Como Implementar "Mobilidade na Votação" em Eleições Brasileiras

Leonardo Kimura[1], **Marcos Simplicio Jr**[1]

[1]Universidade de São Paulo, SP, Brasil

{lkimura,mjunior}@larc.usp.br

Resumo. *As eleições brasileiras apresentam uma taxa significativa de abstenção, situação comumente causada por viagens na data do pleito ou mudança recente de eleitores. Uma solução promissora é a "mobilidade na votação", que permite ao eleitor votar em qualquer seção eleitoral. No entanto, as soluções atuais dependem tipicamente de conexão à Internet para prevenir votos duplos, algo problemático no cenário brasileiro. Assim, neste trabalho, são discutidas quatro alternativas para viabilizar a mobilidade na votação no Brasil. Embora nenhuma das soluções seja perfeita, nossos resultados indicam que a abordagem mais promissora é combinar o uso de hardware seguro com a remoção de votos duplos por meio de mixnets e threshold cryptography.*

1. Introdução

Embora o Brasil adote o voto obrigatório, o país registra uma taxa significativa de abstenção com mais de 20% (31 milhões de eleitores) faltosos nas eleições de 2022 — a maior porcentagem desde 1998 [G1 2022]. Um dos principais fatores associados a esse fenômeno é a distância até o local de votação. Como os eleitores brasileiros só podem votar nas seções eleitorais previamente cadastradas, aqueles que estão viajando ou em processo de mudança muitas vezes não conseguem votar. Embora exista a opção do voto em trânsito — um mecanismo que permite a transferência temporária do local de votação — essa alternativa exige que o eleitor registre a solicitação junto à autoridade eleitoral com pelo menos três meses de antecedência, o que frequentemente se mostra inviável. Uma possível solução é o voto pela Internet; no entanto, ela é inviável devido a desafios de segurança como a suscetibilidade à coerção e a ameaça de *malwares* nos dispositivos utilizados para votação.

Uma forma de aumentar a participação nas eleições é por meio da mobilidade na votação (*anywhere voting* [The Electoral Comission 2023]). Embora isso ainda exija a participação presencial dos eleitores, essa abordagem permite o voto em qualquer seção eleitoral, tornando o voto mais conveniente. Por exemplo, implementações de mobilidade na votação em partes dos Estados Unidos e Canadá resultaram em reduções significativas na abstenção [Chief Election Officer 2015, Stein and Vonnahme 2012]. Entretanto, a maioria das implementações existentes depende de conexão à Internet para autenticar os eleitores e prevenir voto duplo – algo problemático no contexto brasileiro.

Assim, neste trabalho, apresentamos os principais alternativas e desafios para viabilizar a mobilidade na votação no Brasil. São analisadas quatro abordagens: autenticação via conexão à Internet, utilização de fila única de votação, detecção e remoção de votos duplicados, e o uso de hardware seguro.

2. Mobilidade na votação em outros países

Diversos países já adotaram *anywhere voting*, ou mobilidade na votação. Embora os detalhes variem, eles tipicamente seguem uma das seguintes estratégias: (1) cadernos de votação eletrônicos; (2) detectar e punir.

Na primeira abordagem, os eleitores são identificados por meio de cadernos de votação eletrônicos (*Electronic Poll Books - EPBs*, em inglês). Nessa configuração, sempre que um eleitor registra seu voto, sua participação é marcada em um caderno eletrônico, sincronizado com os demais dispositivos para prevenir voto duplo. Por exemplo, em diversos estados dos EUA, EPBs tipicamente consistem em notebooks convencionais conectados à Internet [U.S. Election Assistance Comission 2023].

No entanto, garantir o funcionamento ininterrupto desses sistemas ao longo da eleição é um desafio [Cortés et al. 2018]. Por exemplo, falhas nos EPBs em Los Angeles causaram filas superiores a três horas durante o processo de votação [Zetter 2020]. Assim, é tipicamente recomendado que os EPB conectados à Internet possam ter mecanismos de redundância, como o uso de múltiplos provedores de Internet ou empregar cadernos de votação físicos. Porém, essas abordagens parecem inadequadas no Brasil, um país com desafios consideráveis de infraestrutura. Uma análise mais detalhada desses desafios é apresentada na Seção 3.1.

A segunda abordagem consiste em detectar e punir os eleitores que votam múltiplas vezes, visando desestimular tentativas de fraude. Por exemplo, na Austrália, todos os eleitores que lançam um voto são marcados em uma lista; ao final da eleição, essas listas são cruzadas para identificar votos duplos. Mesmo que essa estratégia não remova os votos duplos do resultado final, ela parece ser efetiva nos países onde é implementado. Por exemplo, nas eleições australianas de 2022, apenas 0,013% dos votos foram identificados como votos múltiplos, um número insignificante segundo a autoridade eleitoral australiana [Puglisi 2023]. Entretanto, a efetividade dessa abordagem em ambientes mais suscetíveis a ataques como o Brasil é questionável. Como muitas eleições no Brasil são decididas por uma margem pequena de votos (e.g., eleições municipais), mesmo um número reduzido de votos duplicados pode alterar o resultado oficial das eleições.

3. Alternativas Discutidas

Nessa seção, discutiremos brevemente o funcionamento de quatro alternativas para mobilidade na votação nas eleições brasileiras: conexão à Internet, fila única, remoção de voto duplo, e hardware seguro.

3.1. Conexão à Internet

Essa é a abordagem mais direta e simples, baseada na utilização de equipamentos conectados à Internet para autenticar eleitores e prevenir votos duplos. Uma opção simples é conectar o terminal do mesário à Internet, pois ele já é responsável por realizar a verificação do eleitor. Porém, isso pode trazer preocupações significativas de segurança, já que comprometeria a sua natureza "offline" – algo fortemente enfatizado pelo TSE como uma propriedade fundamental de segurança. Assim, uma opção mais viável seria introduzir um equipamento segregado, online, para a identificação do eleitor. Esse equipamento poderia ser tanto um notebook tradicional para diminuir custos, ou um hardware customizado para reduzir o risco de malware.

Entretanto, essa abordagem parece ser inviável no cenário brasileiro. Primeiro, nem todas as seções eleitorais possuem acesso confiável à Internet. Muitas seções eleitorais, particularmente em regiões remotas como interior da Amazônia, possuem uma conectividade instável ou mesmo inexistente. Assim, essas áreas dependeriam provavelmente de Internet via satélite, opções demasiadamente custosas e instáveis para serem usadas como um requisito crítico das eleições.

Segundo, é difícil garantir que esses equipamentos não sofram ataques de negação de serviço. Por exemplo, um atacante poderia paralisar completamente as eleições ao desconectar os cabos de Internet ou ao empregar bloqueadores de sinal (*Jammers*, usados para bloquear sinal de GPS em roubo de carga). Dessa forma, seria possível interferir seletivamente em seções eleitorais (e.g., paralisar seções com forte preferência a um candidato) e influenciar de forma inaceitável o resultado das eleições.

3.2. Fila Única

Essa abordagem busca introduzir a mobilidade do eleitor de forma gradual: inicialmente em um mesmo local de votação; em seguida, ao nível municipal ou estadual; e, por fim, em todo o território nacional. A proposta consiste, essencialmente, na adição de uma etapa extra de autenticação na entrada do edifício de votação. Com isso, os eleitores poderiam votar em qualquer seção eleitoral dentro do prédio, evitando que algumas seções fiquem congestionadas e com longas filas. A autenticação inicial seria realizada por um equipamento adicional, denominado Terminal de Autenticação (TA): este emitiria um token impresso (em formato de QR code), que o eleitor levaria até a seção eleitoral designada.

No entanto, essa solução introduz uma complexidade considerável ao processo de votação. Primeiramente, todos os eleitores precisariam se autenticar nos Terminais de Autenticação (TAs), o que aumentaria o número de etapas no processo e poderia gerar confusão. Em segundo lugar, os tokens impressos em papel (como QR codes) estariam sujeitos a danos físicos — podendo ser amassados, rasgados ou perdidos —, o que exigiria a implementação de um mecanismo de recuperação. Em terceiro lugar, a biometria dos eleitores teria que ser verificada duas vezes: uma no TA e outra na urna eletrônica, o que poderia causar atrasos no andamento da votação. Por fim, essa solução implicaria um aumento significativo de custos, devido à introdução de um novo equipamento crítico (os TAs), à possível necessidade de mais mesários e ao acréscimo nos encargos logísticos.

3.3. Remoção de voto no final do pleito

Essa solução propõe uma abordagem alternativa: em vez de tentar *prevenir* votos duplos, adota-se a estratégia de *detectar e remover* esses votos no final da eleição. Assim, é possível evitar os desafios associados à conexão contínua à Internet durante o processo de votação. Para preservar o sigilo do voto, o sistema usa técnicas de anonimização como *mixnet* [Terelius and Wikström 2010] e *threshold cryptography*. Já para garantir a integridade do voto, ele incorpora técnicas de verificação fim-a-fim (E2E-V) adaptado para as eleições brasileiras [Cominetti et al. 2025].

A Figura 1 apresenta uma visão geral dessa solução. Essencialmente, cada eleitor recebe, através do aplicativo e-título, um identificador único (*tokenID*) que permite o voto em qualquer seção eleitoral. Esse token é lido pelas urnas eletrônicas (e.g., através de QR code), que então armazenam o *tokenID* associado ao voto cifrado. Ao término da eleição,

todos os votos são agregados, e os votos duplos são identificados ao se comparar os *tokenIDs*. Essas duplicatas são então extraídas, misturadas por meio de *mixnet*, decifradas usando *threshold cryptography*, e removidas do resultado final da eleição.

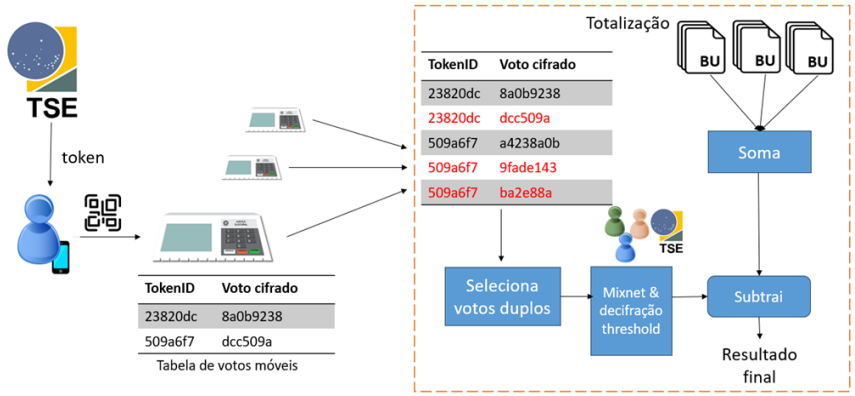

Figura 1. Visão geral da solução de remoção de duplicata

Uma vantagem dessa solução é que ela introduz quase nenhuma modificação para o processo de votação atual. Eleitores que não estão interessados em mobilidade podem votar como sempre (apresentando os documentos e votando em seções previamente designadas), enquanto eleitores interessados em mobilidade podem fazê-lo usando apenas um smartphone com o código QR code. Além disso, os requisitos de hardware são mínimos: é necessário apenas a adição de um leitor de QR code nas urnas eletrônicas.

Entretanto, essa solução apresenta diversos desafios em sua implementação. Primeiramente, sua verificabilidade depende de protocolos criptográficos e provas matemáticas complexas, de difícil compreensão para a maioria da população. Isso pode abrir espaço para interpretações equivocadas e alimentar narrativas de desinformação — por exemplo, alegações de que "o TSE está removendo votos maliciosamente". Outro desafio está na escolha adequada dos guardiões, responsáveis por preservar o sigilo do voto por meio de *threshold cryptography*. Como essa etapa é crítica para a integridade da eleição, a seleção inadequada desses guardiões pode levar a cenários de conluio ou sabotagem (e.g., um guardião que "acidentalmente" perde sua chave de decifração). Por fim, a implementação segura de um protocolo criptográfico complexo exige extremo cuidado, e não se deve subestimar os riscos associados a eventuais falhas ou vulnerabilidades.

3.4. Hardware seguro

Essa solução também visa prevenir votos duplicados, mas busca fazê-lo sem causar grandes impactos no processo de votação. Essencialmente, cada eleitor recebe um hardware seguro (e.g., smart cards), que atua como um hardware de autenticação. Durante a votação, esse dispositivo se comunica com a urna eletrônica e é marcado como "utilizado", impedindo seu reuso em outras seções eleitorais. Para facilitar a adoção desse dispositivo, é possível tirar proveito de iniciativas já existentes, como o e-CPF/CNPJ.

Entretanto, hardware seguros não são capazes de prevenir completamente votos duplos. Embora eles sejam projetados para resistir à extração de chaves, atacantes com recursos substanciais ainda podem, com uma probabilidade não nula, comprometer esses dispositivos. Assim, seria necessário combinar essa solução com algum outro mecanismo

para detectar e/ou remover votos duplos. Além disso, a solução de hardware seguro deve levar em consideração o risco de perda desses dispositivos, bem como os desafios na distribuição, manutenção e atualização desses dispositivos.

4. Discussão e Conclusão

Embora nenhuma das soluções discutidas pareça ser completamente adequada, a alternativa mais promissora parece ser combinar a abordagem de remoção de votos duplicados (Alternativa 3) com o uso de hardware seguro (Alternativa 4). Embora a solução de remoção de duplicatas seja suficiente para proteger contra votos duplos, os riscos de reputação parecem ser demasiadamente altos para o TSE – especialmente para explicar ao público como e por que os votos serão removidos. Por outro lado, o uso de hardware seguro por si só não é o suficiente para prevenir completamente contra ataques de extração de chaves e votos duplos. Assim, a solução mais promissora seria reduzir ao máximo o número de votos duplos usando hardware seguro, e usar *mixnet* e *threshold cryptography* para detectar e remover os eventuais votos duplos.

Trabalhos futuros incluem aprofundar as soluções apresentadas — em especial, a abordagem baseada na remoção de votos duplicados — com foco na especificação dos protocolos criptográficos envolvidos e na análise formal de suas propriedades de segurança. Também incluem desenvolver e testar uma versão experimental da solução, a fim de avaliar sua viabilidade técnica e seu desempenho em eleições brasileiras.

Referências

Chief Election Officer (2015). Administrative report - 2014 municipal election review. Technical report, City of Vancouver. `https://bit.ly/3GIxRvi`.

Cominetti, E., Simplicio, M., Aranha, D. F., Matias, P., and Araujo, R. (2025). E2easy: a simple lattice-based in-person end-to-end voting scheme. In *10th Workshop on Advances in Secure Electronic Voting Schemes*.

Cortés, E., Howard, L., and Norden, L. (2018). Prevent and recover from electronic pollbook failures and outages. Technical report, Brennan Center for Justice.

G1 (2022). Eleições 2022: Abstenção atinge 20,9%, maior percentual desde 1998; em 2018, foi de 20,3%. *G1*. https://bit.ly/4cEf67J.

Puglisi, L. (2023). Here's the facts about multiple voting - it is negligible in australia.

Stein, R. M. and Vonnahme, G. (2012). Effect of election day vote centers on voter participation. *Election Law Journal: Rules, Politics, and Policy*.

Terelius, B. and Wikström, D. (2010). Proofs of restricted shuffles. In *Progress in Cryptology – AFRICACRYPT 2010*. Springer.

The Electoral Comission (2023). Vote anywhere. *The Electoral Comission*.

U.S. Election Assistance Comission (2023). Electronic poll book report. Technical report.

Zetter, K. (2020). L.A. County has found the cause of its hourslong poll lines. It wasn't the new voting machines. *Politico*. https://bit.ly/3VGOLA9.