INSTITUTE OF PUBLIC POLICY

LISBON

POLICY BRIEF 14

Voto eletrónico e eleições: uma questão de confiança

Vasco d'Orey vdof@runbox.com

Policy Briefs

A série de Policy Briefs do Institute of Public Policy pretende apoiar o debate público com trabalhos concisos, onde se analisam políticas públicas de forma rigorosa e se explanam recomendações claras.

Sobre o Institute of Public Policy

O Institute of Public Policy é um "think tank" independente, sob a forma de associação sem fins lucrativos, cuja missão é contribuir para a melhoria da análise e do debate público das instituições e políticas públicas em Portugal e na Europa, através da criação e disseminação de investigação relevante

Enquadramento

O capital mais importante do processo eleitoral livre é a confiança. É fundamental que o eleitorado percecione o desenrolar de uma eleição como livre e imparcial. E aqui não é preciso apenas ser, também é preciso parecer. É preciso que toda sociedade e as suas instituições sejam oleadas em confiança em todo o processo ou corre-se o risco de um colapso generalizado do sistema de representação democrática. A confiança é infelizmente uma moeda de difícil acumulação. Demoramos anos a criar relações sólidas e de confiança entre nós, mas são apenas necessários escassos momentos para que tudo desabe. É um problema difícil mesmo entre pessoas que conhecemos bem, e torna-se muito mais complexo entre estranhos. Tendo isto em conta, qualquer alteração ao sistema eleitoral deve ter em conta o seu impacto no capital acumulado de confiança no sistema.

O objetivo de uma eleição é a tradução das intenções individuais de cada eleitor num total numérico de todas estas preferências, seja para eleger representantes, seja para fazer outro tipo de escolhas, tais como as que são apresentadas em referendos. O mecanismo de voto tem de conseguir fazer esta tradução em larga escala de forma célere, e ao mesmo tempo impedir a fraude em cada etapa do processo. As regras do jogo devem ser claras e transparentes, nomeadamente: quem pode ser eleito e para que cargo, quem tem direito de voto e qual a logística utilizada para que o eleitor expresse o seu voto.

Apesar de ser um problema difícil, as eleições têm sido realizadas em muitas sociedades ao longo da história. São conhecidos não só muitos métodos diferentes, como muitos dos seus limites graças ao acumular do seu conhecimento ao longo dos anos. Nas democracias modernas os sistemas eleitorais são diferentes em muitos detalhes, como por exemplo no grau de proporcionalidade da eleição, nos cargos que são elegíveis diretamente pelos eleitores, na organização dos círculos eleitorais, no tipo de partidos que podem ser formados, se são permitidas candidaturas independentes, entre outras questões. Independentemente do modelo escolhido, o processo tem de ser capaz de cumprir os requisitos fundamentais enunciados acima.

A confiança no mecanismo de voto

Olhando para uma eleição de uma perspetiva adversarial, em que analisamos o mecanismo essencial da democracia sob a ótica de ataque e defesa, podemos avaliar a eficácia dos processos utilizados e qual a sua resistência à fraude eleitoral. Dada a importância do resultado e do que está em jogo, existem enormes incentivos para atacar o processo eleitoral de modo a obter um resultado mais vantajoso para o atacante, daí que seja ainda mais importante ter defesas robustas em jogo. Os ataques podem vir de qualquer quadrante, seja de interesses privados, dos partidos, dos candidatos ou do estrangeiro. O objetivo pode ser a vitória ou derrota de um candidato concreto, ou simplesmente a destruição do processo eleitoral em si mesmo através da erosão do seu principal ingrediente, a confiança.

De modo a obter um ato eleitoral livre e imparcial, é necessário que uma série de processos funcionem ao longo de várias etapas. Antes das eleições propriamente ditas é preciso que os círculos eleitorais não tenham sido viciados, um problema particularmente sério em sistemas eleitorais maioritários como o dos Estados Unidos, que é mais vulnerável a este ataque do que o sistema proporcional português. Este tipo de ataque, apelidado nos Estados Unidos de *gerrymandering*[1], consiste em organizar os círculos eleitorais de modo a

[1] Uma amálgama composta pelo nome de Elbridge Gerry e salamandra, depois de Gerry, na qualidade de governador do Massachusetts, ter criado um círculo eleitoral que o beneficiava e ao seu partido, e cujo mapa se assemelhava a uma salamandra contorcida.

beneficiar um dos candidatos ou partidos a concorrer. Num sistema maioritário, se aglomerarmos as zonas que suspeitamos votarem nos nossos oponentes num só círculo ao mesmo tempo que dividimos os nossos apoiantes em vários círculos, reduzimos fortemente a probabilidade de serem eleitos representantes do nosso rival. Neste sistema, onde cada círculo elege mais que um representante, esta técnica é ineficaz. Num sistema cem por cento proporcional de círculo único, ela é simplesmente impossível. O *gerrymandering*, mesmo que não seja bem-sucedido, mina a confiança do eleitorado no processo, pois cria nos eleitores a perceção de um jogo viciado.

Uma outra via de ataque seria a ameaça e a coerção. Os eleitores não devem estar sujeitos a pressões para votar neste ou naquele candidato ou temer represálias se não votarem da forma "correta". Uma boa defesa aqui é implementar o voto secreto que reduz fortemente a eficácia deste vetor de ataque. O voto secreto é hoje essencial para qualquer eleição livre digna desse nome.

Em relação ao sufrágio propriamente dito, não é do âmbito deste texto ilustrar todos os truques para viciar eleições jamais tentados. Seja qual for o mecanismo que escolhemos para defender a integridade de uma eleição, ele passará sempre pela constatação de que não podemos confiar numa só pessoa ou grupo de pessoas. É imperativo que os locais de voto não sejam entregues a uma só parte que possa adulterar o resultado, e dada a impossibilidade em conceber uma parte totalmente imparcial e imune a pressões externas, um anjo da democracia, a solução encontrada é meter todos os adversários no mesmo saco na expectativa que a rivalidade mútua encontre um equilíbrio imparcial numa espécie de garantia de auto-destruição mútua onde todos tentam viciar o sistema ao mesmo tempo que procuram defender-se contra os ataques dos adversários. Num cenário onde não é possível confiar em ninguém, a única solução é confiar na desconfiança.

O objetivo de qualquer arquitetura do sistema de voto passa, assim, por evitar depender da honestidade de uma só pessoa ou grupo de pessoas. Idealmente, não existiria qualquer dependência das boas intenções de nenhum dos intervenientes. O melhor que poderemos almejar será a confiança na desconfiança, metendo a rivalidade das partes a trabalhar a favor de maior segurança, com a monitorização do sistema a não depender de um só "guarda", mas de todos. Por esta razão é importante que todos os partidos concorrentes tenham acesso às mesas de voto, de modo a poderem fiscalizar os seus adversários e serem eles mesmo fiscalizados. O problema clássico de quem vigia os guardas será resolvido aqui com todos serem guardas encarregues de vigilância mútua. Para além disso, existe mais um fator que joga a favor de quem procura defender o processo democrático. Os ataques diretos ao sistema de voto não beneficiam de economias de escala, pelo contrário. O custo de um ataque em larga escala é proibitivamente elevado, enquanto os pequenos ataques têm impacto reduzido, especialmente em eleições nacionais. Para efetuar um ataque ao sistema de voto em larga escala num país onde as eleições são livres são necessários muitos cúmplices para comprometerem mesas de voto em número suficiente de modo a obter um resultado mais vantajoso. Os riscos são enormes, desde algum dos conspiradores confessar o crime, à probabilidade de vários dos ataques individuais falharem e serem ou descobertos ou ineficazes. Em regimes onde as eleições são essencialmente um instrumento propagandístico nas mãos de um qualquer autocrata, este tipo de ataques é desnecessário, pois o partido dominante possui o monopólio do acesso ao sistema político e eleitoral, constituindo um ponto de confiança único, ou seja, concentra em si mesmo toda a fiscalização do sistema. Isto é exatamente aquilo que devemos evitar e uma das dificuldades em proceder a uma transição eficaz de eleições de fachada a eleições genuinamente livres.

O voto eletrónico

Se, como vimos, o sistema de voto é essencialmente um problema de confiança, é preciso perguntar o que é que a computerização poderá acrescentar à solução do problema, e é aqui que entra a questão do voto eletrónico. Uma boa maneira de tornar o processo eleitoral mais difícil e menos transparente é acrescentar complexidade, exatamente aquilo que a utilização de sistemas eletrónicos consegue facilmente fazer. O termo voto eletrónico abrange vários métodos e técnicas, desde sistemas de voto pela Internet, a máquinas que imprimem boletims de voto que têm de ser postos manualmente na urna. Estes vão de assustadoramente perigosos a quase irrevelevantes, e no meio não se encontra nenhum que contribua de forma positiva para a melhoria das defesas do processo democrático contra quem o procura subverter.

Nas eleições europeias de 2019 o concelho de Évora foi o local escolhido para um projeto piloto de voto eletrónico. Os eleitores que votaram nas freguesias onde este projeto decorreu puderam optar pelo voto convencional ou eletrónico, e a julgar pelos relatos a segunda opção foi bastante popular entre os eleitores. Na prática, o sistema funcionou da seguinte maneira: o eleitor identifica-se e recebe um cartão de plástico com um circuito integrado encarregue de fazer a autenticação perante a máquina onde o eleitor irá marcar a sua escolha e garantir que o cartão só é usado uma vez. Aquando da entrega do cartão ao eleitor, o presidente da mesa de voto terá que ativar o cartão usando equipamento especializado. Na cabine de voto encontra-se um computador que verifica o cartão e permite a escolha do candidato, imprimindo de seguida o boletim que é manualmente inserido na urna.

De acordo com o documento de apresentação do projeto da Secretaria Geral do Ministério da Administração Interna[2], serão fornecidos a cada mesa de voto eletrónico dois computadores portáteis (num total de cem em todo o concelho), para além de um portátil por mesa de voto tradicional. Os primeiros serão utilizados para consulta dos eleitores que já votaram e no processo de facultação do cartão de voto ao eleitor. Os segundos permitirão acesso ao registo de eleitores que utilizaram o método eletrónico. Segundo o mesmo documento, cada mesa de voto eletrónico e de voto tradicional terá um técnico de informática no local. O documento de apresentação indica que o processo decorrerá sem ligação à Internet ou outras redes, mas inclui um diagrama onde as mesas de voto estão ligadas por rede privada virtual a *data centers* em Lisboa e no Porto. O documento não é explícito, mas presumivelmente este diagrama refere-se aos computadores de suporte.

O jornal Público teve acesso ao relatório de avaliação do projeto que será enviado à Assembleia da República para apreciação. Julgando pelo que o mesmo relata, o processo decorreu sem problemas e recomenda-se mais em todo o país. Como veremos adiante, esta avaliação é, no mínimo, apressada, não ponderando os riscos reputacionais associados ao voto eletrónico. O resultado é que até os supostos ganhos na redução de custos financeiros são uma ilusão se não incluirem o significativo custo de uma auditoria ao sistema.

Confiança na informática

A introdução de mecanismos informáticos introduz, do ponto de vista da confiança, enormes dificuldades. Torna-se necessário fiscalizar o equipamento utilizado, desde o mais pequeno componente ao maior. Dada a complexidade das cadeias de abastecimento, seria necessário proceder a uma auditoria a todo o processo de produção dos equipamentos utilizados. Aliás, a exposição destas cadeias é

[2] https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=44e0cd27-b978-428d-b9e6-51734bafefed

suficientemente grande para que existam ataques especificamente orientados para explorar esta vulnerabilidade, os chamados *supply chain attacks*. Estes ataques procuram os pontos vulneráveis da linha de produção e procuram comprometer a integridade do equipamento ou do *software*. Com cadeias de abastecimento tão vastas como são as da informática e que podem facilmente alargar-se por vários continentes, o processo de verificação de toda a cadeia é muito difícil.

No entanto, mesmo numa cadeia de abastecimento mais pequena e inteiramente confiável, isto não será suficiente. O equipamento pode, mesmo assim, estar vulnerável a ataques que nem os fabricantes sabem ser possíveis e que não são forçosamente resultado de intenções maliciosas, mas meramente descuido, o que, dada a complexidade dos computadores, é perfeitamente expectável. As recentes revelações de que a maioria dos processadores x86 da Intel e AMD – usados em quase todos os computadores pessoais, para além de processadores ARM que são endémicos em telemóveis e outros equipamentos portáteis ou de baixo consumo – está vulnerável a ataques que permitem subverter o funcionamento do processador são apenas mais um episódio numa longa lista de vulnerabilidades ao nível do *hardware* informático[3]. Há uns anos era a própria RAM[4] cujo funcionamento produzia efeitos secundários que permitiam uma série de ataques posteriormente apelidados de *Rowhammer*[5]. O que isto nos diz é que nos temos de precaver contra vulnerabilidades intencionais produzidas por agentes maliciosos e vulnerabilidades acidentais. Estes dois exemplos são apenas a ponta do icebergue no que diz respeito ao que pode correr mal com o equipamento utilizado.

Mesmo assim, mesmo se fossem resolvidos os problemas anteriores, estaríamos longe de ter um sistema seguro. Como é que conseguimos garantir que o *software* utilizado nas máquinas de voto é aquilo que deve ser, que faz o que deve e nada mais? Não conseguimos, na verdade. Alguns leitores poderão estar neste momento a pensar em *software* livre, acesso ao código fonte, somas de verificação, criptografia, entre outras possibilidades. Na prática nenhuma delas resolve o problema.

Em relação ao acesso ao código fonte, é preciso ter em mente que não é uma representação fidedigna daquilo que acaba por ser compilado e executado no equipamento final[6]. Se conseguirmos fazer uma auditoria a todo o código, esse tem de ser convertido em código executável, um processo a que se dá o nome de compilação. A conversão é feita por outra peça de *software*, o compilador que terá agora também de ser fiscalizado. Mesmo que o seja, o próprio código fonte do compilador tem de ser compilado com um compilador em forma executável pré-existente. Podemos simplesmente confiar neste último, ou continuamos por esta interminável cadeia? Podemos fazer o nosso próprio compilador para resolver este dilema, mas isto não funciona fora da esfera individual verdadeiramente. Na prática, estaríamos a delegar poder em quem desenvolver este novo compilador supostamente "limpo". Estas pessoas, maliciosas ou não, são agora um vetor de ataque.

Somas de verificação[7] e criptografia também não ajudam, pois os programas que produzem as somas e as chaves criptográficas também têm de ser verificados, para além da matemática que está por detrás dos algoritmos utilizados. Portanto temos de verificar o algoritmo e a implementação concreta do mesmo.

[3] https://spectreattack.com/spectre.pdf
[4] Memória volátil de acesso muito rápido, mas que não mantém a informação armazenada quando desligada.
[5] https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

[6] Código fonte é código produzido por um programador humano. Antes de poder ser executado por um computador tem que ser convertido em forma binária. Nesta forma binária é possível, mas muito difícil, determinar exactamente o que o programa está a fazer. É largamente um exercício de confiança no fornecedor do programa.
[7] Somas de verificação são dados produzidos por um algoritmo com o objectivo de verificar a integridade de um bloco de dados. São usados não só em contextos de segurança, mas também como método de deteção de erros quando a informação é copiada de um suporte para outro ou através da Internet.

Suponhamos agora que todos estes problemas sem solução são resolvidos. As nossas máquinas de voto perfeitas são distribuídas pelas várias mesas de voto do país. Teremos agora de confiar que as máquinas perfeitas que saem da fábrica cem por cento segura chegam inalteradas aos locais de voto. Enquanto lá estão, antes do dia do sufrágio, é preciso garantir que ninguém com acesso às máquinas pode adulterar o *software* ou o *hardware*. O mesmo que se passa com os eleitores que não podem ter maneira de alterar a máquina. Mesmo uma máquina hermeticamente selada e sem qualquer dispositivo de acesso externo, tais como portas USB ou série, apresenta outro problema. Imagine-se que uma vulnerabilidade é descoberta no dia anterior ao sufrágio: como é que podemos corrigir a falha em milhares de máquinas especificamente concebidas para não serem alteradas após serem produzidas? No caso do projeto testado em Évora, para além do relatório não ter sido tornado público, ficámos sem saber que medidas foram tomadas para verificar os equipamentos utilizados e as pessoas que os fornecem e operam.

Reflexões finais

O que foi exposto acima é apenas uma pequena fração dos problemas que enfrentaria alguém que se propusesse a implementar um sistema de voto eletrónico e levasse a segurança do procedimento a sério. As empresas que vendem "soluções" e "sistemas completos" são ou ingénuas ou desonestas quando asseguram a segurança do seu produto. Mesmo que uma delas fornecesse um produto perfeito, seria sábio da nossa parte enquanto sociedade confiar neles, e neles apenas, e introduzir um ponto de ataque único e altamente apetecível no nosso sistema eleitoral? Técnicas de criptografia outrora tidas por seguras são hoje muito fáceis de subverter. Garantir a continuidade do *software* que utilizamos é um problema grande e de difícil auditoria.

O leitor poderá estar a pensar que tudo isto é hipérbole e que estamos a exigir um padrão de perfeição impossível que não é exigido noutros domínios. Até certo ponto sim. Mesmo sabendo da impossibilidade de criar um sistema perfeito, continuamos a utilizar os computadores para inúmeras tarefas importantes. Utilizamos regularmente a Internet para pagar impostos, tratar de assuntos bancários e marcar consultas médicas. Milhões de pessoas recorrem a estes serviços que trazem muita conveniência e conforto, para além de poupança de tempo. Nenhum deles, contudo, apresenta riscos tão elevados como uma eleição, especialmente de âmbito nacional. Quando estamos perante situações de fraude bancária[8] existem mecanismos de correção para além da informática, como os seguros e outras medidas implementadas ou pelos bancos ou exigidas por lei, que nos permitem o ressarcimento dos bens perdidos. Quando a confiança no nosso sistema eleitoral é minada, qual é o mecanismo de compensação a que podemos recorrer?

Os inimigos da democracia são internos e externos e a complexificação e opacidade são as suas armas. A informática, neste contexto, facilita o aumento da complexidade e a diminuição da transparência. Com tudo isto em mente, só podemos concluir que o voto eletrónico, longe de reduzir custos e facilitar o processo, tem o potencial de minar o principal capital de uma democracia liberal, a confiança.

[8] Aqueles que defendem um sistema de voto pela Internet parecem ignorar que a tecnologia utilizada por exemplo no *online banking* depende da capacidade de ambas as partes se identificarem, banco e cliente. As eleições livres exigem que o voto seja secreto. A separação de autenticação do utilizador e a garantia do segredo de voto são provavelmente impossíveis de conciliar.

IPP *Policy Brief* 14. Setembro 2019

ISSN: 2183-9352

Voto eletrónico e eleições: uma questão de confiança

Autor: Vasco d'Orey

INSTITUTE OF PUBLIC POLICY
LISBON

Rua Miguel Lupi, nº20, 1249-078 Lisboa, Portugal
+351 213 925 986 admin@ipp-jcs.org