Quem controla o voto eletrônico?

o declínio silencioso do controle cidadão[1]

Este texto é a versão longa de uma palestra dada no colóquio "O voto eletrônico hoje: da máquina de votar ao voto pela Internet" organizado pela Associação dos Prefeitos das Grandes Cidades Francesas em 6 de abril de 2006. Por fazer parte de uma mesa redonda sobre as máquinas de votar atuais, este texto não trata de máquinas de votar em rede nem do voto pela Internet[2].

Quem somos? Somos uma maioria de cidadãos reunidos pela nossa inquietação frente ao advento das máquinas de votar em nossas cidades respectivas, sem o mínimo debate[3], como se se tratasse de renovar o parque de microcomputadores. Sou profissional de informática, como cerca de metade de nós[4]: este texto é, portanto, o ponto-de-vista duplo de um cidadão e de um informático. Nossa primeira reação foi a de questionar nossas prefeituras. Elas nos falaram de uma organização melhor e economia, sem levar a sério nossos questionamentos. Isto nos incitou a procurar documentação na Internet. Nós descobrimos rapidamente a moratória de fato da Bélgica[5], a recusa da Irlanda[6] de usar máquinas Nedap mesmo compradas em quantidade, no mesmo ano em que a França autorizava seu uso, assim como inúmeras dificuldades nos Estados Unidos[7]. Alguns meses após a criação, observamos de perto a catastrófica eleição municipal do Québec[8]. Descobrimos que a comunidade informática havia levantado muitas reservas, como testemunham o posicionamento da ACM[9], ou a "Resolution on Electronic Voting[10]" de David Dill (professor de informática em Stanford). Nós compreendemos rapidamente o imenso potencial das informações disponíveis no exterior. Tudo isso contrastava fortemente com a ausência de inquietação na França. Nós fomos em seguida entrevistar os diversos atores do voto eletrônico: as prefeituras, equipadas ou não, o Ministério do Interior, os organismos de fiscalização (Bureau Veritas e Ceten-Apave) e os importadores.

---

[1] Título inspirado por Ulrich Wiesel, informático alemão que contesta na justiça as últimas eleições legislativas realizadas com máquinas Nedap.

[2] A este sujeito nós já publicamos uma tradução do relatório da SERVE, que levou o exército americano a abandonar este projeto de voto pela internet. Igualmente uma tradução da audiência do especialista em segurança informática Bruce Schneier na Câmara dos Representantes dos Estados Unidos, o que explica por que a Internet não é segura, e que não se trata apenas de um problema de tecnologia.

[3] Sem o mínimo debate, e até mesmo sem uma deliberação do Conselho Municipal. Os que não lêem os boletins municipais, nem aos jornais locais, descobrem a existência de máquinas de votar no momento da eleição.

[4] Nós nos sentimos obrigados a precisá-lo regularmente, sob pena de sermos tratados de retrógrados, como o fez o prefeito de Brest: "Francamente, creio que contestar a confiabilidade destas máquinas, é também contestar no fim do século XIX que o trem poderia ser uma ferramenta de progresso e que deixava doente quem entrava nele". Retrógrado é finalmente um qualificativo um tanto banal: um dia, no parlamento irlandês, o ministro responsável pela introdução das máquinas de votar tratou de atrasados os membros da Irish Computer Society, associação profissional de informáticos.

[5] A Bélgica iniciou as experiências de voto eletrônico em 1991, e alcança agora 44% dos eleitores, proporção estagnada desde 1999. Vários incidentes técnicos: notadamente Antuérpia e Schaerbeek (cuja única explicação são os raios cósmicos). Uma associação cidadã combate este sistema desde 1992 ("Por uma ética do voto automatizado" www.poureva.be), e três dos quatro partidos francófonos se manifestaram agora contra. Um projeto de lei propõe abandonar o voto eletrônico e permanecer com a automação da apuração (Nyssens 3-120). O custo é o triplo.

[6] A Irlanda deveria votar eletronicamente desde 2004 com máquinas Nedap. Depois de uma contestação cidadã crescente (que a oposição política só apoiou no fim), uma comissão independente foi formada (a CEV, "Commission on Electronic Voting") que desaconselhou seu uso. 7300 máquinas estão desde então no depósito. Cf. Irish Citizens for Trustworthy Evoting (http://evoting.cs.may.ie).

[7] As dificuldades não provêem apenas do voto eletrônico: as listas eleitorais contam também. A novela das eleições presidenciais de 2000 não foi devida ao voto eletrônico, mas a uma tecnologia mais antiga: cartões perfurados. Estes, mal projetados, foram difíceis de recontar. Pelo menos havia algo para recontar... Em reação, a lei HAVA foi votada. Ela incitou a substituir as tecnologias antigas: em 2004, cerca de 30% dos eleitores usaram máquinas totalmente eletrônicas. A tomada de consciência que eram "caixas-pretas" (pretas no sentido de opacas), assim como a suspeita envolvendo a eleição presidencial de 2004, popularizou o conceito de boletim de papel impresso verificado pelo eleitor. 26 estados incorporaram este princípio a sua legislação, e 13 estão em vias de fazê-lo. No momento, os fabricantes desconversam para não ter que modificar suas máquinas, apenas acrescentando uma impressora sem pensar na ergonomia do eleitor, nem na facilidade de recontagem. Muitas leis sobre recontagem são ainda muito restritivas. (www.VerifiedVoting.org, www.BlackBoxVoting.org, www.VotersUnite.org)

[8] "As ratas das eleições municipais". Direction informatique (directioninformatique.com).

[9] A ACM (Association for Computer Machinery), associação de informáticos fundada em 1947, com 80 000 membros, pede máquinas de votar concebidas com mais rigor e com a impressão de um boletim verificado pelo eleitor.

[10] Assinada por universitários americanos especialistas do voto eletrônico, tais como David Jefferson. Douglas W. Jones. Rebecca Mercuri, Avi Rubin, Barbara Simons, Dan Wallach... ou especialistas em segurança informática como Bruce Schneier. Um outro apelo é o "the free e-democracy project" cujo sentido é muito próximo da "Resolution on Electronic Voting", mas cujos signatários são preferencialmente europeus.

Quem somos? Somos também portadores de más notícias. Queremos lembrar:

- que o voto eletrônico, como proposto, leva inevitavelmente ao **desaparecimento do controle das eleições pelo cidadão em proveito dos técnicos**[11]. Que se trata de trocar de sistema político: da democracia (poder ao povo) pela tecnocracia (poder aos técnicos), voltando à etimologia desta palavra. Esta mudança, que nos é mostrada como inevitável, merece um verdadeiro debate nacional.
- que na prática, este controle que o cidadão é obrigado a entregar aos técnicos **se perdeu totalmente no caminho**. O resto deste texto visa demonstrá-lo.
- que os sistemas de voto eletrônico têm **uma particularidade que os diferencia dos outros sistemas informáticos**: a impossibilidade de verificar seu bom funcionamento. O motivo é o segredo do voto. Comparações infundadas com os sistemas bancários são frequentemente feitas. Você pode controlar a exatidão de uma transação bancária a posteriori, por exemplo, verificando seu extrato bancário, impressos em papel bem tangível. Todas as informações necessárias à integridade dos dados podem ser memorizadas: não há segredo entre você e seu banco. Se sua reserva aérea se perde no éter informático, não o deixarão subir no avião e você poderá protestar, com a passagem documentada em papel. Todos os sistemas informáticos possuem registros verificáveis no mundo real. Quase todos... Se a máquina engolir seu voto, quem saberá?
- que **as máquinas de votar são computadores**, mesmo se o marketing de um fabricante[12] procura fazer crer o contrário, talvez para evitar comparações desagradáveis com nossos microcomputadores caprichosos. É uma falácia[13] total, e como todo computador, as máquinas de votar contém um programa que vai determinar essencialmente seu comportamento. Conhecer o comportamento deste programa integrado é, portanto, crucial.
- que a segurança informática não se resume a evitar a conexão destas máquinas à Internet. Que a segurança informática é complicada, custosa e incompreensível para o eleitor comum[14]. Que **é preciso evitar confundir confiabilidade e segurança**: uma máquina que não quebra não garante um resultado autêntico.
- que **a acessibilidade[15] por todos os eleitores não foi estudada cientificamente** sob o ângulo da interação homem-máquina[16]. Uma pesquisa de satisfação não conseguiria responder a este questionamento. De tanto ouvir que votar numa máquina é tão fácil, que eleitor ousará confessar que ele não está confiante?
- que é preciso convencer-nos que algumas tecnologias podem não ser aplicáveis. Antigos romances de ficção científica imaginavam que nós iríamos nos deslocar em carros voadores. Por que isso nunca aconteceu? Não se trata de problema técnico. Seria simplesmente perigoso[17] demais.
- que repetir mecanicamente "nossa situação é diferente da dos Estados Unidos" nos faz fugir da pergunta de saber se não estamos na mesma direção. Todo mundo conhece a frase "a França faz a mesma coisa que os Estados Unidos com dez anos de atraso". Tanto[18] é que nossas máquinas[19] não são muito

---

[11] Ler também "L'exigence de transparence", Relatório CNIL 2003. pág. 93.

[12] A comunicação municipal nos parece influenciada porNedap/France-Élection. Alguns exemplos: "A tecnologia empregada faz uso de soluções mecânicas", Service élections de Brest. "Contrariamente a outros sistemas de voto eletrônico, a máquina de votar não contém elementos informáticos", Prefeitura de Suresnes.

[13] A máquina de concepção mais antiga, a Nedap, contém o mesmo processador 68000 que os Apple Macintosh dos anos 80. Seu programa integrado é constituído de cerca de 25.000 linhas escritas em linguagem "C". Para imprimir seu código fonte seriam necessárias cerca de 400 páginas (cf relatório do PTB "Test report 2 - Voting machine ESI2" de 17/09/2003 nas Nedap destinadas à Irlanda, pág. 7). É preciso ter cuidado com as aparências: são computadores com gabinete e tela inusitados. O ES&S iVotronic é de concepção semelhante mas mais moderna: ele usa uma tela de toque. O Indra é mais complexo, porque contém um Windows XP.

[14] Ainda seria necessário avaliar sistematicamente as máquinas sob o ângulo da segurança: isto nunca é previsto quando elas são autorizadas. Coincidências felizes fazem que estudos de segurança sejam às vezes feitos a posteriori: na Irlanda, ou em alguns Estados americanos. Dependendo da prefeitura, o custo é o principal freio ao equipamento. São anunciadas agora máquinas de votar em rede, como a e-Poll requerendo, portanto, segurança adicional. Onde estará o compromisso entre custo e segurança?

[15] A acessibilidade é a capacidade de ser utilizável pelo máximo de eleitores. Não confundir com facilidade de uso ou ergonomia.

[16] Um estudo científico da máquina de votar brasileira mostrou que ela constituía uma barreira à expressão do voto para uma proporção importante de pessoas idosas, deficientes ou não familiarizados com computadores (G.Michel-W.Cybis-M.Pimenta-J.M.Robert : "Electronic voting for ail : the expérience of the Brazilian computerized voting System").

[17] Nós já temos dificuldade em reduzir os acidentes nas estradas, devidos essencialmente a erros humanos. Imagine milhares de carros cruzando-se no céu, sem o simples recurso de parar à beira da estrada em caso de quebra...

[18] Princípio de um certificador independente ao se pronunciar sobre um referencial definido pelo Estado. Máquinas protegidas pelo segredo industrial.

[19] O iVotronic é fabricado por ES&S, um dos principais fabricantes americanos. Nedap tenta se implantar no mercado americano, notadamente no Estado de Nova Iorque.

diferentes.

- que a simplificação da organização material das eleições que essas máquinas proporcionam é real, mas não pesa frente a todos estes questionamentos. Trata-se afinal apenas de informatizar um processo raro: nada comparável com o processo de distribuir milhões de cartas por dia no Correio. Tira-se do armário uma máquina cara[20] uma vez por ano.

As máquinas de votar são, portanto, computadores. Não somos todos conscientes da **flexibilidade infinita do comportamento de um computador**. Quando viramos a direção de um carro para a direita, sabemos que ele irá para a direita. É assim porque há uma ligação mecânica entre a direção e as rodas.

Imagine agora que esta ligação seja substituída por um sistema informático: a direção passa a ser semelhante a um joystick de jogo, cujos sensores são conectados na entrada de um computador, cuja saída comanda motores elétricos agindo na direção das rodas. . Numa auto-estrada pode-se imaginar uma espécie de piloto automático: o computador ignora os sinais provenientes da direção e dirige o carro em função de outras informações (cartografia da auto-estrada e posição de outros veículos). O programa contido neste computador tem toda a liberdade de orientar as rodas a seu bel-prazer.

Ao sair da auto-estrada este piloto automático seria desligado. O termo "desligar" é enganador: não se corta um sistema como se desliga uma lâmpada, senão as rodas ficariam inertes. Basta desviar o programa para outra parte, na qual ele foi orientado para transcrever fielmente os movimentos do motorista.

Uma concepção maliciosa poderia, por exemplo, mandar o carro para o abismo cada primeiro de janeiro entre meia-noite e quatro horas da manhã. Ou até mesmo comportar-se desta maneira uma vez em cada dez. Definir um comportamento condicionado por uma data precisa é jardim da infância para um programador de computadores[21]. Por este motivo, **simular alguns votos antes da eleição, ou mesmo no dia, não traz nenhuma garantia[22].**

Então, quem controla o voto eletrônico? É muito mais fácil responder à pergunta "quem controla o voto em papel?". O eleitor pode verificar o essencial ele mesmo, e exercer seu próprio senso crítico, porque ele entende o funcionamento dos objetos em jogo (cédula, urna, etc.) despojados de tecnologia. Ele deve apenas ter confiança nos concidadãos fiscais para que a urna não seja aberta antes da apuração, a qual é uma operação pública e compreensível por todos. A grande quantidade de pessoas envolvidas numa eleição (na França: entre 200.000 e 300.000 fiscais, mas os escrutinadores), cada uma fazendo uma pequena parte do controle, só permite fraudes esporádicas e de alcance limitado.

Mas quem controla o voto eletrônico?

- O eleitor? Ele não tem prova tangível do registro de seu voto: um computador pode mostrar algo numa tela e gravar outra. Ele também não tem garantia que seu voto será contabilizado, por falta de apuração com mecanismo confiável. Mesmo que esse eleitor seja um técnico, ele não poderia saber mais, **o código-fonte[23] do programa integrado à máquina de votar sendo guardado em segredo pelo fabricante**. Ele deseja conhecer em que condições esta máquina foi autorizada? Impossível: comunicar-lhe o relatório do organismo de inspeção violaria o "segredo industrial e comercial" e "poderia comprometer o bom andamento das eleições[24]". Este último ponto é totalmente surrealista: a integridade de nossas eleições depende agora da qualidade da fechadura do armário onde esses relatórios são guardados?
- Os fiscais[25]? Eles não têm maiores competências em informática. Eles certificam a honestidade das eleições assinando a ata dos resultados, mas **podem garantir algo mais do que o respeito aos procedimentos técnicos** enumerados num manual de instruções? Por exemplo, no lugar de uma urna transparente onde eles verificariam com seus próprios olhos que ela está vazia, um computador imprime um boleto afirmando que a memória está limpa. O que eles podem realmente saber? Eles vigiam

[20] As máquinas Nedap são vendidas a cerca de € 6000 cada.

[21] Esta flexibilidade infinita é acompanhada da possibilidade de atuar com antecedência, sem precisar estar presente quando o comportamento programado se produz.

[22] Há entretanto uma utilidade. Antes da eleição, o pessoal municipal deve programar a máquina: notadamente indicar os nomes dos candidatos, e a que botão da máquina eles correspondem. "Programar" tem aqui o sentido de programar um videocassete, e não o sentido de escrever um programa. No dia da eleição, os fiscais devem se assegurar (já que são eles que assinam o termo de abertura do escrutínio) que não havia erro na programação, dois candidatos invertidos, por exemplo.

[23] O que é o código-fonte é explicado mais adiante neste texto.

[24] Opinião da CADA (Comissão de Acesso aos Documentos Administrativos) de 26 de janeiro de 2006. Um recurso perante o Conselho de Estado está sendo preparado.

[25] Os fiscais são os quatro cidadãos que acompanham o presidente da seção eleitoral. Eles devem estar todos na abertura e no fechamento do escrutínio, e no mínimo dois devem estar presentes a qualquer momento do dia. Eles são de partidos políticos diferentes. O presidente é geralmente um conselheiro municipal (NT: vereador).

fisicamente a máquina durante o dia da eleição, evitando assim que o programa seja modificado, mas eles não têm nenhuma garantia que ele estava autêntico no início do dia. Como poderiam a não ser iniciando sua tarefa fazendo examinar a máquina por dentro por um especialista em segurança informática[26]? O que seria de qualquer modo transferir sua responsabilidade de controle a terceiros. Pior, uma verificação de "checksum[27]", cujo nome já é obscuro, lhes daria **a ilusão de ter controlado alguma coisa**. E continuaria a ser totalmente ineficaz porque é impresso pelo programa que ele supostamente deve garantir[28]. Como podem se certificar que a máquina conta os votos digitados pelos eleitores já que não podem vigiar os elétrons de uma memória de computador como eles fazem com o conteúdo de uma urna: eles sabiam que a tinta de uma cédula em papel colocada numa urna lacrada é incapaz de se modificar.

- Os escrutinadores[29]? Eles só podem assistir à magia da impressão instantânea dos resultados. O Conselho da Europa recomenda a "possibilidade de segunda apuração[30]", mas um escrutinador pode obter algo mais do que a segunda impressão de um boletim?
- Os delegados dos partidos? Novamente, sua falta de conhecimentos em informática os deixa desamparados. Eles deveriam então se fazer acompanhar de um especialista em segurança informática. Não é o caso, provavelmente porque ninguém percebeu a necessidade, e que, de qualquer modo, nada foi organizado tecnicamente para permitir o trabalho deste especialista[31].
- A prefeitura? Ela confia na homologação dada pelo Estado às máquinas de votar. Quando as máquinas são compradas, como elas são estocadas entre duas eleições? Provavelmente trancadas a chave, às suas custas, mas alguém tem consciência da **extrema facilidade de modificação do programa integrado[32]**, facilidade que não é compensada por nenhum procedimento sério de controle? Quando as máquinas são alugadas, a responsabilidade do armazenamento é do prestador de serviços (na prática, é o importador das máquinas).
- O Estado?

  I. O Ministério do Interior está na origem do funcionamento das máquinas, e compartilha com as prefeituras a organização prática das eleições. Para cada modelo de máquina, ele fornece uma homologação baseando-se integralmente no relatório feito pelo organismo de inspeção (Bureau Veritas ou Ceten-Apave). Seu papel é portanto menor.

  II. A DCSSI[33], normalmente encarregada das questões de segurança informática, interessou-se por duas oportunidades[34] nas máquinas de votar, mas **nunca publicou relatório**.

  III. A CNIL (Comissão Nacional da Informática e das Liberdades) ficou um quadro teórico para o voto eletrônico em 2003[35], e depois se pronunciou em várias oportunidades sobre as eleições pela Internet[36], mas nunca especificamente sobre as máquinas de votar. A lógica de sua missão parece concentrar-se prioritariamente nas ameaças sobre a liberdade e a vida privada, isto é, o respeito ao

---

[26] Nesta ordem de idéias, Michael Scott (Dublin City University) recomenda que uma autoridade independente examine máquinas selecionadas aleatoriamente, a véspera da eleição, com a finalidade de verificar a autenticidade do programa integrado (relatório CEV, ap. 2B, pág. 140).

[27] Operação solicitada aos fiscais usando as máquinas Nedap/France-Election. No dia da eleição, a máquina imprime um boletim indicando estes checksums: são duas séries de 8 algarismos ou letras (isto é, dois números de 32 bits expressos em hexadecimal). Os fiscais verificam que são idênticos ao que indica o manual de uso. "Checksum" se traduz por "soma de controle": pergunta-se por que o termo inglês foi conservado. Para acrescentar um pouco de "magia tecnológica"?

[28] Ver em anexo nosso documento detalhado "a verificação de checksums é uma farsa".

[29] Os escrutinadores são os eleitores que participam na apuração, ou a vigiam.

[30] Recomendação Rec(2004)l 1 "sobre as normas jurídicas, operacionais e técnicas relativas ao voto eletrônico", ponto 26.

[31] O finado projeto de lei sobre máquinas de votar em rede (quiosques) ia nessa direção: ele previa uma "célula de vigilância técnica composta pelos membros da sede eleitoral centralizadora e de especialistas designados pelo prefeito e os candidatos" (segundo exposição do representante do Ministério do Interior no Fórum e-democracia 2005).

[32] Máquinas Nedap/France-Election: dois minutos bastam para substituir o programa integrado, de acordo com Michael Scott (Dublin City University) (relatório CEV, ap. 2B, pág. 139). Máquinas Indra: o programa é colocado num disco rígido. De acordo com Ceten-Apave, organismo que produziu o relatório para homologação, há somente um controle da fábrica e nenhum mecanismo de assinatura do programa. A exigência n° 45 do Regulamento técnico fixando as condições de homologação é: "Os programas [...] devem estar [...] guardados de forma inalterável". As máquinas Nedap/France-Election parecem violar esta espírito: suas memórias podem ser consideradas inalteráveis (embora sejam EPROMs, não se pode reprogramá-las pela máquina), mas são removíveis. As máquinas Indra parecem não respeitar nem o espírito nem a letra: um disco rígido permite por princípio modificar facilmente seu conteúdo.

[33] A DCSSI é uma das cinco diretorias da SGDN (Secretaria Geral da Defesa Nacional), que depende do Primeiro Ministro. Ela é encarregada das questões de segurança informática. (Apresentação).

[34] Uma primeira vez há muitos anos, agora no outono de 2005. O voto pela Internet foi também estudado recentemente.

[35] Deliberação n°03-036 de 1º de julho de 2003. Ver também relatório 2003, pág. 92 e seguintes.

[36] Franceses no Exterior (CSFE) 2003 (03-0191 CCI (04-0731 Tribunais de Paris (2005-272) Lyon e Nanterre.

segredo do voto. Com as máquinas de votar atuais[37], a identificação e a anotação do eleitor se fazem segundo os procedimentos tradicionais: o segredo do voto parece[38] naturalmente preservado pela separação física do voto e da identificação. Em seu relatório de atividade de 2004[39], a CNIL recomenda uma "avaliação global dos dispositivos de voto eletrônico", **recomendação que não foi cumprida até hoje**.

IV. A justiça: ela foi interpelada por um candidato no Tribunal de Paris, relativo ao voto pela Internet, e indeferiu[40] a ação porque "contentava-se em enumerar os riscos[41]". Ela nunca teve que se pronunciar sobre uma eleição política efetuada em máquinas de votar.

- O organismo de inspeção (Bureau Veritas ou Ceten-Apave)? Ele examina uma máquina num determinado momento: **a homologação é dada sobre um modelo de máquina, e não sobre cada exemplar fabricado desta máquina**. Ele não tem sempre acesso ao código-fonte do programa: a CNIL o recomenda[42], mas o "Regulamento Técnico" não o impõe. Não ficou claro se o programa pode ser modificado posteriormente sem necessitar uma nova homologação[43]. Não é solicitada a este organismo a avaliação global da segurança, somente de verificar sua conformidade com **um caderno de encargos[44] que tem seus limites**. Este último atende, sobretudo, às necessidades das prefeituras: confiabilidade da eletrônica, longevidade e facilidade de uso. Em resumo, pergunta-se a estes organismos algo muito preciso: como esta questão (o "Regulamento Técnico") está mal colocada, a resposta (o relatório produzido) não tem nenhum interesse[45].
- Na extremidade da corrente, situam-se o fabricante e o importador[46]. Uma organização bem concebida deveria ter como objetivo evitar dúvidas a este respeito. **O controle deveria ser exercido pelos primeiros elos da corrente: numa democracia representativa, os únicos legítimos são os eleitores, os fiscais, os delegados e os escrutinadores**. Este elo é efetivamente muito crítico. Desnecessário imaginar a conivência de uma empresa com um partido político. Um pequeno número (um só talvez) de programadores ou técnicos da cadeia de produção pode, num ato único, comprometer centenas de máquinas e, portanto, uma eleição inteira. Este caso de figura é o que permite a fraude mais eficaz. Ele ilustra uma regra geral da informática: **ela permite fazer o que antes era manual, em maior escala, às vezes com muita antecedência, sem se deslocar, sem deixar vestígios[47] e com menos gente (às vezes uma só pessoa)[48]**. Por outro lado, o modelo econômico destas empresas é o motivo do segredo que envolve as máquinas de votar[49].

A que conclusão isto nos leva? Ela poderia articular-se nas palavras a seguir: **o controle e a transparência. Os dois estão cruelmente ausentes**. A confiança, para ter fundamento, deve apoiar-se no seu corolário: o controle.

---

[37] Na será mais o caso com as máquinas de votar em rede do tipo e-Poll. Elas integram em um só dispositivo a identificação do eleitor, o registro do seu voto e sua anotação.

[38] Mas por falta de transparência, o eleitor não pode intuitivamente excluir que a máquina registra a ordem de passagem dos votantes, ou ainda que o gabinete de controle das máquinas Nedap/France-Élection (nas mãos do presidente da seção) mostre o voto que o eleitor está digitando. Isto leva a refletir sobre os usos desviados de câmeras miniaturizadas (proibidas na Itália) que seriam menos facilmente detectadas num ambiente tecnológico da seção eleitoral informatizada: um cabo a mais poderia passar despercebido (relatório CEV, ap. 2B. pág. l43).

[39] CNIL, relatório de atividades 2004 (publicado início de 2005), pág. 70.

[40] Uma primeira vez em Paris em 27 de janeiro de 2005, julgamento anulado pela Tribunal de Recursos em 7 de junho de 2005, e uma segunda vez em Lyon em 3 de outubro de 2005.

[41] Estabelecer uma prova informática não é simples, e pressupõe o acesso ao sistema de voto no mínimo na véspera da eleição (mas isso não basta no que diz respeito às manipulações que apagam seus rastros uma vez a fraude executada, ou que não deixam nenhuma significativa). Este acesso não é facilitado pelo segredo industrial acrescido às legítimas exigências de segurança envolvidas no escrutínio.

[42] "A Comissão estima que no caso de uma eleição organizada por uma coletividade pública, o código-fonte dos programas usados pelo sistema de voto eletrônico deveria ser acessível sem restrição, a fim de permitir a realização de todas as perícias julgadas necessárias", deliberação 03-036 de 1º de julho de 2003.

[43] Por exemplo, nos Estados Unidos, a NASED indica qual número de versão do programa integrado do ES&S iVotronic é certificado. Nada aparece no decreto de homologação francês. O parágrafo 2.2.1 do "regulamento técnico", referente às "modificações por iniciativa do fabricante" não diz nada sobre o software.

[44] Isto é, sempre este mesmo "regulamento técnico fixando as condições de homologação das máquinas de votar".

[45] Nosso interlocutor num dos organismos envolvidos nos confessou que teria apreciado que sua empresa tivesse sido consultada na redação do "regulamento técnico". Um outro organismo esperava que o "regulamento técnico" fosse melhorado até as eleições de 2007.

[46] France-Élection importa Nedap dos Países-Baixos, Datamatique importa ES&S dos Estados Unidos, Berger-Levrault importa Indra da Espanha.

[47] Ou então vestígios sem valor jurídico, ou simplesmente um resultado eleitoral plausível não incitará o esforço de pesquisá-las.

[48] O Professor Roberto Di Cosmo, autor do artigo "E-duquemos o e-cidadão!", usa a analogia a seguir: seu carteiro abre talvez suas cartas com vapor, para lê-lo à sua revelia. Seria desagradável, mas seriam apenas algumas cartas num lugar muito preciso. O equivalente eletrônico é um computador que analisa os e-mails de todo o mundo. Nada surrealista...

[49] A segurança é um pretexto: trata-se do conceito discutível de "segurança por obscurantismo" (cf nota n°53). O verdadeiro motivo é que o investimento feito por essas empresas é em grande parte o desenvolvimento do programa integrado.

Para que esta confiança não seja cega, a transparência deve ser total.

Que solução preconizamos, Já ouço alguns perguntando. Sejamos claros: nós não criamos o problema, nós já temos bastante dificuldade para alertar sobre ele, portanto não nos sentimos na obrigação de indicar uma solução. **O encargo da prova não nos cabe**. Aos promotores do voto eletrônico de demonstrar sua inocuidade. **O princípio da precaução** deve ser aplicado igualmente neste domínio. Entretanto, algumas pistas existem.

Com relação à falta de controle, a solução geralmente preconizada[50] pelos universitários e especialistas em segurança informática, é **a impressão de um boletim verificado pelo eleitor (VVAT)[51]**. A máquina, assim que o voto é digitado, imprime um boletim repetindo as escolhas feitas. Este boletim é mostrado ao eleitor atrás de um visor. Ele o compara com a tela e o valida. O boletim é em seguida conservado dentro da máquina. A noite da eleição, uma proporção estatisticamente significativa dos boletins é contada. Os votos são desta forma verificáveis por meio de um circuito independente da informática: boletins em papel conservados numa urna e apuração manual.

Com relação à falta de transparência, a solução reside em sistemas de concepção totalmente aberta, tanto no nível hardware quanto software. Como os clientes dos sistemas de voto são coletividades públicas, o modelo do software livre é aqui particularmente pertinente[52]. A segurança, atualmente baseada no conceito duvidoso de "segurança por obscurantismo[53]", seria reforçada. **Deve-se, entretanto, lembrar que obter a transparência sem garantir o controle é praticamente inútil**. O código-fonte de um programa pode até estar publicado na Internet, se você não puder garantir que o mesmo programa está presente em todas as máquinas no dia da eleição, você não progrediu nada.

Nosso sistema político é a democracia representativa. A maioria não participa nas decisões políticas. Entretanto, **detentores da "soberania popular"**, nós delegamos temporariamente nosso poder aos nossos prefeitos, nossos deputados, ao nosso presidente... por cinco ou seis anos. Nós só detemos realmente esse poder no dia das eleições. Neste dia preciso por que nos é solicitada uma **confiança cega** num sistema informático cuja integridade é vagamente controlada por um punhado de técnicos mal identificados?

A confiança nos homens políticos ou sua possibilidade de ação já foi rompida. Seria perigoso acrescentar uma desconfiança em relação à honestidade das eleições.

Eis agora algumas questões precisas:

Como devolver ao cidadão o controle da eleição, como os exigem os princípios da democracia representativa[54]?

Que mecanismo garante o conteúdo das máquinas de votar, notadamente a autenticidade de seu programa? Não sabemos de nenhum sério, e consideramos este problema insolúvel.

Se uma eleição é contestada, quem parecerá responsável pela incerteza criada pelo voto eletrônico[55]? A quem será imputada a falta de controle?

Qual é a explicação do marketing inverossímil praticado por France-Élection/Nedap[56], que quer fazer crer que suas máquinas não são computadores? Nenhum técnico informático pode levar a sério estas afirmações.

Por que tal opacidade envolve o voto eletrônico, indo até mesmo os relatórios de homologação?

A CNIL recomendou uma "avaliação global dos dispositivos de voto eletrônico". Quando será realizada? Não deveria ser levada em conta a opinião da DCSSI[57]? Ir até mais longe, e seguir o exemplo da Irlanda, criando uma comissão independente para investigar o voto eletrônico?

---

[50] Afim de não insultar o futuro, as petições, como a de David Dill, ou a do "the free e-democracy project", usam a expressão "rastro de auditoria verificado pelo eleitor". Elas explicam em seguida que no estado atual dos conhecimentos, só o papel permite realizar este rastro de auditoria.

[51] No nosso site: o boletim de papel verificado pelo eleitor (VVPB/VVAT), detalhes deste conceito, dificuldades de implantação e realizações (abortadas) no exterior.

[52] "O dinheiro público só deve pagar uma vez", como diz o ADULLACT.

[53] Cf. Wikipedia (em inglês): "Security through obscurity". Um uso razoável so segredo é possível, inspirando-se na criptografia: os programas e métodos de cálculos (algoritmos) são públicos, só a chave é secreta. No caso do vôo eletrônico, ver relatório CEV, ap. 2B, pág. l45, Apêndice B.

[54] Segundo a CNIL, "o recurso de técnicas informáticas sofisticadas não deve levar a fazer os sistemas de voto escaparem ao controle democrático dos membros da seção eleitoral, dos escrutinadores e dos eleitores em proveito de técnicos informáticos". Infelizmente, a transição com o parágrafo seguinte é "esquizofrênica". Relatório 2003, pág. 94.

[55] "Nenhum sistema de voto conhecido pela CNIL prevê a produção de elementos de prova em caso de contencioso eleitoral. Estes elementos de prova entendem-se sobre o funcionamento do próprio sistema de voto durante o escrutínio, de modo a demonstrar de maneira convincente que não deu margem a um funcionamento anormal, seja involuntário ou deliberado". Relatório CNIL 2003, pág. 93

[56] Cf. nota nº 12.

[57] Cf. nota nº 33.

A democracia eletrônica é portadora de inúmeras promessas. Entretanto, é preciso ter consciência que um de seus componentes, o voto eletrônico, levanta problemas muito específicos. Tratar-se-ia de um recuo democrático?

www.recul-democratique.org

Máquinas Nedap/France-Élection:a verificação de checksums é uma farsa

A explicação a seguir é um pouco técnica. É natural que você não a compreenda. Nós o convidamos então a submetê-la a alguém de seu relacionamento com alguma base de informática. ***Que você não esteja entendendo não deixa de ser significativo****. Se você fosse um fiscal, você teria a ilusão de efetuar um controle da máquina, mas a presença da tecnologia lhe impediria de exercer seu senso crítico, e de entender que este controle é inoperante.*

Durante o procedimento de homologação, uma só máquina (ou no máximo algumas) é examinada pelo organismo de inspeção. A homologação é concedida para um modelo de máquina, e não para cada exemplar fabricado. É portanto crucial garantir que todas as máquinas em uso nas seções eleitorais sejam idênticas à que foi examinada. Um ponto essencial é o programa integrado, porque a essência da inteligência da máquina de votar reside nele.

France-Élection, importador das máquinas Nedap, pretende controlar a autenticidade deste programa por meio da verificação dos checksums. Do que se trata? A máquina de votar sabe calcular um número chamado checksum (em português: soma de controle) a partir de todos os 0 e 1 que constituem seu programa integrado. Se o menor destes 0 ou 1 for modificado este checksum vai mudar de valor. Na prática, dois checksums são calculados, cada um relativo à metade da memória. Seu valor é indicado no manual de uso da máquina. No dia da eleição, os fiscais devem portanto pedir à máquina para imprimir estes checksums e verificar que estão idênticos ao que indica o manual.

Este procedimento é recomendado e é considerado eficaz pelo relatório do PTB (Physikalisch-Technische Bundesanstalt), organismo independente encarregado de certificar o programa integrado. Na exigência[58] *"No caso de uma máquina com microprocessador, toda alteração do programa integrado por uma pessoa não autorizada será detectada*", o **PTB** responde que a exigência é satisfeita, e se justifica desta forma:
"Os números de versão dos programas e os checksums do programa integrado, para a placa principal de controle, a placa de conexão (comunicação) e as cinco placas de vídeo podem ser visualizados e impressos pela máquina de votar. Isto permite ao pessoal eleitoral de comparar estes números de versão dos programas e estes checksums com os valores impressos pelo fabricante da documentação (manual do usuário), ou, por exemplo, inscritos sobre o certificado de homologação".

O que não está certo? Já é um engano de tecnologia. Um checksum tem por vocação detectar modificações ***acidentais***: por exemplo, se um dos 0 ou 1 foi modificado por falha física do chip eletrônico interno. Por outro lado, não protege de modificações ***intencionais***. Para este caso deverá ser usada a técnica do hash criptográfico.

Sejamos caridosos, e coloquemos esta escolha em perspectiva com a época da concepção desta máquina. Porque finalmente, tudo isso não tem importância: ***o próprio princípio desta verificação é inepto***, qualquer que seja a técnica empregada. Afinal, pede-se para imprimir este checksum ao programa que se quer controlar. A alternativa se apresenta assim: se for autêntico ele vai realmente calculá-lo e o resultado baterá, exceto se houver falha eletrônica; se tiver sido modificado fraudulentamente, ele não fará cálculo algum, e simplesmente imprimirá o valor indicado no manual do usuário. A flexibilidade infinita de um programa faz com que não haja nenhuma dificuldade de realização.

Ter confiança nesta verificação de checksum é como perguntar a uma pessoa na rua se ela é honesta e, em caso afirmativo, pedir-lhe para sacar um dinheiro entregando-lhe o cartão do banco e a senha. **A inépcia desta verificação de checksum foi apontada pelo relatório[59] da Commission on Electronic Voting,** comissão independente que desaconselhou o uso das máquinas Nedap na Irlanda.

Por qualquer lado que se olhe este procedimento de verificação de checksum, não se entende sua implantação. Se o objetivo fosse o de verificar o bom funcionamento da eletrônica, um procedimento bem mais simples bastaria: se tudo estiver correto a máquina inicia sem dizer nada, senão ela pára mostrando uma mensagem de erro. Todos os PCs do mundo verificam assim sua memória quando são ligados[60], sem que para isso seja

[58] "Type testing of a voting machine for elections/referenda in Ireland...", pág. 7, exigência (4).

[59] "O programa integrado à máquina de votar poderia ser modificado para alterar os votos. O programa tem um checksum, que o protege contra as modificações acidentais, mas não contra manipulações deliberadas". Em versão original: "The controlling program inside the voting machine could be modified to affect the vote. The program has a "checksum" which protects it against accidental changes, but does not protect against deliberate tampering". Michael Scott (Dublin City University), relatório da CEV, ap. 2B, pág. 139.

[60] Para ser preciso, trata-se de verificar a memória viva (RAM), e não a memória morta (ROM ou EPROM).

necessário consultar o manual do usuário. Aliás, a máquina Nedap utiliza, para este efeito, um terceiro checksum interno.

A dificuldade de controle da autenticidade do programa integrado é geral em todas as máquinas de votar. A máquina concorrente Indra[61] não faz melhor. Ela nem tenta realizar esta verificação do programa integrado. Pode-se, entretanto, reconhecer-lhe o mérito da franqueza..

O código-fonte, definição

A essência da inteligência de um sistema informático está no seu programa (em inglês: software). Este existe sob duas formas:

- O "código-fonte": escrito e legível por humanos, mais precisamente por uma categoria chamada programadores ou desenvolvedores. É a descrição metódica, nos mínimos detalhes, de tudo o que o programa faz. Esta descrição é digitada como você digitaria uma carta, mas em vez da sua língua, numa linguagem informática. Existem centenas delas, as mais conhecidas são o C, C++, Pascal, Basic, Java,... Estas linguagens têm como particularidade não permitir nenhuma ambigüidade, contrariamente às linguagens naturais onde uma palavra pode ter vários sentidos.
- O "código binário" ou "executável", formado de 0 e 1, portanto somente utilizável pelo computador. Ele é produzido automaticamente a partir do "código-fonte" por meio de um processo chamado compilador. Ele vai fazer o computador funcionar, no início um simples arranjo eletrônico inerte (em inglês: hardware).

Com a exceção notável dos softwares livres, você somente compra o direito de uso do executável. O código-fonte permanece secreto e propriedade de seu autor. Sem ele, você só pode observar o comportamento aparente do executável. Funcionalidades escondidas (ovos de Páscoa, *cheat codes, backdoor*...) não são reveladas se não se conhece a astúcia para dispará-las.

[61] Só a cadeia de produção é controlada pelo organismo de inspeção independente Ceten-Apave. Nenhuma informação sobre a ES&S iVotronic.