* a votação, a máquina de votação anula a cédula (por exemplo, perfurando-a) e imprime o valor r usado para o ciframento, também no formato de código de barra. Esta cédula anulada, agora contendo a tripla (v, e, r), é então levada para outro equipamento que escaneia v e r, calcula $e' = E(v, r)$ e verifica se $e' \stackrel{?}{=} e$. Os smartphones de hoje em dia são suficientemente poderosos para executar esta verificação. Se o teste falhar, isso é uma indicação de que a máquina de votação produziu uma cédula incorreta e uma investigação começará. Se o teste passar, o eleitor retorna à Etapa 1 para imprimir uma nova cédula.

5. Se o eleitor optar por *depositá-la*, ele dobra a cédula de forma a esconder o texto simples v impresso nele e entrega-o a um mesário. Na frente do eleitor o código de barras que representa e é escaneado. Em seguida, a cédula é dividida em duas, a parte dobrada contendo v é depositada na urna, e o código de barras contendo e é devolvido ao eleitor como um recibo.

6. Depois que a eleição termina, as autoridades publicam uma lista com todos os valores de recibo e_i, ou seja, as cédulas recebidas. Isso constitui o equivalente digital de uma urna. Conceitualmente, esta lista tem a seguinte forma:

Número	cédula cifrada
1	$e_1 = E(v_1, r_1)$
2	$e_2 = E(v_2, r_2)$
$\vdots$	$\vdots$
n	$e_n = E(v_n, r_n)$

7. O sistema usa uma forma muito especial de criptografia de chave pública, chamada *criptografia homomórfica*, que preserva propriedades algébricas no seguinte sentido: o produto de duas mensagens cifradas corresponde ao ciframento da soma das duas mensagens:

$$Enc(m_1) \cdot Enc(m_2) = Enc(m_1 + m_2).$$

Isso pode ser realizado por uma técnica de ciframento conhecida como El-Gamal exponencial. Veja [8] ou [5] para mais detalhes.

Figura 7.2: Exemplo de cédula, com o voto impresso em formato claro, e em formato cifrado na forma de um código de barras. O eleitor dobra sobre a parte legível e entrega a cédula a um mesário. Posteriormente o código de barras é escaneado, e então a cédula é dividida em duas. A parte de texto simples dobrada é depositada em uma urna, enquanto o código de barras é devolvido ao eleitor como um recibo.

Usando esta propriedade em todos as cédulas cifradas e publicados, as autoridades são capazes de contabilizar os resultados das eleições mantendo todas as cédulas cifradas. Em outras palavras, as autoridades podem calcular o resultado da eleição, cifrado. Em seguida elas decifram esse valor, juntamente com uma prova de corretude.

8. (Opcional) As autoridades contam as cédulas impressas v_i depositadas na urna e compararam o resultado com o do passo anterior.

Propriedades do novo sistema

Então vamos discutir por que esse sistema oferece mais transparência.

Dualidade: Este sistema eleitoral implementa dualidade: O voto é impresso em papel e também processado em formato eletrônico. Obviamente a contagem eletrônica do Passo 7 deve coincidir com a contagem manual no Passo 8. A vantagem do papel é que ele fornece evidências físicas da intenção do eleitor, permitindo assim uma recontagem. O formato eletrônico tem a vantagem

de velocidade. Existem várias estratégias para comparar os dois resultados. Por exemplo, a contagem mais pesada de votos em papel pode ser executada somente se a eleição se revelar apertada. Além disso, a contagem manual poderia ser executada em alguns recintos selecionados aleatoriamente como um procedimento de auditoria adicional.

Verificabilidade individual:

Então, como um eleitor pode ter certeza de que seu voto é contabilizado? Primeiro, devido à possibilidade de auditoria nas Etapas 3 e 4, o eleitor pode estar seguro de que seu voto esteja fielmente cifrado em e. Em segundo lugar, ele recebe este e como recibo e, quando as eleições terminam, ele pode verificar se este realmente aparece na página da eleição. Ou ele pode delegar essa verificação, mostrando ou entregando seu recibo a outra pessoa de sua confiança, que verifica em seu lugar. Se o recibo não aparecer na lista publicada, esta é uma forte evidência de que uma cédula foi desviada (especialmente se o recibo foi assinado digitalmente) e o dono do recibo pode divulgar este fato e reclamar com as autoridades. Mas no caso em que ele aparece, o eleitor pode estar convencido de que sua cédula cifrada está incluída na lista de cédulas publicadas pelas autoridades.

Verificabilidade universal: Observe que a contagem dos votos é totalmente transparente e verificável publicamente: qualquer pessoa, seja ele eleitor ou uma pessoa de fora, pode copiar as cédulas da página eleitoral e reproduzir os passos de contagem homomórficos calculando o produto e verificando que as autoridades decifraram e publicaram o resultado correto.

Isto é o que se entende por verificabilidade universal: qualquer pessoa interessada pode verificar a contagem calculada a partir do conjunto de cédulas cifradas. Observe também que as autoridades eleitorais não podem alterar o resultado da eleição: dados os valores da segunda coluna, é matematicamente impossível mudar o resultado eleitoral sem ser descoberto.

Independência do software: Para enfatizar o último ponto, esta propriedade também é conhecida como independência de software, já mencionada no Capítulo 5 na página 39. A corretude do resultado eleitoral não depende mais da corretude do software ou hardware, nem do comportamento honesto dos trabalhadores eleitorais. Desde que os auditores certifiquem o resultado da eleição, isso implica que o resultado é correto uma vez que a verificação é baseada em provas matemáticas. E esta afirmação permanece verdadeira mesmo se o software de

votação subjacente tiver erros ou se as autoridades eleitorais conspirarem. Eles podem violar a privacidade dos eleitores, mas não podem alterar o resultado da eleição. Não há mais necessidade de auditar o software ou testes públicos da segurança.

Privacidade: Enquanto o ciframento não for quebrado, as informações no recibo e copiadas para a página da Web não revelam o voto.

Sistemas de votação da próxima geração: STAR-Vote

Um problema desses novos sistemas transparentes, pode-se argumentar, é que eles são meramente teóricos, feitos por acadêmicos sem valor prático. Isso não pode ser dito sobre o STAR-Vote [1], que generaliza o protocolo anterior como um sistema de votação no mundo real.

O sistema de votação STAR-Vote foi projetado por uma equipe composta por pessoas com diferentes antecedentes: cerca de metade deles eram pesquisadores, mas a outra metade eram pessoas que tinham responsabilidades do dia a dia com organizar eleições.

O objetivo do STAR-Vote[(b)] é recorrer à pesquisa sobre votação transparente, conforme esboçado acima, e projetar sistemas de votação práticos e funcionais. O título do *paper* é "STAR-Vote: um sistema de votação seguro, transparente, auditável e confiável"; seu resumo lê:

> STAR-Vote é uma colaboração entre alguns acadêmicos e a repartição de eleições da [Cidade de Austin (Texas)][(c)], que atualmente usa um sistema de votação DRE e anteriormente usava um sistema de votação com scanner óptico. O STAR-Vote representa uma rara oportunidade para uma variedade de tecnologias sofisticadas, como criptografia de fim-a-fim e auditorias com risco limitado, para serem projetadas em um novo sistema de votação, desde o início, com uma variedade de restrições do mundo real, como centros de votação do dia de eleição que devem suportar milhares de estilos de cédula e funcionar o dia inteiro mesmo em caso de falha de energia. Este artigo descreve o design atual do STAR-Vote que agora está amplamente definido e cujo desenvolvimento começará em breve.

O STAR-Vote usa essencialmente a mesma criptografia que mostrado no início

deste capítulo. Mas o que faz o STAR-Vote interessante é que ele usa várias idéias sobre votação, nenhuma delas nova por si só, mas que estavam flutuando na comunidade acadêmica para obter um sistema de votação transparente, ainda que prático e robusto.

Os aspectos chave são:

- o uso de uma tela para capturar a intenção do eleitor e reduzir os erros dos eleitores;
- um sistema de votação dual com uma representação eletrônica e em papel da cédula;
- um desafio do eleitor, permitindo que o eleitor audite ou lance uma cédula para contar os votos e garantir o resultado;
- o uso da criptografia homomórfica;
- um tipo especial de procedimentos de auditoria chamado auditoria com risco limitado usado para comparar a contagem eletrônica de votos e a contagem de votos em papel.

Outro aspecto interessante do STAR-Vote é o objetivo do uso do hardware comum para reduzir custos. Certamente nos EUA, onde a máquina de votação é muito cara, isso pode reduzir drasticamente o custo do hardware. Que o mesmo é verdade para o Brasil não é imediatamente óbvio porque o hardware já é produzido em grandes quantidades.

Mas ainda assim é uma ideia interessante. Imagine que uma nova geração da urna brasileira usa um tablet como interface de usuário. Nota-se que, devido à independência do software, nenhum hardware seguro precisa ser incluído, então isso pode ser razoável. Pode-se imaginar que esses tablets seriam utilizados em duas eleições, e após dois anos seriam doados para escolas no Brasil. Esta seria uma maneira de tornar este hardware mais útil do que hoje. Lembre-se de que a urna é usada apenas um ou dois dias a cada dois anos, ficando ociosa pelo resto do tempo.

Votações e o *blockchain*

Ultimamente a tecnologia de *blockchain* tem estado muito na moda. Trata-se essencialmente um registro (ou log ou livro-razão) seguro, público, e distribuído, de documentos e transações. Sendo optimista, os proponentes do *blockchain* afirmam que o *blockchain* também resolveria os problemas com votações, mas esta convicção é equivocada. Nas palavras do colega-pesquisador Josh Beneloh:[(d)]

> [...] contar votos num *blockchain* não elimina a necessidade de uma autoridade central. Os funcionários eleitorais continuarão responsáveis pela criação das cédulas e pela autenticação dos eleitores. E se você confia neles para fazer isso, não há razão para que eles também não devam registrar os votos.

O único problema que o *blockchain* resolve é de oferecer uma plataforma de publicação das cédulas verificável, mas não resolve nenhum dos outros Requisitos definidos no Capítulo 2. Em particular, nas novas sistemas propostas o eleitor recebe uma comprovação do voto, algo que o *blockchain* não resolve.

Conclusão

A imagem geral é a seguinte: A pesquisa sobre sistemas de votação transparentes começou há mais de quinze anos e agora é uma área estabelecida com sua própria comunidade, *workshops* e revista científica. E recentemente um livro de pesquisa muito interessante foi publicado [6].

A urna brasileira não desempenha nenhum papel nesta área de pesquisa. É considerada como um exemplo perfeito de como **não** fazer as coisas, não de como fazer as coisas. Pode ter algum respeito dos governos no exterior, mas este não é certamente o caso entre os especialistas em votação.

Não há vestígios de uma evidência de que o TSE esteja ciente ou tenha reconhecido a existência desta área de pesquisa, sistemas de votação transparentes e verificáveis.

Com uma exceção[(e)], o TSE nunca interagiu com essa comunidade até onde eu sei. Se isso é devido a ignorância ou arrogância não é claro. O TSE está tão focado na segurança que se esqueceu da transparência.

Não estou dizendo que o STAR-Vote solucionará imediatamente todos os problemas de votação do Brasil, mas seria um ótimo lugar para começar. Se a única consequência de eu escrever este livro é que o TSE abandonará a abordagem atual e **seriamente** começará a estudar as idéias presentes no STAR-Vote, minha missão estará cumprida.[f]

Anotações

[a]Na criptografia é feita uma distinção entre criptografia ponto-a-ponto, em que o canal de comunicação é cifrado e criptografia de fim-a-fim, na qual o aplicativo fornece o ciframento. Esta é, por exemplo, a situação de serviços como o WhatsApp, no qual o smart phone cria uma chave privada, de modo que nem a empresa conhece as mensagens que estão sendo enviadas. Muitos governos afirmam que essa criptografia ajuda os terroristas (uma reivindicação que tem sido amplamente contestada por especialistas) e estão tentando aprovar leis que obrigam os provedores a implementar um *backdoor*. O próximo passo será a forma mais alta possível de criptografia de fim-a-fim, na qual isso é retirado do aplicativo, e feito pelo usuário. O PGP é um exemplo disso.

[b]A estrela é uma referência à bandeira do Texas.

[c]Um pouco simplificado para leitores não-americanos. No original a frase está mais próxima de "...e o Travis County (Austin), repartição de eleições do Texas,..."

[d]"Benaloh points out that tallying votes on a blockchain doesn't obviate the need for a central authority. Election officials will still take the role of creating ballots and authenticating voters. And if you trust them to do that, there's no reason why they shouldn't also record votes." https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

[e]Em 2007 eu tive que recusar um convite para participar do *Dagstuhl Workshop Frontiers of Electronic Voting*. Para ter um representante do Brasil, Oswaldo Catsumi foi em meu lugar. https://www.dagstuhl.de/no_cache/en/program/calendar/semhp/?semnr=07311

[f]O STAR-Vote sofreu um revés dramático: para uma parte indispensável do projeto nenhuma empressa participou da licitação, portanto a implementação toda teve que ser cancelada. https://www.austinchronicle.com/news/2017-10-13/county-ditches-star-votes-innovative-voting-system/

Capítulo 8

O mito em ação

A segurança da urna é um mito da sociedade brasileira, e cada mito tem sua lógica própria. É uma bolha de lógica, uma auto-ilusão coletiva, que deve ser mantida a qualquer custo. Neste capítulo damos alguns exemplos deste mito, alguns já mencionados anteriormente, e alguns exemplos novos. Repare como, para manter o mito, o senso comum é violado.[(a)]

Relatório SBC

Como discutido na Introdução (pg. 14, em 2003 o Prof. Ricardo Felipe Custódio e eu entregamos o relatório RELSBCcom críticas e sugestões à urna eletrônica. O relatório foi engavetado, nunca fomos convidados para explicar nossas observações.

A urna é segura. Pensar diferente é heresia.

"Juiz nega perícia de urnas eletrônicas"

> O juiz alegou, dentre outros aspectos: [...] que o pedido de perícia teria como finalidade "conturbar a boa imagem e eficiência com que os pleitos eleitorais vêm sendo realizados pela Justiça Eleitoral."[(b)]

Este é meramente um entre vários casos. Eu me lembro de ter lido, uns dez anos atrás, um juiz argumentando que não poderia aceitar uma perícia da urna, pois

isso colocaria em xeque o resultado de toda a eleição. Isso é um raciocínio circular porque impossibilita investigar se há problemas. Um problema aqui é que a instância que executa (uma eleição) é a mesma que julga.[c]

A urna é segura. Pensar diferente é heresia.

O caso de João Lyra

Nos Estado Unidos é comum que, quando um candidato solicita recontagem dos votos, primeiro ele tem que fazer um depósito em dinheiro, que será devolvido somente caso a recontagem lhe dê razão. Mas na legislação brasileira não há previsão para isso. No entanto, em 2006, João Lyra contestou o resultado do pleito para governador em Alagoas, e foi condenado:[d]

> Na sessão plenária desta quinta-feira (8), o Tribunal Superior Eleitoral (TSE) manteve a multa aplicada a João Pereira de Lyra, candidato derrotado ao governo de Alagoas nas eleições de 2006, por litigância de má-fé.

A urna é segura. Pensar diferente é heresia.

"O Registro Digital do Voto é uma comprovação física"

Talvez o maior mito é a afirmação de que o Registro Digital do Voto constitua uma comprovação física independente da vontade do eleitor. Isso simplesmente é uma mentira. Como já foi explicado na página 53, trata-se meramente de uma segunda cópia na memória da urna. A definição de uma comprovação física da vontade do eleitor implica um ato físico irreversível e verificável pelo eleitor, como tinta em papel ou uma perfuração de papel, ou uma pedrinha depositada em uma das duas urnas. Todo mundo sabe que a memória de um computador pode ser modificada sem deixar rastros físicos, e que, de qualquer maneira, um eleitor não consegue verificar esta representação física de seu voto.

A urna é segura. Pensar diferente é heresia.

“Voltar ao voto impresso é um retrocesso”

Este argumento é muito usado pelos ministros do TSE. Recentemente um deles chegou a afirmar que o voto impresso é voltar para a fase das cavernas.[e]

Como já dito anteriormente, a introdução da urna eletrônica foi um grande progresso em vários aspectos, mas em termos de transparência foi um retrocesso, já que acabou com a existência de uma comprovação física da vontade do eleitor. Ou seja, neste aspecto o verdadeiro retrocesso foi a introdução da urna eletrônica; voltar ao voto impresso seria restabelecer o estado normal e desejável.

Sem comprovação física não existe auditabilidade, portanto não há credibilidade. Quem continua alegando que o voto impresso é um retrocesso se baseia em ‘fatos alternativos’, pois esta afirmação não é sustentada por pesquisa acadêmica.

A urna é segura. Pensar diferente é heresia.

“O voto impresso é inconstitucional”

A ‘inconstitucionalidade’ do voto impresso já foi discutida na página 56. Suspeita-se de um raciocínio deste tipo:
1) A urna é perfeita.
2) Portanto ela é segura.
3) Portanto o voto impresso é desnecessário.
4) Portanto o voto impresso é inconstitucional.

Porém, o que é realmente inconstitucional, o fato que a urna pode vincular um voto a um eleitor (pg. 31), não está sendo discutido no STF.

A urna é segura. Pensar diferente é heresia.

“O ataque não é uma quebra total”

Como descrito na página 53, o Prof. Diego Aranha quebrou a segurança da urna, mostrando que era possível vincular cada eleitor ao seu voto. O tratamento ao qual Aranha foi submetido pelo TSE depois desta descoberta foi escandaloso e humilhante. Destacam-se os seguintes pontos:

- Para provar que o ataque funcionou de verdade foi feito um teste numa cerimônia desnecessariamente demorada e tortuosa.
- O TSE não considerou o ataque uma quebra (total ou parcial), e numa escala de 0 a 400, o ataque de Aranha ganhou míseros 0.0313 pontos. Isso não é um erro de digitação![f] E foi a melhor nota de todas equipes que participaram.

  Isso é infantil. Aparentemente o TSE precisa mostrar sua superioridade, deixando claro quão insignificante estes ataques eram diante da urna perfeita. Tão insignificante que este ataque se tornou notícia no Jornal da Globo, mas foi misteriosamente tirada da pauta do Jornal Nacional no última instante, provavelmente por causa da pressão exercida pelo TSE à Globo.

A urna é segura. Pensar diferente é heresia.

"Questionar a urna é ameaçar a democracia"

Ainda sobre o Prof. Diego Aranha.

No início o TSE elogiou a participação de Aranha e funcionários da UnB nos testes de segurança da urna. Mas quando Aranha mostrou este grande furo de segurança na urna, uma das linhas de defesa do TSE era acusá-lo indiretamente de ameaçar a democracia. Numa entrevista dada a Globo[g], a última frase da réplica do TSE é:

> Querer enfatizar [...] o fato de se ter descoberto, num teste público, uma fraqueza técnica que pode ser consertada e a partir daí defender medidas sem a devida cautela é ameaçar a democracia.

É a velha estratégia: se você não consegue matar a mensagem, tente atacar a credibilidade do mensageiro. Presidente Obama tentou isso com Edward Snowden, e a equipe de Avi Rubin sofreu o mesmo tipo de ataques:[h]

> Embora os elogios fossem realmente muitos, a pesquisa de sua equipe foi menosprezada como se fosse um dever de casa, e o administrador para eleições do estado de Maryland (onde Rubin vive e trabalha) declarou publicamente que 'cientistas da computação (uma referência direta a Rubin e sua

> equipe) que questionam a segurança das máquinas eletrônicas de votação estão prejudicando nossa democracia'.

Usando uma analogia tirada de um outro contexto: culpar Diego para os problemas da urna é como culpar Al Gore pelo aquecimento global.[(i)]

Numa democracia, discutir e criticar a tecnologia eleitoral é um direito fundamental de cada cidadão, como foi confirmado pelo Tribunal Constitucional Alemão (pg. 45). O TSE não detém o monopólio sobre esta discussão e do TSE, guardião da democracia brasileira, não se espera este tipo de atitude antidemocrática.

A urna é segura. Pensar diferente é heresia.

"A urna é um exemplo para o mundo"

O fato de que hoje a votação eletrônica estar implementada em todo o país é motivo de orgulho sim. Mas a segurança da urna infelizmente não é.

Quando vou a congressos e *workshops* internacionais de tecnologia eleitoral e alguém me pergunta sobre a urna brasileira, eu levo menos que 30 segundos para detoná-la. Eu simplesmente falo que é um DRE e ainda por cima que a identidade do eleitor é inserida no mesmo dispositivo (veja pg. 31). Neste instante meu interlocutor começa a rolar os olhos ou a rir.

Quando participei de um *workshop* sobre tecnologia eleitoral em 2011, fui abordado duas vezes por pesquisadores europeus diferentes, me contando que o comportamento das autoridades eleitorais brasileiras era constrangedor, porque eles continuavam insistindo que não existiam problemas, que tinham encontrado a Solução e que todos os países do mundo deveriam seguir o exemplo brasileiro.

Contudo, o fato de tantos países rejeitarem tecnologias similares à urna brasileira deveria fazer com que os sinos de alarme tocassem, ou pelo menos tornasse o TSE curioso sobre possíveis abordagens alternativas. Não vimos nenhum sinal de tais preocupações, ou de tentativas de estudar tecnologias alternativas.

O TSE acha que não pode exportar a urna porque está muito à frente do resto do mundo. A verdade é que não pode exportar porque está muito atrás. DREs foram abandonados em outros países desde 2005.

Na sala de aula tampouco poupo a urna. Como pesquisador com formação em matemática eu costumo lidar com verdades, não com vaidades.

A urna é segura. Pensar diferente é heresia.

Uma tentativa de explicação

A seguinte hipótese é puramente especulação minha, mas às vezes penso que o mito da urna foi causado por um tremendo problema de comunicação entre a área técnica do TSE, a Secretaria de Tecnologia da Informação – STI, e a área jurídica, os ministros do TSE.[j] No zelo e orgulho profissional o STI 'vendeu´ a urna como se fosse uma das sete maravilhas do mundo, inclusive perante os ministros do TSE.

Esses ministros, sem conhecimento profundo do assunto (e atrapalhados pelas mudanças frequentes nos mandatos no TSE[k]) confiam nas afirmações do STI cegamente, o que é até compreensível numa mesma entidade. E eles começaram a defender a urna contra ataques, ataques não merecidos nos olhos deles. Ainda, os ministros começaram a acreditar que a impressão do voto é desnecessária.

Acredito que o cerne da confusão seja este maldito registro digital do voto. O pessoal da STI defendeu, e continua defendendo, que este substitui a comprovação física do voto, mas eles são as únicas pessoas no universo que acreditam isso. Não existe nenhum pesquisador nacional ou internacional que apoia esse raciocínio, e já dez anos atrás outros países começaram a abandonar essa tecnologia e procurar sistemas eleitorais alternativos.

Mas a STI criou uma 'Insula Brasiliensis' onde eles são os donos da verdade em tecnologia eleitoral, com sua lógica distorcida. E onde a pesquisa internacional, mostrando as falhas neste lógica, não entra. Neste aspecto os ministros do TSE estão sendo mal assessorados pela STI, com todas as consequências.[l]

Anotações

[a]Em agosto de 2017 o TSE criou uma página com mitos e verdades sobre a urna. http://www.tse.jus.br/imprensa/noticias-tse/2017/Agosto/tudo-o-que-voce-precisa-saber-sobre-mitos-da-urna-eletronica. Aqui respondo resumidamente às afirmações do TSE. *Verdade – A urna*

eletrônica brasileira é um modelo para o mundo. Discordo. Veja pg. 73. *Mito – A urna é insegura e não confiável.* Não é mito, é verdade. A urna não provê um voto secreto, e não é transparente. Veja os Capítulos 4 e 5. *Verdade – Não houve fraude detectada na urna.* O fato que nunca fraude for detectada não prova que não aconteceu. Veja a resposta a argumento 1 na página pg. 38. *Mito – Não há como auditar os votos dados na urna.* Não é mito, é verdade. Veja os Capítulos 4 e 5. *Verdade – A tecnologia empregada na urna é brasileira.* Concordo que é verdade. Até onde eu vi em 2002, o TSE mantém controle total sobre as técnologias principais da urna. *Mito – A urna eletrônica não é testada antes da eleição.* Concordo que é mito. A urna é testada de todas as manieras concebíveis. *Mito – Pode-se vazar a urna pela internet no dia da votação.* Concordo que é mito. Como continua o texto desta página web do TSE: "A urna não fica ligada a nenhum dispositivo de rede, seguindo importante preceito de segurança. O sistema eletrônico não tem qualquer comunicação (contato/link/telefônico) com uma rede no processo de votação dos eleitores."

[b] https://jus.com.br/jurisprudencia/16349/juiz-nega-pericia-de-urnas-eletronicas

[c] Amilcar Brunazo já argumentou mais que quinze anos atrás uma separação mais clara entre a STI e os ministros. Ele disse que, em aspectos eleitorais, o TSE é a combinação dos três poderes, legislativo, executivo e judiciário, numa única entidade só. Combinar a legislação é compreensível até certa altura; no entanto, repare que a nova proposta do Senador Aécio Neves para o voto impresso vai na contramão das opiniões proferidas pelos ministros do TSE. Mas quanto ao executivo e judiciário eu concordo com Brunazo. Como um juiz eleitoral vai mandar investigar a segurança de uma urna quando é o próprio TSE que faz a urna? Ele estará com medo de tachar a reputação do TSE, ou pior, colocar em risco a credibilidade do processo eleitoral. Talvez uma separação mais clara entre quem executa a eleição e quem julga seja saudável. Na grande maioria de outros países este problema não existe porque lá a fabricação da equivalente local á urna é feita pelo setor privado, inclusive a tecnologia empregada.

[d] https://tse.jusbrasil.com.br/noticias/2146730/tse-rejeita-recurso-de-joao-lyra-contra-governador-de-alagoas

[e] "Para o ministro Tarcísio Vieira, a impressão não traz uma segurança adicional e implica dificuldades de toda ordem, com o aumento no tempo de votação e o risco de mau funcionamento das impressoras. 'Isso vai inspirar custos adicionais gigantescos. O país destroçado economicamente, agora fica desperdiçando dinheiro com isso? É voltar para a fase das cavernas do ponto de vista eleitoral.' " http://politica.estadao.com.br/noticias/geral,impressao-de-voto-vai-custar-r-2-5-bi-diz-tse,70001900669

[f] http://web.archive.org/web/20120518151603/http://www.tse.jus.br/hotSites/testes-publicos-de-seguranca/arquivos/RelatorioFinal.pdf

[g] http://g1.globo.com/tecnologia/blog/seguranca-digital/post/falha-na-urna-brasileira-reproduzia-fielmente-erro-de-1995-diz-professor.html

[h] "While the accolades were indeed many, his team's research was maligned as being that of a homework assignment, and the Administrator for Elections for the state of Maryland (where Rubin lives and works) publicly stated that 'computer scientists (a direct reference to Rubin and his team) who question the security of electronic voting machines are undermining our demo-

cracy.' " https://www.rsaconference.com/blogs/brave-new-ballot-the-battle-to-safeguard-democracy-in-the-age-of-electronic-voting

(i) https://twitter.com/mikko/status/452474520214204416

(j) http://www.tse.jus.br/institucional/o-tse/organograma-tse

(k) https://oglobo.globo.com/brasil/troca-de-ministros-deixara-tse-com-perfil-mais-rigido-em-2018-21977722

(l) A minha sugestão seria o seguinte: O TSE deve criar uma comissão para começar um diálogo com a sociedade, com pesquisadores de engenharia, computação, interface homem-computador e da área de direito. A STI deveria também participar desta comissão, claro. Mas para evitar qualquer conflito de interesse, a STI não deve coordená-la. Os próprios ministros deveriam assumir este papel.

Capítulo 9

Além do mito

Resumo das falhas principais

A urna foi uma grande conquista em 1996, trazendo estabilidade ao processo eleitoral. Mas vinte anos depois a tecnologia no resto do mundo evoluiu, mas a urna não.

(A) O projeto da urna não elimina a possibilidade de que o voto do eleitor seja vinculado à identidade do eleitor. Nenhum sistema eleitoral no mundo tem essa propriedade.

(B) Mesmo desconsiderando o item anterior, a urna sem voto impresso tem a propriedade de não produzir uma comprovação física do voto. Este tipo de tecnologia já foi criticado por pesquisadores internacionais há mais de dez anos atrás, e por esse motivo tais sistemas são proibidos na Holanda, EUA e Alemanha.

(C) Portanto, o argumento proferido por ministros do TSE de que a impressão do voto seria um retrocesso não é sustentado por pesquisa científica. Ao contrário, a comunidade científica, no nível nacional e internacional, argumenta que, para um sistema eleitoral ser auditável, é necessário uma comprovação física do voto.

(D) A ideia de que a urna seria orgulho nacional e um exemplo a seguir pelo mundo inteiro é mito, cultivado para consumo doméstico. Em termos de

tecnologia eleitoral o Brasil está na contramão internacional, não porque a urna é superior mas por ser inferior.

(E) Dada a falha apontada no Item A, não faz sentido meramente acrescentar uma impressora a urna e investir 2 bilhões nesta abordagem ultrapassada. A urna deveria ser projetada novamente, do ponto zero.

(F) Não há motivo para se abandonar a urna atual enquanto um novo projeto é elaborado, processo que vai levar vários anos.

(G) Em essência, todas estas conclusões já foram levantadas no relatório SBC de 2002, quinze anos atrás.

(H) O TSE se tornou vítima e refém do mito que ele mesmo criou. Criticar a urna brasileira se tornou heresia; uma discussão racional, impossível.

Conclusão

No Brasil não existe um diálogo aberto e racional entre o TSE e a sociedade sobre a segurança do processo eleitoral, um dos pilares de uma democracia. A razão é que o TSE monopoliza e polemiza esta discussão. Projetar sistemas eleitorais é uma grande área de pesquisa acadêmica, mas o TSE nunca se interessou em acompanhar esta área ou dialogar com esta comunidade científica, seja no nível nacional ou internacional. Nunca houve um debate franco e aberto sobre outras tecnologias que oferecem mais auditabilidade. Críticas foram completamente desconsideradas e, às vezes, os autores destas críticas pessoalmente atacados pelo TSE.

Este livro provavelmente não é a mensagem que o TSE gostaria de receber. Também não é uma mensagem agradável para transmitir, mas tem que ser feito. E alguém tem que fazer, infelizmente: o risco de fazer nada poderia levar a um colapso total da credibilidade da urna e portanto das eleições brasileiras, com possíveis consequências catastróficas para a democracia e sociedade.

Mas ao mesmo tempo a mensagem transmitida pelo livro constitui uma abertura, uma oportunidade de começar este diálogo tão necessário. Que este livro seja entendido desta maneira.

Posfácio pelo autor

A redação deste livro foi, sem dúvida, uma tarefa árdua.

Na verdade, eu nunca quis escrever este livro. Em termos de desafio intelectual, tudo que eu quis falar já falei quinze anos atrás, no RELSBC. Pouca coisa mudou desde então, portanto de ponto de vista acadêmico 'a urna' é um assunto morto. E criticar o trabalho de outros somente traz energia negativa, como raiva e frustração. Ainda por cima corro o risco de me tornar alvo dos joguinhos mesquinhos do TSE. Eu prefiro muito mais uma agenda construtiva e ir para frente, como fazer pesquisa de verdade sobre assuntos mais quentes, ou tomar caipirinha na praia. Foi o democrata em mim que me obrigou a escrever este livro, como dever cívico. *Bad karma.*

Um outro fator complicador é que este assunto, a urna, está na interseção de tecnologia e direito. Nunca escrevi um livro para o público geral, e a metodologia da pesquisa e a redação são completamente diferentes. O maior desafio foi encontrar uma estrutura lógica e coerente para explicar o assunto a quem não é especialista. Na verdade, a ideia de escrever este livro nasceu no final de 2014, mas esta primeira tentativa fracassou, porque eu não consegui achar a estrutura certa. Tentei procurar co-autores para sair deste impasse, mas sem sucesso. Retomei a redação em maio de 2017, quando eu li que o TSE pretende gastar 2 bilhões com a urna atual.

Repare então que a ideia de escrever este livro surgiu antes da grande crise institucional entre os três poderes. Obviamente, a questão que não quer calar é o seguinte: para que ter um sistema eleitoral transparente e com voto secreto, se a Câmara e o Senado, violando o espírito da Constituição, destituem uma presidente legitimamente eleita, com a conivência do STF? Em outras palavras, parece que o Brasil tem problemas ainda muito mais sérios do que seu sistema eleitoral. Porém, esse assunto está fora do escopo deste livro e das minhas competências.

Basta dizer que, nascido e criado na Holanda, fiquei profundamente chocado pelos acontecimentos nos últimos três anos. Parece que muito poucas pessoas entendem o que é uma democracia e uma constituição.

E ainda tem a questão da língua. A minha língua materna é o holandês, enquanto uso o inglês, língua com estrutura parecida, no meu trabalho há mais que três décadas. Comecei a aprender o português com 38 anos de idade. Portanto, exprimir meus pensamentos em português de forma precisa é um processo árduo e demorado, enquanto escrever em português correto é impossível. É por este motivo que várias seções e capítulos deste livro foram esboçadas primeiro em inglês, e depois traduzidas. Mesmo assim, várias vezes, quando o assunto era muito sutil e delicado, começarem a surgir provérbios e ditos populares em holandês, infelizmente na grande maioria intraduzíveis.

Também intraduzíveis são os preceitos de Musashi do japonês de 1640 na pg. 3. A minha tradução para o inglês é tirada do livro *The Book of Five Rings*, editora Bantam Books (1982). Quando comecei a procurar traduções para o português na internet, encontrei várias interpretações com diferenças substanciais. Meu colega Hani Yehia, que fez seu doutorado no Japão, me sugeriu a seguinte tradução:

> Não dê apoio a projetos perversos.
> Persista na busca do caminho das duas espadas.
> Cultive o interesse em uma ampla gama de artes.
> Conheça uma variedade de ocupações.
> Seja discreto quanto aos negócios comerciais.
> Cultive a capacidade de ver a verdade em todos os assuntos.
> Perceba aquilo que não pode ser visto.
> Não seja negligente, mesmo nas pequenas coisas.
> Não se envolva em atividades inúteis.

Uma modernização apropriada do segundo preceito seria talvez: 'Não pare de treinar, não pare de aprender.'

Agradecimentos

Primeiramente, gostaria de agradecer o Diego Aranha. Além de prestigiar este livro com um prefácio, ele me ajudou muito em resolver pequenas dúvidas específicas, e releu o manuscrito várias vezes dando boas sugestões.

As seguintes pessoas ajudaram com a tradução ou correção de partes do livro: João Penna, Rodrigo Porto, Roberto Samarone, Thiago Silva, Hani Yehia. Se o português da versão final se tornou aceitável é graça aos esforços deles. No entanto, a responsabilidade de todos os erros restantes continua sendo minha. João Moreno ajudou com a página web do livro.

Jeroen van de Graaf
Belo Horizonte,
17 de novembro de 2017.

Referências Bibliográficas

[1] BENALOH, J., BYRNE, M. D., EAKIN, B., KORTUM, P. T., MCBURNETT, N., PEREIRA, O., STARK, P. B., WALLACH, D. S., FISHER, G., MONTOYA, J., PARKER, M., AND WINN, M. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. In *EVT/WOTE* (2013).

[2] CAMARÃO, P. C. B. *O Voto Informatizado: Legitimidade Democrática*. Empresa das Artes, 1997. ISBN: 8585628308.

[3] CHAUM, D., VAN DE GRAAF, J., RYAN, P. Y. A., AND VORA, P. L. Secret ballot elections with unconditional integrity. *IACR Cryptology ePrint Archive 2007* (2007), 270.

[4] GALLO, R., KAWAKAMI, H., DAHAB, R., AZEVEDO, R., LIMA, S., AND ARAUJO, G. T-DRE: a hardware trusted computing base for direct recording electronic vote machines. In *Proceedings of 26th Annual Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA, 6-10 December 2010* (2010), ACM, pp. 191–198.

[5] GÓMEZ, C., MORENO, J., VAN DE GRAAF, J., AND HEVIA, A. Variations on wombat: end-to-end voting on a shoestring. In *Workshop de Tecnologia Eleitoral, Anais so SBSeg 2017 (Brasília)* (2017).

[6] HAO, F., AND RYAN, P. Y. A. *Real-World Electronic Voting: Design, Analysis and Deployment*. CRC Press, 2016. ISBN: 9781498714693.

[7] RUBIN, A. D. *Brave New Ballot*. Broadway, 2006. ISBN: 0767922107.

[8] VAN DE GRAAF, J. Long-term threats to ballot privacy. *IEEE Security & Privacy 15*, 3 (2017), 40–47.

[9] VAN DE GRAAF, J., AND CALDAS, W. S. Melhorando a segurança e a transparência da urna eletrônica. In *Terceiro simpósio sobre segurança em informática* (São José dos Campos (SP), 24 a 26 de outubro 2001), pp. 221–230.

[10] VAN DE GRAAF, J., AND CUSTÓDIO, R. F. Tecnologia Eleitoral e a Urna Eletrônica. Tech. rep., Sociedade Brasileira da Computação, 2002.

Apêndice A

Internet Voting

Criar um sistema web que implementa uma votação *on-line* parece relativamente fácil, comparado a um sistema para compras online ou reservas de voos. Pode parecer que a única coisa a aplicação precisaria fazer seria incrementar um contador associado a um determinado candidato ou opção. Esta linha de pensamento é exatamente a razão que nenhum dos sistemas no mercado hoje oferece a transparência como discutida neste livro. É o mesmo problema que o da urna: a votação *on-line* é uma caixa preta e o eleitor não tem como verificar se seu voto foi realmente incluído na votação.

Implementar uma votação *on-line* justa e verificável é mais difícil que uma uma votação presencial, já que neste caso não existe a possibilidade de entregar um comprovante físico. Porém, usando técnicas criptográficas é possível solucionar este problema: é possível entregar um recibo criptográfico ao eleitor que garante que seu voto foi contado corretamente.

Apresentamos aqui uma solução muito parecida à solução do Capítulo 7. A diferença é que não existe máquina de votação, o navegador do eleitor substitui o gabinete de votação.

Para votar, a página da eleição manda um aplicativo para o navegador do eleitor. Este aplicativo é escrito em *JavaScript*, uma linguagem que é interpretada e executada pelo navegador. Trata-se de software aberto, portanto o eleitor pode ver e analisar o código fonte deste programa, se quiser. O eleitor entra com sua opção (seu voto) neste aplicativo; em seguida o aplicativo cifra esta opção, resultando numa cédula cifrada. Esta será o recibo do eleitor, enquanto uma cópia será publicada na página web da eleição, depois da eleição.

Assim obtemos o seguinte esquema:

1. O eleitor entra na página web da eleição, que envia o aplicativo de votação para o navegador do eleitor. O eleitor faz sua escolha. Por simplicidade assumimos que é uma escolha entre duas opções, codificadas respectivamente como 0 e 1.

2. O navegador cifra o voto: $e = E(v, r)$ e mostra ao eleitor.

3. O eleitor decide: ou auditar a cédula cifrada, ou depositá-la.

4. Se o eleitor optar por auditar a cédula cifrada, o navegador exibe o valor r usado para cifrar. A tripla (v, e, r) é então usado como entrada para um programa de verificação independente, que calcula $e' = E(v, r)$ e verifica se $e' \stackrel{?}{=} e$. Se o teste passar, o eleitor retorna ao Passo 1 para criar uma nova cédula.

5. Se o eleitor optar por depositar a cédula cifrada, ele deve se autenticar perante o sistema como eleitor. Se a autenticação for bem sucedida, o servidor aceita a cédula e envia um e-mail de confirmação contendo e ao eleitor.

6. Após a conclusão da eleição, as autoridades publicam uma tabela mostrando os pares recebidos, o equivalente digital de uma urna. Conceitualmente, esta tabela é assim:

Número	cédula cifrada
1	$e_1 = E(v_1, r_1)$
2	$e_2 = E(v_2, r_2)$
$\vdots$	$\vdots$
n	$e_n = E(v_n, r_n)$

   É a mesma tabela que a da pg. 62.

7. As autoridades calculam e publicam o resultado, usando o mesmo método explicado no Passo 7 na pg. 62.

Então, no final da votação o eleitor pode consultar a página da eleição e se convencer que sua cédula cifrada consta na lista. Se não, o eleitor tem motivos para reclamar publicamente.

Em termos de propriedades, é óbvio que este procedimento de votação remota não pode oferecer dualidade. Também não protege contra coação, já que as autoridades não controlam mais o ambiente em que o eleitor vota. Mas percebe que a privacidade, a correção e a verificabilidade individual e universal são preservadas. Também realiza a verificabilidade de elegibilidade, uma vez que os nomes dos eleitores que votaram podem aparecer na página da web de eleição.

Este esquema é essencialmente uma descrição simplificada do sistema de votação da internet Helios[(a)(b)]. A única diferença prática é que Helios usa um resumo criptográfico como um número de rastreamento para facilitar a tarefa de verificação do eleitor.

O Helios já foi usado em grandes eleições com milhares de eleitores: pela Sociedade Brasileira de Computação para eleger a diretoria; pela Associação Internacional de Pesquisa em Criptografia (*International Association of Cryptographic Research* – IACR); pela *Université catolique de Louvain* para eleição do Reitor; e pela Tribunal de Justiça de Minas Gerais, entre outros. E em 2017 a reitoria da UFMG decidiu adotar o Helios para executar todas as eleições internas desta universidade. O laboratório INSCRYPT da UFMG tem ampla experiência com Helios.

Criptografia transparente

A pesquisa em sistemas de votações transparentes faz parte de um programa de pesquisa mais amplo. Tradicionalmente a criptografia é usada para esconder informações. Mas ela pode também ser usada para permitir transparência e auditabilidade, concretizando tarefas que sem criptografia seriam impossíveis. Exemplos são:

- *Block chain e contratos inteligentes:* O block chain é um livro-razão distribuído, permitindo transações transparentes. Os objetos cadastrados podem ser: documentos, contratos, tokens, transações, madeira amazônica etc. Quando estas transações representam valores monetários, trata-se de uma criptomoeda. Quando o blockchain é fortalecido com uma linguagem de scripting mais poderosa, com é o caso no Ethereum, é possível implementar funcionalidades mais inteligentes, os chamados contratos inteligentes (*smart contracts*).

- *Leilões, licitações e sorteios transparentes:* Muitos destes processos conduzidos pela internet carecem de verificabilidade: como se sabe se o resultado é correto? Por exemplo, como se sabe que o sorteio dos casos no STF é justo?[(c)] Existem protocolos criptográficos transparentes para provar que estes processos são executados de forma justa e idônea.

- *Computação segura nas nuvens:* A computação nas nuvens traz grandes vantagens, mas também problemas de segurança:
  – confidencialidade: como proteger seus dados durante a transmissão? E perante o provedor?
  – verificabilidade: como você terceiriza uma tarefa computacional e verifica o resultado?

- *Mineração de dados preservando a privacidade:* A mineração de dados pode ser dificultada por motivos de confidencialidade ou privacidade quando se trata de dados de saúde, dados genéticos, dados confidenciais de empresas, etc. Exemplo: Dois hospitais querem cruzar dados para fazer análise estatística, mas por motivos de privacidade não é possível que uma parte revele seus dados à outra. Existem soluções criptográficas para este tipo de problemas.

O que unifica estas questões é o objetivo de usar criptografia, não para ocultar, mas para ser mais aberto, mais transparente, mostrando a idoneidade de quem executa estes processos, enquanto preservando a confidencialidade das partes.

Anotações

[(a)] www.heliosvoting.org

[(b)] https://votacoes.inscrypt.dcc.ufmg.br

[(c)] https://jornalggn.com.br/noticia/xadrez-dos-sorteios-do-supremo-tribunal-por-luis-nassif