

VOTO ELECTRÓNICO

*Discussão técnica
dos seus problemas e oportunidades*

Edição:

Pedro Antunes

Autores (por ordem alfabética):

André Zúquete

António Ferreira

Carlos J. Costa

Domingos Magalhães

Duarte Vieira

Filipe Simões

João Ferreira Dias

Luís Carriço

Paulo Ferreira

Pedro Antunes

Rui Joaquim

Maio de 2008

Financiado pela

FCT Fundação para a Ciência e a Tecnologia

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR Portugal

ÍNDICE

Introdução	2
Voto electrónico	2
Tipos de sistemas	2
Propriedades	2
<i>Propriedades inerentes à democracia</i>	2
<i>Propriedades inerentes aos sistemas de votação electrónica</i>	2
<i>Requisitos desejáveis dos sistemas de votação electrónica</i>	2
Sistema genérico	2
<i>Comparação entre ambientes de votação</i>	2
Questão da caixa negra	2
Fontes de complexidade	2
Voto electrónico e resiliência	2
Riscos dos sistemas de votação electrónica	2
Riscos associados a falhas de sistema	2
<i>Falhas de componentes</i>	2
<i>Falhas de sistema</i>	2
Erro humano	2
<i>Lapsos e deslizes</i>	2
<i>Enganos relacionados com procedimentos</i>	2
<i>Enganos relacionados com conhecimento</i>	2
Riscos de sabotagem	2
Análise de riscos	2
Perspectiva técnico-jurídica	2
<i>Organizações Internacionais</i>	2
<i>Voto Electrónico</i>	2

<i>Quadro do sistema eleitoral em Portugal</i>	3
<i>Quadro para o voto electrónico em Portugal</i>	3
<i>Sobre a legislação a produzir em Portugal</i>	3
Arquitecturas	3
<i>Sistema proposto por Fujioka, et al.</i>	3
<i>Sistema FOO</i>	3
<i>Sistema EVOX</i>	3
<i>Sistema Sensus</i>	3
<i>Sistema REVS</i>	3
<i>Sistema proposto por Kofler, et al.</i>	3
<i>Oasis Election</i>	3
<i>Cybervote</i>	3
<i>Quadro resumo</i>	3
Arquitectura de referência	3
Perspectiva sobre o voto pela Internet	3
REVS – Um protocolo robusto de votação electrónica pela Internet	3
<i>Análise dos protocolos existentes</i>	3
<i>Arquitectura do REVS</i>	3
<i>Processo eleitoral no REVS</i>	3
<i>Avaliação do sistema REVS</i>	3
<i>Experiência</i>	3
MobileREVS - um sistema de votação electrónica para dispositivos móveis	3
<i>Requisitos específicos</i>	3
<i>Desafios técnicos</i>	3
<i>Arquitectura e processo de votação</i>	3
<i>Módulo Eleitor</i>	3
<i>Processo de votação</i>	3
Voto Electrónico	3

<i>Criptografia</i>	4
<i>Comunicação</i>	4
<i>Tratamento dos boletins de voto</i>	4
<i>Armazenamento</i>	4
<i>Avaliação das propriedades</i>	4
<i>Avaliação dos requisitos</i>	4
Suporte à mobilidade dos votantes	4
<i>Vulnerabilidades do Módulo Eleitor do REVS</i>	4
<i>Novo sistema do votante</i>	4
<i>Funcionalidade</i>	4
Votação electrónica no Brasil: reflexões	4
<i>Introdução</i>	4
<i>Montagem do sistema eleitoral</i>	4
<i>Arquitectura do sistema</i>	4
<i>Processo de votação</i>	4
<i>Resultados de auditorias</i>	4
<i>Reflexões</i>	4
Experiências europeias	4
<i>Síntese dos resultados das experiências europeias</i>	4
Experiências portuguesas de 2004 e 2005	4
<i>Análise dos relatórios de auditoria das experiências</i>	4
<i>Síntese dos resultados das experiências portuguesas</i>	4
Experiência portuguesa de 2004: Perspectiva técnica	4
<i>Sobre o contexto em que foi realizada a experiência</i>	4
<i>Sobre o papel dos avaliadores</i>	4
<i>Falhas detectadas relacionadas com os equipamentos</i>	4
<i>Falhas detectadas nos procedimentos de operação do sistema</i>	4
<i>Voto Electrónico</i>	4

<i>Falhas detectadas no processo de votação</i>	5
<i>Usabilidade dos dispositivos</i>	5
<i>Informação disponibilizada aos eleitores</i>	5
O caso das eleições na Flórida	5
Auditoria	5
<i>Objecto da auditoria</i>	5
<i>Definição da metodologia de avaliação</i>	5
<i>Definição dos objectivos a atingir</i>	5
Auditoria proactiva	5
Simulador de auditoria	5
<i>Característica técnicas do protótipo</i>	5
<i>Funcionalidades do protótipo</i>	5
Identidade digital e voto electrónico	5
Suspeições e teorias da conspiração	5
Mais propriedades	5
Ainda mais propriedades: A visão do Conselho da Europa	5
Pareceres oficiais	5
<i>Reino Unido</i>	5
<i>EUA</i>	5
<i>Comissão Europeia</i>	5
<i>Portugal</i>	5
Sobre os autores	5

INTRODUÇÃO

Pedro Antunes

Os sistemas de votação electrónica são sistemas que, quer pelas suas características e limitações quer pelo seu impacto social, estão actualmente sujeitos a um escrutínio muito cuidadoso em todo o mundo.

São de certo modo nobres os objectivos que levam ao desenvolvimento de sistemas de votação electrónica, sobretudo após um decréscimo significativo do interesse na participação em processos eleitorais que se tem vindo a verificar nas democracias ocidentais¹.

Proporcionar mais canais de voto, oferecer maior liberdade geográfica relativamente aos locais onde se pode exercer o direito de voto, desobrigando o eleitor de se apresentar em determinado local e período de tempo para votar, reduzir o número de votos nulos não intencionais, ou ainda garantir maior rapidez e exactidão na contagem dos votos são alguns dos objectivos fundamentais dos sistemas de votação electrónica.

No entanto todos estes benefícios têm de ser pesados face a um leque também alargado de riscos potenciais introduzidos pela tecnologia, de entre os quais se destacam os riscos de segurança e falha dos sistemas².

Apesar do desenvolvimento deste tipo de sistemas se centrar na aplicação de tecnologia já existente a um processo corrente em democracia, deve-se dar redobrada ênfase de que é crucial manter, ou mesmo reforçar, a confiança dos eleitores e do público em geral em todo o processo eleitoral, o que traz implicações fundamentais no desenvolvimento, teste, adopção e utilização de sistemas de votação electrónica.

Do ponto de vista da ciência informática, a questão fundamental que se coloca está em identificar qual a combinação óptima entre tecnologia e processos sociais que garanta um conjunto muito vasto de propriedades que a sociedade considera como adquiridas relativamente ao processo de votação. Os desafios são portanto inúmeros, desde a necessidade de garantir que um sistema de votação electrónica funciona em grande escala, sem problemas de fiabilidade e segurança que coloquem uma votação em causa; que o sistema seja capaz de garantir o aumento das oportunidades de voto e ao mesmo tempo o anonimato, privacidade, integridade dos votos e outras propriedades; que o sistema seja acessível e utilizável por uma enorme diversidade de pessoas; e, finalmente, que o sistema e processos eleitorais sejam facilmente compreendidos e aceites pelo cidadão comum e pelas entidades administrativas e políticas.

¹ Gerk, Ed, (2001). Voting Systems: From Art to Science, Voting Technology Conference, Caltech/MIT.

² Pratchett, L. (2002). The Implementation of Electronic Voting in the UK, De Montfort University of Essex, May.

Este documento procura contribuir para a compreensão e resolução dos problemas associados aos sistemas de votação electrónica. O documento está estruturado de uma forma intencionalmente simples, linear, capítulos curtos e um número limitado de citações bibliográficas. Mais do que construir uma argumentação sofisticada e profusa de citações, procurou-se apresentar os problemas e as soluções de forma directa e numa perspectiva eminentemente pragmática.

VOTO ELECTRÓNICO

João Ferreira Dias

Voto electrónico

A expressão “voto electrónico” pode ser utilizada numa acepção restrita ou numa acepção ampla. No primeiro caso, a expressão voto electrónico (por vezes referido como e-voto) é empregue como sinónimo de acto de votar; no sentido de que nos actos eleitorais ou referendários, o direito de voto pode ser exercido através de um dispositivo electrónico situado na assembleia de voto ou fora dela.

No segundo caso, aquela expressão abarca alguns ou todos os actos necessários à realização de eleições e referendos: o recenseamento, o acto de votar propriamente dito, a transmissão dos resultados parciais, e a publicação oficial dos resultados finais. Nesta acepção, voto electrónico e sistema de votação electrónica são sinónimos.

Teoricamente, é possível conceber um sistema de votação electrónica totalmente integrado por componentes electrónicos e/ou digitais. Na prática, porém, um sistema com essas características ainda não foi testado em eleições políticas de sufrágio universal. O que já é possível encontrar em vários países são sistemas mistos, em fase experimental ou já em uso (veja por exemplo o capítulo dedicado ao sistema brasileiro).

Os sistemas de votação electrónica mistos são sistemas parcialmente electrónicos, de extensão e complexidade muito variáveis, em que se mantém o carácter de processamento tradicional de algumas operações em articulação com a utilização de meios electrónicos para a realização de outras. Estes sistemas mistos podem empregar meios electrónicos apenas na fase de votar ou estenderem os referidos meios às fases de recolha e/ou contagem e/ou apuramento dos votos.

A utilização de meios electrónicos na fase da votação visa, em primeira linha, alargar a participação política dos cidadãos, abrindo novos canais que apelam mais a uma camada jovem 18-22, e agilizar a contagem de votos. A extensão desses meios a outras fases do processo eleitoral terá já como objectivo mais amplo a desburocratização, a celeridade processual e a redução de custos se associada a uma re-engenharia de processos nas mesas de voto.

A decisão de utilizar meios electrónicos, em menor ou maior grau, num determinado processo eleitoral passa não só pela respectiva realização técnica, mas também por opções políticas que deverão ter em conta as perspectivas técnicas, sociológicas, económicas e jurídicas deste fenómeno.

Voto electrónico presencial e não presencial

O emprego dos meios electrónicos na fase da votação propriamente dita é feito por uma de duas formas que são normalmente designadas pelas expressões “voto electrónico presencial” e “voto electrónico não presencial” (ou à distância). Trata-se de opções com implicações muito diferentes.

O voto electrónico presencial pressupõe a deslocação dos cidadãos à assembleia de voto, ou seja, em recinto controlado, a respectiva identificação dos cidadãos perante os membros da mesa, o exercício do direito de voto através da utilização de uma interface electrónica e/ou o respectivo depósito do voto numa urna electrónica.

São-lhe apontados três tipos de vantagens em relação ao sistema de votação tradicional. Em primeiro lugar, trata-se de uma forma de votar que torna o sufrágio potencialmente mais apelativo e acessível, designadamente no que se refere a eleitores com necessidades especiais (se a tecnologia for desenvolvida e configurada com esse fim em vista). Além disso, se o sistema estiver ligado através de uma rede de comunicação de dados, os cidadãos eleitores poderão votar numa qualquer mesa de voto. Por último, o processo permite caminhar na direcção da desburocratização e da conseqüente celeridade no apuramento dos votos.

Mais complexo do ponto de vista técnico e com evidentes implicações técnicas, políticas, sociológicas, económicas e jurídicas é o voto electrónico não presencial (à distância ou remoto). Trata-se de um processo em ambiente não controlado.

Neste sistema, o eleitor não tem de se deslocar a uma assembleia de voto. O voto é processado num dispositivo electrónico, que pode ser um computador pessoal ou até mesmo um telemóvel, desde que ligados a uma rede de comunicação de dados, como por exemplo a Internet. Após o processamento local, o voto é enviado automaticamente para um servidor onde é registado e incluído no apuramento.

As vantagens do voto remoto são: o sufrágio é mais apelativo, acessível e confortável, designadamente no que se refere a eleitores com necessidades especiais; o período de votação pode decorrer por um período temporal amplo; todo o processo é muito mais rápido e económico. No entanto, a garantia de algumas propriedades associadas à democracia (ver capítulo dedicado a esse tema) e a conformidade integral com os princípios jurídicos eleitorais (não assegura o segredo do voto, proporciona o chamado “voto familiar” ou, em última instância a “compra do voto”) é mais difícil de satisfazer tecnicamente o que alimenta a desconfiança dos cidadãos e acarreta uma atitude muito cautelosa dos políticos. Desaparece ainda o carácter simbólico que actualmente rodeia o sufrágio presencial.

Voto reversível

O conceito do “voto reversível” (ou voto sucessivo) é a possibilidade de votar várias vezes no mesmo acto eleitoral, apenas sendo validado o último voto. O voto reversível pretende dar resposta a “pressões” de compra de voto ou de voto familiar. Está por exemplo consagrado na Estónia em razão da introdução do voto em ambiente não controlado, e ainda na Suécia e Dinamarca, por força da maior sofisticação dos processos eleitorais naqueles países e pelo facto de o processo eleitoral se desenrolar muito mais rapidamente do que em Portugal.

Em geral, quando há voto reversível a votação electrónica remota decorre num período anterior à votação presencial para que a eventual expressão de voto presencial em ambiente controlado se sobreponha ao voto não presencial.

TIPOS DE SISTEMAS

Pedro Antunes

Um sistema de votação electrónica resulta da combinação de equipamento mecânico, electro-mecânico, electrónico e todo o tipo de software usados para implementar um processo eleitoral³. Há variadas formas de concretizar este objectivo. Neste capítulo iremos dar uma panorâmica geral sobre a implementação destes sistemas. Não se pretende dar uma perspectiva social nem política, focando antes nos aspectos tecnológicos.

Sistema de votação baseado em papel

Trata-se naturalmente do sistema tradicional, relativamente ao qual todas as comparações podem e devem ser realizadas. A votação em papel foi introduzida no século 19⁴, e é ainda hoje a forma de votação mais usada no mundo. De forma muito simplificada, o eleitor faz uma marca num boletim em papel e deposita-o numa urna, sendo os boletins contados manualmente quando termina o processo de votação.

Note-se que o facto de o sistema ser baseado em papel não significa que não seja utilizada tecnologia e em particular sistemas informáticos no apoio ao processo eleitoral. Significativo é o facto de o primeiro computador comercial (UNIVAC I) dos EUA ter sido desenvolvido para o organismo que realiza o censo demográfico, com implicações na definição das listas eleitorais. É também de realçar que o mesmo UNIVAC I serviu nas eleições americanas de 1952 para estimar os resultados eleitorais⁵.

Deve ainda ser referido que o sistema de votação em papel tem sido contestado em alguns países, designadamente no Brasil, por em determinadas condições permitir a fraude.

Sistema de alavancas

Com origem e uso nos EUA, o sistema de alavancas utiliza tecnologia electro-mecânica para recolher os votos dos eleitores. Os votos são registados em contadores, não exis-

³ Federal Election Commission (2001). Voting System Standards. July. Federal Election Commission.

⁴ The Caltech/MIT Voting Technology Project (2001). Residual Votes Attributed to Technology. Caltech/MIT.

⁵ Grad, B. The First Commercial Univac I Installation. The Software Industry Special Interest Group.

tindo portando necessidade de contagem. Não existe também possibilidade de recontagem dos votos.

O sistema de alavancas foi muito popular nos EUA por causa da quantidade de votações simultâneas que se realizam em alguns estados. Dada a dimensão física das máquinas utilizadas, o sistema de alavancas permite que o eleitor realize com facilidade dezenas de escolhas em simultâneo⁶. Este sistema está hoje obsoleto.

Sistema de cartões perfurados

Este tipo de sistema recorre a uma tecnologia de aquisição de dados muito comum nos anos 60 para automatizar a contagem de votos. Ao eleitor é fornecido um boletim em papel com um formato especial. Na cabina de voto, o eleitor coloca o cartão perfurado numa moldura e utiliza um objecto perfurante para identificar as suas opções de voto. O cartão perfurado é depois colocado numa urna, tal como no sistema de votação em papel. A contagem dos votos corresponde à contagem dos furos existentes nos cartões.

Este tipo de sistema ficou muito famoso, por maus motivos, nas muito contestadas eleições presidenciais Americanas de 2000⁷ (ver capítulo sobre as eleições na Flórida).

Sistema de leitura óptica

Este sistema destina-se a automatizar a contagem de votos através da leitura óptica dos boletins. Recorre a um processo de votação muito similar ao da votação tradicional em papel, onde o votante coloca o seu voto numa urna fechada. Note-se que, de modo a garantir o anonimato do votante, a colocação do boletim de voto na urna requer a utilização de um envelope especial.

Após o fim do processo de votação, os votos são passados pelo sistema de leitura óptica, que apresenta as contagens obtidas.

Este sistema pode ainda realizar a leitura imediata do boletim de voto, permitindo nesse caso ao votante verificar no próprio local se o seu voto está correcto⁸.

⁶ The Caltech/MIT Voting Technology Project (2001). Voting: What is What Could Be. Caltech/MIT.

⁷ Agresti, A. and B. Presnell (2002). Misvotes, Undervotes and Overvotes: The 2000 Presidential Election in Florida. *Statistical Science*, 17(4), pp. 436-440.

⁸ The Caltech/MIT Voting Technology Project (2001). Voting: What is What Could Be. Caltech/MIT.

Sistema baseado em máquinas electrónicas de registo directo⁹

Corresponde a uma versão electrónica das máquinas de alavancas. O primeiro modelo a operar com registo directo, largamente usado nos EUA, foi construído a partir da máquina de alavancas, exactamente por um construtor desse tipo de máquinas.

As máquinas electrónicas de registo directo registam os votos dos eleitores sem recorrer a suporte em papel. Normalmente os votos são armazenados na própria máquina durante o processo de votação. Após a votação, podem ser utilizados dois processos na contagem dos votos:

- A máquina apresenta uma contagem dos votos, seja em suporte de papel ou num ecrã;
- A máquina é temporariamente ligada a uma rede de comunicação de dados, transmitindo a contagem dos votos para um local que centraliza os resultados das eleições.

As máquinas electrónicas de registo directo apresentam tipos variados de interface com o eleitor, existindo versões com botões mecânicos, outras com teclado e algumas com ecrã táctil. Dada a sua flexibilidade e capacidade de interacção com os eleitores, este é o sistema que tem preferencialmente vindo a ser adoptado, designadamente nos EUA.

A possibilidade de este tipo de máquinas fornecer comprovativos em papel tem sido largamente debatida, designadamente nos EUA e no Brasil¹⁰. O recurso ao comprovativo em papel tem sido considerado fundamental para garantir a auditabilidade dos sistemas de votação electrónica¹¹. No entanto, a sua utilização levanta alguns problemas processuais, por exemplo, relativos aos procedimentos a adoptar no caso de a contagem electrónica não ser coerente com a contagem dos comprovativos em papel.

O Brasil, em Outubro de 2003, aprovou uma lei que eliminou a confirmação em papel no seu sistema de votação electrónica.

Sistema baseado na Internet

Trata-se de um sistema de votação electrónica em que os votos podem ser enviados pelos eleitores para a entidade organizadora das eleições através da infraestrutura Internet. A votação pela Internet realiza-se de forma não presencial.

⁹ DRE - *Direct Recording Electronic voting machines*.

¹⁰ Brunazo Filho, A. (1999). *A Segurança do Voto na Urna Eletrônica Brasileira*, Simpósio Sobre Segurança Informática. Brasil.

¹¹ Mercuri, R. (1992). *Physical verifiability of computer systems*. In 5th International Computer Virus and Security Conference.

Uma discussão mais alargada sobre este tipo de sistema será realizada em capítulo próprio.

PROPRIEDADES

Filipe Simões e Pedro Antunes

Apresenta-se neste capítulo introdutório um conjunto de propriedades que mais directamente se relacionam com os sistemas de votação electrónica. Por questões de organização e melhor entendimento, optámos por agrupar as propriedades em três grupos:

- Propriedades inerentes à democracia

Engloba um conjunto de propriedades que concretizam o conceito de democracia. Estas propriedades são inerente a qualquer processo de votação, independentemente de recorrer ou não a um sistema de votação electrónica.

- Propriedades inerentes aos sistemas de votação electrónica

Incluímos neste grupo as propriedades necessárias para garantir a credibilidade e a confiança nos sistemas de votação electrónica.

- Requisitos desejáveis dos sistemas de votação electrónica

Incorpora um conjunto de propriedades mais gerais, decorrentes de conhecimento empírico, experiência e boas práticas no desenvolvimento de sistemas informáticos.

Propriedades inerentes à democracia

Autenticidade

Apenas os eleitores autorizados devem poder votar. Autenticar o indivíduo é o meio pelo qual a identificação de um votante é verificada e validada.

Singularidade

O processo de votação deve garantir que os eleitores não possam votar mais do que uma vez em cada eleição. Para esse efeito deve ser realizado o registo do votante.

Direito de Voto

O Direito de Voto de um eleitor é uma propriedade que obriga à verificação simultânea das propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de o autorizar a votar.

Anonimato

A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam a manutenção do sistema) quer após a votação. O anonimato pode ter de ser garantido mesmo nas circunstâncias em que exista uma ordem administrativa ou judicial para analisar o processo eleitoral e os votos dos eleitores.

Integridade dos Votos

Os votos não podem ser modificados, forjados ou eliminados, quer durante quer após a conclusão do processo eleitoral.

Não-Coercibilidade

O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.

Privacidade

O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.

Propriedades inerentes aos sistemas de votação electrónica

Auditabilidade

O sistema deverá poder ser auditado quer por agentes independentes, através por exemplo da análise dos registos de eventos, quer pelo próprio sistema, através da confrontação automática dos diversos dados geridos pelo sistema.

Certificabilidade

O sistema deve poder ser testado e certificado por agentes independentes.

Confiabilidade

O sistema deve funcionar de forma robusta, tornando-se confiável ao olhos dos diversos actores que nele participam.

Detectabilidade

O sistema deve ter a capacidade para detectar tentativas de intrusão de agentes externos e dar alertas aos diversos operadores do sistema.

Disponibilidade

O sistema deve estar sempre disponível durante o período eleitoral, para que o processo decorra normalmente.

Integridade do Sistema

O sistema (visto do exterior) deve poder ser posto à prova por forma a validar que opera como previsto mesmo em situações excepcionais e condições extremas.

Invulnerabilidade

O sistema deve ter a capacidade de resistir a tentativas de intrusão e ataques de agentes externos. A invulnerabilidade do sistema deverá ser garantida através de mecanismos que sirvam de barreiras, defesas ou salvaguardas do mesmo.

Precisão

As eleições podem ser decididas por apenas um voto. O sistema não deve tolerar margens estatísticas de erro durante a sua operação.

Rastreabilidade

O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir registos de entrada e saída de utilizadores, bem como registos do envio e recepção de dados, que obviamente não comprometam as propriedades inerentes à democracia (Anonimato e Privacidade).

Recuperabilidade

No caso de ocorrência de falhas de componentes ou falhas de sistema, o sistema deve permitir a retoma da operação precisamente no ponto em que ocorreu a interrupção, sem perda de informação.

Verificabilidade

O sistema deve permitir a verificação de que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a Autenticidade dos registos dos votos sem no entanto quebrar as propriedades inerentes à democracia, como o Anonimato ou a Privacidade.

Requisitos desejáveis dos sistemas de votação electrónica

Autenticação dos Operadores

Os indivíduos autorizados a operar o sistema devem ser sujeitos a mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação actualmente existentes (cartões inteligentes, palavras-chave, biometria, impressão digital, retina ocular, voz, etc).

Documentação

Todo o projecto, realização e teste do sistema deve estar documentado, devendo não conter ambiguidades e ser coerente. Deve ser dada máxima atenção à documentação gerada ao longo de todo o processo de desenvolvimento, desde o estudo inicial dos requisitos do sistema, passando pelas várias fases evolutivas de construção, até à elaboração do manual de operação, continuando depois pelo registo das ocorrências ao longo da vida do sistema.

Cifra dos Dados

Os dados guardados nos servidores, bem como aqueles que viajam pela rede de comunicações, quer seja pública quer privada, devem encontrar-se cifrados.

Fisicamente Seguro

A segurança física dos diversos dispositivos ou componentes do sistema, incluindo servidores, consolas, computadores, periféricos, impressoras e cabos de alimentação e comunicação, deve ser garantida.

Integridade do Pessoal

O pessoal envolvido no projecto, desenvolvimento, administração, operação, distribuição e guarda de dados e equipamentos, deve ser incorruptível e de integridade inquestionável.

Política de Salvaguarda e Recuperação de Informação

O sistema deve prever mecanismos de prevenção e mitigação de uma possível perda de informação, quer seja causada por falhas de equipamento, falhas de software, erro humano, sabotagem ou mesmo desastres naturais. Devem existir políticas adequadas de gestão de cópias de segurança e recuperação de dados, e procedimentos de salvaguarda e de recuperação de dados.

Tolerância a Ataques

O sistema deve ser planeado e desenvolvido de raiz de acordo com o pressuposto de que será alvo privilegiado de ataques mal intencionados. As barreiras, defesas e salvaguardas, não só contra agentes externos mas também contra os próprios agentes que projectam e desenvolvem o sistema devem ser concebidas de raiz, ser rigorosas e redundantes.

Tolerância a Falhas

É desejável a existência de métodos de detecção e tolerância a falhas nos equipamentos e componentes do sistema. A falha de um componentes do sistema não deve impedir o normal decorrer do processo eleitoral, que está quase sempre delimitado do ponto de vista temporal.

SISTEMA GENÉRICO

Filipe Simões e Pedro Antunes

Neste capítulo abordamos a estrutura genérica de um sistema de votação electrónica. Esta informação será completada de forma bastante mais detalhada no capítulo dedicado às arquitecturas dos sistemas.

De forma genérica podem considerar-se quatro componentes que concretizam todo o processo eleitoral.

Registo do eleitor

Na perspectiva do sistema de votação electrónica, o componente de registo do eleitor realiza uma função essencial relacionada com a propriedade de Autenticidade: o registo prévio das pessoas que cumprem as condições de serem eleitores. Na fase de registo é necessário fornecer ao eleitor um mecanismo de comprovação da qualidade de eleitor, que pode consistir num cartão de eleitor, cartão inteligente, um envelope com uma palavra-passe de acesso ao processo de votação ou qualquer outra forma de identificação inequívoca perante o sistema de votação electrónica ou membro oficial, nomeadamente através de características bio-métricas.

O registo dos eleitores poderá ser realizado presencialmente (como acontece actualmente em Portugal, numa Junta de Freguesia) ou através de um processo remoto. Por exemplo, o estado da Califórnia (EUA) permite o registo do eleitor através de um mecanismo disponibilizado na Internet^{12 13}, sendo este complementado por um passo final que exige um documento em papel assinado pelo eleitor.

Note-se que o registo do eleitor é um componente integral do sistema de votação electrónica, não devendo ser considerado independente deste, por forma a evitar que falhas operacionais ou violação das propriedades do sistema sejam induzidas por problemas relacionados com o registo do eleitor.

Pré-Votação

O componente de pré-votação destina-se a proceder a um conjunto vasto de acções, essencialmente de natureza técnica, destinadas a preparar o processo eleitoral, incluindo-se:

¹² California Internet Task Force (2000). Final Report. California Secretary of State.

¹³ ovr.sos.ca.gov.

- Registo da eleição ou eleições, data de realização, período de eleição e locais de voto;
- Registo dos eleitores que podem exercer o seu direito de voto;
- Registo dos candidatos.

Num contexto não técnico, podem ainda ser consideradas nesta fase funções relacionadas com a divulgação do processo eleitoral ou mecanismos destinados a promover a disseminação de opiniões e o debate.

Votação

O componente de votação realiza o processo de votação propriamente dito. Este componente deverá permitir a identificação do eleitor, tendo por base uma interacção com a componente de registo, de forma a validar as condições de votação dos potenciais eleitores (Autenticidade e Singularidade).

Após validação das condições de votação, este componente procede à disponibilização de uma interface onde o eleitor poderá escolher as suas opções de voto. Esta funcionalidade envolve interacção com a componente de pré-votação. Consideram-se três ambientes distintos em que se poderá disponibilizar esta interface:

- Presencial e em recinto controlado. Os eleitores votam presencialmente em recinto controlado, à semelhança do que hoje acontece em Portugal, mas substituindo o voto em papel por outro em formato electrónico. Neste contexto são normalmente utilizadas máquinas electrónicas de registo directo do voto controladas por entidades oficiais.
- Presencial e em local público. Os eleitores votam num local público pré-determinado (supermercados, lojas dos correios, máquinas dispensadoras de dinheiro, ou outros locais preparados para o efeito). Neste contexto são utilizadas máquinas de registo directo do voto não controladas por entidades oficiais.
- Por acesso remoto. Os eleitores votam remotamente, através de qualquer ponto onde seja possível o acesso ao sistema de votação electrónica, como por exemplo através de um dispositivo ligado à infraestrutura da Internet ou a partir de um telefone fixo ou móvel.

Não conhecemos casos concretos em que tenha sido utilizada a votação presencial em local público, mas ela constitui uma possibilidade teórica. Tem como vantagens aumentar o número de locais onde o eleitor poderá votar, comparativamente ao ambiente de recinto controlado, mitigando também alguns problemas decorrentes da votação remota (e.g. impossibilidade de garantir a Privacidade e a Não-coercibilidade, dificuldade em garantir que a máquina e a rede de comunicação de dados são Fisicamente Seguras).

Contagem

O componente de contagem tem como finalidade o apuramento e contagem de todos os votos, bem como a publicação e divulgação dos seus resultados.

Devem ser consideradas duas variantes do componente de contagem:

- Contagem localizada, realizada em recinto controlado, sendo os votos posteriormente transmitidos a uma autoridade superior;
- Contagem centralizada, onde os votos são enviados para uma central de contagem.

Comparação entre ambientes de votação

A tabela abaixo apresenta uma comparação, identificando os pontos positivos e negativos, entre os três ambientes considerados para o processo de votação do ponto de vista das propriedades dos sistemas de votação electrónica.

Propriedades	Votação		
	Recinto controlado	Local público	Acesso remoto
Anonimato	+	+	+
Auditabilidade	+	+	+
Autenticação do Operador	+	-	-
Autenticidade	+	+	+
Certificabilidade	+	+	+
Cifra dos Dados	+	+	+
Confiabilidade	+	+	+
Detectabilidade	+	+	+/-
Disponibilidade	+	+	+
Documentação	+	+	+
Fisicamente Seguro	+	+/-	-
Integridade do Pessoal	+	-	-
Integridade do Sistema	+	+	+
Integridade dos votos	+	+	+
Invulnerabilidade	+	+	+
Não-coercibilidade	+	+/-	-

Política de Salvaguarda e Recuperação de Informação	+	+	+
Precisão	+	+	+
Privacidade	+	+	-
Rastreabilidade	+	+	+/-
Recuperabilidade	+	+	+
Singularidade	+	+	+
Tolerância a Ataques	+	+	+
Tolerância a Falhas	+	+	+
Verificabilidade	+	+	-

QUESTÃO DA CAIXA NEGRA

Pedro Antunes

No contexto da engenharia, designa-se caixa negra um sistema que, recebendo dados de entrada e produzindo dados de saída, não fornece para o exterior quaisquer indicações sobre o seu modo de funcionamento interno. O oposto do sistema caixa negra será um sistema do tipo caixa de vidro, capaz de mostrar de forma clara quais os seus componentes internos e a forma como estes se relacionam e operam em conjunto por forma a transformar os dados de entrada nos dados de saída.

No âmbito dos processos eleitorais e em particular dos sistemas de votação electrónica, a questão da caixa negra é fundamental para permitir discutir como é que se constrói uma relação de confiança entre os eleitores e um sistema votação electrónica.

O conceito de confiança tem evoluído significativamente ao longo do tempo, pelo que não tentaremos dar aqui uma definição precisa. No entanto, diremos que o conceito moderno de confiança integra¹⁴:

- Uma perspectiva racional sobre o objecto no qual se aplica a confiança;
- Um consenso razoável entre os membros da sociedade sobre os valores utilizados para avaliar a confiança;
- Um comprometimento de ambas as partes (quem avalia a confiança e o objecto de avaliação) relativo ao comportamento estável e previsível do objecto no qual se confia;
- A existência de reputação, i.e. informação pública sobre o comportamento do objecto no qual se confia.

Podemos assim analisar como construir a confiança num sistema de votação electrónica. Em primeiro lugar, por via de instituições que garantam a confiança no sistema: autoridades legais, organizações independentes de inspecção, certificação e auditoria, empresas reputadas no desenvolvimento de sistemas. Em segundo lugar, pela geração de consensos na sociedade resultantes de testes, ensaios e experimentação directa do sistema. E finalmente, pela capacidade do sistema de votação electrónica em gerar confiança no seu funcionamento.

Esta última via está necessariamente associada à questão da caixa negra: um sistema de votação electrónica que opera como uma caixa negra dificilmente será capaz de gerar confiança no seu funcionamento, pois não oferece mecanismos que permitam aos seus utilizadores analisar, avaliar e predizer o seu funcionamento.

¹⁴ O' Hara, K. (2004). *Trust: From Socrates to Spin*. Cambridge, UK, Icon Books, Ltd.

Ao invés, um sistema de votação electrónica do tipo caixa de vidro oferece esses mecanismos geradores de confiança: mostrando que componentes constituem o sistema, como se relacionam, que informação trocam, como actuam individual e colectivamente para realizar os objectivos previstos, e como actuam para evitar ou corrigir problemas.

Nesta perspectiva, analisemos diversas alternativas de implementação de um processo eleitoral. Dado que o nosso objectivo é discutir a questão da caixa negra, não será apresentado o processo eleitoral completo, sendo apenas ilustrado o processo de votação propriamente dito (e.g. sem considerar a pré-votação ou a contagem de votos).

Processo tradicional em papel

Este processo é aqui apresentado por constituir de facto o padrão de comparação que os eleitores utilizam para avaliar a confiança num sistema de votação electrónica. Numa perspectiva geral, o processo de votação em papel apresenta uma variedade de informação sobre o funcionamento interno que o permite considerar do tipo caixa de vidro¹⁵:

- Mesa de voto - Com um mecanismo simples e claro de verificação do Direito de Voto, Singularidade do voto e validação do votante recorrendo a listas de eleitores em papel, que podem ser facilmente controladas pelos membros da mesa;
- Câmara de voto - Oferecendo um mecanismo simples de garantia da Privacidade do votante;
- Urna - Mais uma vez, utilizando mecanismos simples de garantia da Singularidade e Anonimato do voto;
- Acrescem a estes componentes fundamentais do sistema, um conjunto diversificado de procedimentos que oferecem garantias adicionais, como sejam os procedimentos de verificação visual das urnas no início do processo, controlo de presenças no local de voto, contagem parcial dos votos, etc.

No geral, deve observar-se que este processo é bastante confiável se todos os procedimentos e salvaguardas instituídos forem seguidos, sendo ainda de relevar que esses procedimentos são observáveis, em muitos casos pelos eleitores e noutros casos pelos membros da mesa de voto.

É claro que o sistema falha se os procedimentos e salvaguardas não forem seguidos pelos membros da mesa de voto nem vigiados pelos eleitores. Uma das justificativas fortes para adoptar sistemas de votação electrónica, especialmente em países com significativos problemas a este respeito, deve-se a uma menor dependência deste ponto de falha.

¹⁵ Comissão Nacional de Eleições. Glossário, disponível em www.cne.pt.

Processo electrónico - solução maximalista

Uma solução maximalista para a implementação do processo de votação electrónica consiste em replicar todos os componentes do processo tradicional em papel:

- Mesa de voto electrónica - Com tecnologia para verificação do Direito de Voto recorrendo a listas de eleitores em formato digital.

Observa-se que o formato digital pode fornecer menos evidências de confiança que a versão em papel (já que a informação digital pode mais facilmente ser modificada fora do controlo dos membros da mesa). No entanto, podem mesmo assim os membros da mesa realizar um controlo razoável sobre a Autenticidade e a Singularidade do voto.

- Máquina electrónicas de registo directo - Com tecnologia para permitir ao eleitor seleccionar as suas preferências, garantindo a Privacidade.

A separação física entre mesa de voto e máquina de registo directo oferece uma garantia razoável de que será difícil relacionar um determinado registo de um votante e o seu voto, isto se estiver garantido que não existe um mecanismo de comunicação de dados entre estes componentes (excluindo uma ligação simples, por exemplo eléctrica, destinada a desbloquear a máquina de registo directo na altura de votar). Esta garantia não é no entanto tão forte como no caso do processo em papel já que, por exemplo, a existência de registos detalhados de operações mal concebidos pode nalguns casos permitir retrospectivamente associar os votantes aos votos.

- Urna electrónica - Com tecnologia para registar o voto do eleitor.

Essencialmente, a urna electrónica destina-se a dar garantias ao eleitor de que o voto realizado na máquina de registo directo será contado, é singular e é anónimo.

No geral, deve observar-se que este processo é bastante confiável por ser muito semelhante ao processo de votação em papel. As eventuais perdas de confiança resultam fundamentalmente da desmaterialização dos votos e de alguns processos, como o registo dos votantes ou a verificação de que a urna está vazia no início do processo. Em todo o caso, o sistema permite observar e verificar diversas funções importantes, relacionadas com a Singularidade, Anonimato e Privacidade.

Processo electrónico - solução intermédia

Uma solução intermédia para a implementação do processo de votação electrónica consiste em eliminar a urna:

- Mesa de voto electrónica - Como no caso anterior.
- Quiosque de votação - Agora combinando as funcionalidades da máquina electrónica de registo directo e da urna.

Esta solução destina-se naturalmente a simplificar o processo de votação e reduzir custos, em tempo e dinheiro, derivados da separação de funções por hardware distinto. No entanto, na perspectiva aqui em discussão, observa-se que o sistema retira informação sobre o seu funcionamento. Por exemplo, pode levantar-se a dúvida razoável sobre se o voto de um eleitor é ou não contado. Por isso mesmo, esta opção incorpora algumas características de caixa negra.

Processo electrónico - solução minimalista

Uma solução minimalista para a implementação do processo de votação electrónica consiste em eliminar a mesa de voto electrónica, restando um único componente:

- Quiosque de registo do votante e votação - Com tecnologia que combina as funcionalidades da mesa de voto, máquina de registo directo e urna.

De novo, esta solução destina-se a simplificar o processo de votação e reduzir custos (tempo, dinheiro, logística), pois todas as funções passam a estar integradas num único dispositivo. Observa-se que o sistema retira de novo informação sobre o seu funcionamento interno. Por exemplo, podem levantar-se dúvidas sobre o Anonimato dos votos, já que a autenticação do eleitor e a votação são realizados no mesmo dispositivo. Surge também o problema da Singularidade do voto, já que desaparecem mecanismos visíveis que ajudem a verificar se alguém vota mais de uma vez.

Concluindo esta discussão, observamos que a implementação de um sistema de votação electrónica pode adoptar um funcionamento que se aproxima mais da caixa de vidro, logo mais confiável, ou que se aproxima mais da caixa negra, eventualmente menos confiável. Neste último caso, observamos ainda que, face à ausência de mecanismos que criem confiança nos eleitores, estes terão de ser substituídos por outros, designadamente certificações e auditorias por instituições confiáveis. Retira-se assim a confiança dos cidadãos para as instituições.

FONTES DE COMPLEXIDADE

Pedro Antunes

O que torna um sistema de votação electrónica complexo? A questão é particularmente interessante porque, numa abordagem superficial, este tipo de sistemas não aparenta ser muito complexo, nem aparenta oferecer desafios tecnológicos ou científicos particularmente inovadores. No entanto essa complexidade efectivamente existe. Iremos recorrer a uma abordagem proposta por Kim Vicente¹⁶ para identificar as principais fontes de complexidade.

Espaço do problema alargado

Na verdade, um sistema de votação electrónica não pode ser resumido a um único problema - contar votos. Por detrás desse problema simples, encontram-se muitos outros problemas: como contar todos os votos, como garantir a comunicação de dados durante o período estipulado para a votação, como garantir o anonimato dos votos, como garantir que a votação é realizada de forma segura mas ao mesmo tempo anónima, como introduzir redundância no sistema, como garantir a disponibilidade do sistema face a um numero elevado de pedidos num mesmo instante, como garantir que o sistema é seguro e ao mesmo tempo auditável, como garantir que o sistema é seguro mas ao mesmo tempo simples de utilizar, como garantir que o sistema é simples de usar por todos os eleitores, que características têm todos esses utilizadores, como resolver problemas relacionados com os eleitores invisuais, mas também as pessoas que vêm mal, como garantir que o sistema é transparente, compreensível por todos os eleitores, o que fazer quando algo no sistema deixa de funcionar, o que pode deixar de funcionar, o que fazer quando as contagens de votos nuns dispositivos não correspondem às contagens de outros dispositivos, o que fazer quando um partido reclama sobre o funcionamento do sistema, etc.

¹⁶ Vicente, K. (1999). *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*, Lawrence Erlbaum Associates, Inc.

Natureza social

Um sistema de votação electrónica tem uma elevada componente tecnológica. No entanto apresenta também uma muito significativa natureza social. Por exemplo, relativa ao número e variedade de pessoas que podem operar o sistema. Em particular tem que se considerar que a função do sistema não é técnica mas política: o objectivo principal é eleger pessoas para cargos políticos, ou avaliar a posição dos eleitores perante uma determinada questão política. Neste contexto, funções técnicas como comunicar votos, confirmar votos ou contar votos são cruciais mas não correspondem à função principal do sistema.

Diversidade de visões sobre o sistema

Esta fonte de complexidade está relacionada com uma questão técnica que corresponde à especificação dos requisitos do sistema. Estes requisitos podem ser obtidos a partir de diversas origens, nas quais se incluem os organismos reguladores (dos processos eleitorais, da protecção dos dados, das actividades de engenharia, etc.), as instituições que adquirem ou certificam os sistemas, as organizações que desenvolvem software, os partidos políticos, os operadores do sistema, os auditores do sistema, o público em geral, etc. Ora muitas destas fontes de informação têm valores e visões diferentes sobre a natureza e função dos sistemas, o que naturalmente origina requisitos ambíguos e por vezes contraditórios que se tornam difíceis de clarificar, negociar e conciliar.

Distribuição

Um sistema de votação electrónica nacional é pela sua própria natureza um sistema distribuído e de grande escala. Ora, este tipo de sistemas tem requisitos técnicos complexos, por exemplo no que se refere à disponibilidade, segurança, sincronização e replicação dos dados. Sendo verdade que diversos sistemas distribuídos correntes operam sem grandes problemas técnicos, designadamente os sistemas bancários e as bolsas de valores, os sistemas de votação electrónica apresentam alguma complexidade adicional no que se refere à escala geográfica (milhares de dispositivos espalhados pelo país), disponibilidade (e.g. não é crítico procurar outro local onde levantar dinheiro, porque uma máquina não funciona, mas é crítico não poder votar no local designado), funcionamento em tempo real (o período de funcionamento do processo eleitoral está previamente fixado e é limitado no tempo) e afluxo dos utilizadores (que podem acorrer em simultâneo ao sistema).

Dinâmica

Um sistema de votação electrónica não tem uma dinâmica muito complexa, mas tem rigidez temporal. Considerando a diversidade de problemas, incidentes e acidentes que podem ocorrer, combinados com os períodos fixados para a realização do processo eleitoral, o recurso a determinados tipos de barreiras, defesas e salvaguardas pode ficar significativamente dificultado.

Acaso

Todos os sistemas dependem do acaso. No entanto, os sistemas que apresentem, como consequência desses acasos, significativos danos - no caso económicos, sociais e políticos - são naturalmente complexos. Uma das fontes de complexidade associadas ao acaso está na dificuldade em aplicar a estratégia de teste e erro. Não se nos afigura possível, por exemplo, realizar ensaios gerais de eleições nacionais. E temos de considerar que os ensaios localizados deste tipo de sistemas não permitem garantir o seu bom desempenho em larga escala. Ou seja, um sistema de votação electrónica tem de funcionar bem logo na primeira vez em que opera.

Acoplamento

Um sistema de votação electrónica é composto por um número significativo de subsistemas interligados e interdependentes, constituindo uma fonte de complexidade, já que a falha de um subsistema pode implicar falhas inesperadas em outros sistemas. Veja-se o capítulo sobre erro humano, onde são apresentados alguns exemplos de interacções inesperadas entre componentes de um sistema de votação electrónica.

Excepções

Todos os sistemas que aplicam automação estão sujeitos a problemas relacionados com o tratamento de excepções. No caso dos sistemas de votação electrónica, a automação de diversas funções, como por exemplo a recolha de votos, a contagem local de votos ou a transmissão electrónica de resultados, pode estar sujeita a excepções (e.g., o que fazer quando o utilizador se enganou? quando a contagem de votos apresenta um erro? quando o sistema não consegue transmitir os dados? quando um componente falha?). A fonte de complexidade está neste caso na necessidade de prever a ocorrência de excepções e mecanismos para o seu tratamento.

VOTO ELECTRÓNICO E RESILIÊNCIA

Pedro Antunes

O conceito de resiliência é relativamente recente. Na área da engenharia, só a partir de 2006 é que a engenharia da resiliência foi adequadamente definida e estruturada¹⁷. Numa perspectiva geral, a engenharia da resiliência preocupa-se com os riscos dos sistemas e a necessidade de tornar os sistemas e organizações complexos mais resistentes e flexíveis quando confrontados com vários tipos de falhas, incidentes e acidentes.

O conceito de resiliência integra diversos outros conceitos frequentemente associados ao combate a falhas de sistema e ao erro humano.

Resistência

Envolvendo a definição, concepção e desenvolvimento de mecanismos de defesa, barreiras e salvaguardas nos sistemas que os tornem mais protegidos contra ocorrências não desejadas, incluindo as falhas de sistema, o erro humano, as violações do sistema, ou os actos de sabotagem.

Flexibilidade

Capacidade para aplicar a criatividade e soluções de recurso, frequentemente envolvendo intervenção humana, no combate e prevenção dos acidentes de sistema.

Antecipação

Ao nível do planeamento e gestão operacional dos sistemas, considera-se fundamental adequar os sistemas e as organizações de regras, procedimentos, práticas, técnicas, mecanismos e ferramentas de antecipação dos riscos que podem ocorrer em sistemas complexos, considerando-se ainda nesta mesma perspectiva a capacidade de planeamento das acções que podem ser empreendidas para conter as consequências dos acidentes após a sua ocorrência.

¹⁷ Hollnagel, E., D. Woods and N. Levenson (2006). Resilience Engineering: Concepts and Precepts. Hampshire, England, Hashgate.

Adaptação

Capacidade para, de forma proactiva, planear e gerir as modificações dos sistemas requeridas quer pela inovação tecnológica, pela constante avaliação dos riscos, quer ainda pelo estudo de acidentes e incidentes que ocorram no sistema.

Recuperação

Capacidade para recuperar rapidamente um nível de funcionamento adequado aos objectivos do sistema após a ocorrência de incidentes ou acidentes.

Observa-se assim que o conceito de resiliência integra capacidades activas e proactivas de gestão dos riscos dos sistemas¹⁸. Este conceito é fundamental em áreas como a aviação, cuidados de saúde, gestão de infra-estruturas críticas (transportes, comunicações, distribuição de água, electricidade) e em indústrias complexas como a exploração petrolífera, petroquímica ou produção automóvel. Todos estes exemplos se caracterizam pelo elevado risco de operação e pelas consequências catastróficas derivadas da ocorrência de acidentes, com elevado impacto na saúde ou vida das pessoas, impacto económico ou impacto ambiental.

Considerando os casos referidos acima, surge naturalmente a dúvida sobre se um sistema de votação electrónica se enquadra neste âmbito. É verdade que a falha de um sistema de votação electrónica não tem impacto directo ao nível da saúde ou vida das pessoas, nem no ambiente. Poderá eventualmente ter um significativo risco económico, em particular nas empresas que desenvolvem este tipo de tecnologia. No entanto os sistemas de votação electrónica têm potencial para apresentar um elevado risco social:

- Desacreditar um determinado processo eleitoral, ou mesmo todo o sistema eleitoral de uma região ou país;
- Em sequência, desacreditar as instituições e pessoas que governam um país;
- E finalmente, desacreditar o próprio conceito de democracia.

Nesta perspectiva julgamos que os sistemas de votação electrónica se devem enquadrar no conjunto de sistemas alvo da engenharia da resiliência. As vantagens deste enquadramento são muito significativas, pois permitem aproveitar uma enorme quantidade de informação e experiência aplicada na compreensão das falhas de sistema, erro humano e interacções complexas que levam à ocorrência de acidentes, assim como dos mecanismos de defesa, barreiras e salvaguardas desenvolvidos para evitar e combater os acidentes e

¹⁸ Sheffi, Y. (2007). *The Resilient Enterprise*. Cambridge, MA, MIT Press.

delimitar os seus danos. Apresentam-se em seguida alguns princípios fundamentais da engenharia da resiliência com aplicação directa nos sistemas de votação electrónica:

- As falhas de componentes e falhas de sistema, assim como o erro humano, não são totalmente previsíveis, pelo que não podem ser totalmente evitáveis. Por outro lado, ao longo do tempo tem-se vindo a verificar que a complexidade tecnológica dos sistemas tem aumentado, o que aumenta o risco de acidentes devidos às interacções complexas entre os seus componentes. Logo, os acidentes são ocorrências normais na vida dos sistemas complexos. Esta é a chamada “teoria dos acidentes normais”¹⁹.
- Uma consequência importante da teoria dos acidentes normais é que os sistemas de votação electrónica devem ser desenvolvidos na assunção de que as falhas vão ocorrer, apesar de não ser totalmente previsível que falhas vão ocorrer. Consequentemente, os sistemas de votação electrónica devem ser equipados com barreiras, defesas e salvaguardas contra falhas de sistema e erro humano.
- A resiliência envolve um compromisso organizacional com a segurança (incluindo segurança operacional) dos sistemas. Este compromisso deve ser estendido a todas as organizações envolvidas no processo de votação, incluindo em particular as empresas que fornecem e desenvolvem software para sistemas de votação electrónica. Resulta deste compromisso a adopção de regras, procedimentos e melhores práticas sobre a segurança dos sistemas, assim como a utilização de mecanismos organizacionais que realizem o seu controlo operacional.
- A resiliência envolve um entendimento alargado sobre o que é um sistema. Um sistema de votação electrónica envolve não apenas a tecnologia mas também os seus diversos operadores, o treino desses operadores, os procedimentos e manuais de operação, documentação técnica descrevendo o sistema, especialmente a destinada aos eleitores e aos auditores do sistema. Todos estes componentes do sistema estão sujeitos a falhas e podem estar na origem de acidentes de sistema.
- A resiliência envolve análise e gestão de riscos. O desenvolvimento de um sistema de votação electrónica deve ser acompanhado de estudos conducentes à análise, modelação e estimação dos riscos associados a este tipo de sistemas. Estes estudos são parte integrante e fundamental da fase de análise típica em qualquer projecto de desenvolvimento de software, por forma a garantir que a segurança do sistema é concebida desde o início do projecto. Estes estudos são igualmente fundamentais na fase de testes de um sistema de votação electrónica. No geral, tal significa que o processo de desenvolvimento de um sistema de votação electrónica é bastante mais complexo que o processo de desenvolvimento de software tradicional.

¹⁹ Perrow, C. (1999). *Normal Accidents, Living with High-Risk Technologies*. Princeton, New Jersey, Princeton University Press.

RISCOS DOS SISTEMAS DE VOTAÇÃO ELECTRÓNICA

Pedro Antunes e Filipe Simões

Como já foi dito, não há sistemas infalíveis. Os sistemas de votação electrónica, pela complexidade que envolvem, encontram-se sujeitos aos mesmos tipos de falhas e erros humanos que ocorrem em todos os sistemas complexos.

Neste pressuposto, as abordagens ao desenvolvimento dos sistemas de votação electrónica devem considerar desde a sua génese a existência de riscos e a consequente necessidade de gerir esses riscos, seja pela via da prevenção, mitigação ou contenção das suas consequências.

Adaptamos o modelo de Reason²⁰ para analisar os riscos dos sistemas de votação electrónica em três grandes grupos:

- Falhas de sistema;
- Erro humano;
- Sabotagem.

Por outro lado, uma visão sistémica é fundamental na compreensão dos sistemas de votação electrónica, isto porque não é possível dissociar o sistema técnico (infraestrutura de suporte) dos seus utilizadores durante o processo eleitoral (eleitores e operadores) e outros intervenientes (e.g., auditores, técnicos que configuram e mantêm o sistema), assim como da sociedade em geral (que exige e garante a democracia). A falha de um destes componentes leva à falha de todo o sistema de votação electrónica.

Nesta vertente do problema, a complexidade na avaliação dos sistemas de votação electrónica resulta da necessidade de analisar um conjunto vasto de questões fronteira: o processo eleitoral (registo dos eleitores, votação e contagem) e outros processos relacionados, incluindo o da própria auditoria, a gestão de uma mesa de voto e a divulgação de resultados. Uma questão chave que é fundamental analisar é a visibilidade e transparência necessárias para uma aceitação pela sociedade do processo eleitoral.

Note-se que existe um risco muito elevado de a sociedade rejeitar o novo processo eleitoral simplesmente porque, em contraste com o processo antigo, se pode transferir o controlo de qualquer eleitor (que pode pertencer a uma mesa de voto) para especialistas

²⁰ Reason, J. (1990). *Human Error*, Cambridge University Press.

em informática. Esta questão tem sido muito veementemente levantada nos EUA, a propósito, por exemplo, da falta de confirmação do voto por recibos em papel e impossibilidade de recontagem dos votos.

Nos próximos capítulos iremos analisar com detalhe os tipos de riscos aqui identificados.

RISCOS ASSOCIADOS A FALHAS DE SISTEMA

Pedro Antunes

Utilizando um modelo proposto por Perrow²¹, um sistema complexo pode ser analisado em quatro níveis distintos:

- Parte - O componente mais pequeno do sistema que pode ser analisado;
- Unidade - Um conjunto de partes relacionadas funcionalmente;
- Subsistema - Um conjunto coerente de unidades;
- Sistema - Uma colecção de subsistemas.

Considera-se que uma falha corresponde à incapacidade de uma parte, unidade, subsistema ou sistema em desempenharem as suas funções de acordo com os requisitos especificados²².

Recorrendo ainda ao modelo proposto por Perrow, pode fazer-se a distinção entre falha de componente e falha de sistema:

- Falha de componente - Envolve a falha de um ou mais componentes do sistema (partes, unidades ou subsistemas), que estão ligados de forma conhecida;
- Falha de sistema - Envolve uma interacção não esperada entre múltiplas falhas de componentes.

Falhas de componentes

As falhas de componentes de um sistema de votação electrónica podem ter várias causas:

- Acidentes da natureza

²¹ Perrow, C. (1999). *Normal Accidents, Living with High-Risk Technologies*. Princeton, New Jersey, Princeton University Press.

²² IEEE 610.12-1990.

Inundação, incêndio, curto-circuito, etc.

- Falhas de energia

As falhas de energia podem afectar um ou mais componentes do sistema de votação electrónica.

- Falhas de hardware

Quando um dispositivos físico do sistemas de votação electrónica falha, por exemplo por sobre-aquecimento, envelhecimento ou deterioração por uso intensivo. Os dispositivos de interface com os utilizadores estão particularmente sujeitos à deterioração por uso.

- Falhas de software

Quando um dispositivo lógico do sistema de votação electrónica falha devido a erros (*bugs*) de software. A ocorrência de erros de software nos sistemas é bem conhecida, mesmo em sistemas com longos períodos de maturação.

- Falhas de canais de comunicação

Ocorrem quando componentes que têm que comunicar entre si não o conseguem fazer.

Os riscos associados a falhas de componentes são normalmente mitigados através de redundância (por exemplo, várias urnas onde colocar os votos, fontes de energia alternativa), substituição (máquinas de voto de substituição) ou recurso a procedimentos alternativos (por exemplo, votação em papel).

Existe uma vasta literatura científica com dados estatísticos sobre falhas de componentes em vários sectores. Por exemplo, na área dos sistemas de distribuição eléctrica, a taxa de falhas de um transformador industrial é de 0.5 / 100 transformadores, ano²³.

Na área da votação electrónica os dados existentes são escassos mas indicam valores substancialmente mais elevados. Um artigo de Kai Larsen²⁴ refere que 17.7% das máquinas de voto utilizadas numa eleição na Noruega falharam.

Um estudo realizado na Flórida indicou uma taxa de falha durante o período de votação de 6%²⁵ (se bem que estes dados podem englobar erro humano). Um estudo realizado na Califórnia²⁶ indicou uma taxa de falha de cerca de 20%.

²³ Roos, F., Lindahl, S. (2004). Distribution System Component Failure Rates and Repair Times – An Overview, Nordic Distribution and Asset Management Conference 2004.

²⁴ Larsen, K. (1999). Voting technology implementation, Communications of the ACM 42(12).

²⁵ Stephen, A. (2000). A Black view of the US, New Statesman, 129(4514).

Outros dados empíricos²⁷ indicam taxas de falha de componentes no dia das eleições de cerca de 10%.

Falhas de sistema

As falhas de sistema são devidas à interacção complexa (inesperada ou não antecipada) de várias falhas de componentes, eventualmente combinadas com erro humano. De acordo com Perrow²⁸, podem ser identificadas três fontes principais de interacção complexa.

Funções de modo comum

Quando o sistema utiliza funções que dependem umas das outras, pelo que falham em conjunto. Um exemplo concreto é a dependência do sistema de votação electrónica de um sistema operativo.

Proximidade

Os componentes independentes mas fisicamente próximos tendem a falhar em conjunto. Note-se que, apesar de um sistema de votação electrónica ser naturalmente descentralizado, normalmente há mesas eleitorais e máquinas de votação suficientemente próximas para poderem sofrer deste tipo de falha.

Fontes indirectas

Quando as interacções entre componentes não são totalmente visíveis ou compreensíveis, por exemplo por existir retroalimentação, demasiadas variáveis em jogo ou automação de funções. Um exemplo concreto de fonte indirecta de complexidade foi observado na auditoria realizada nas eleições Europeias de 2004²⁹, quando se observou que todo o pro-

²⁶ California Secretary of State's Voting Systems Technology Assessment Advisory Board (2005). Analysis of Volume Testing of the AccuVote TSx/AccuView.

²⁷ Stanislevic, H. (2006). DRE Reliability: Failure by Design? VoteTrustUSA E-Voter Education Project, www.votetrustusa.org.

²⁸ Perrow, C. (1999). Normal Accidents, Living with High-Risk Technologies. Princeton, New Jersey, Princeton University Press.

²⁹ Pedro Antunes, Nuno neves, Luís Carriço, Paulo Veríssimo, Rui Rocha Pinto, Filipe Simões (2004). Projecto de Avaliação de Sistemas de Votação Electrónica – Resultados da Auditoria.

cesso de verificação dos votantes realizado na mesa de voto era afectado por uma quantidade inesperada de repetições do acto de votar, decorrentes de erros dos votantes; que por sua vez eram provocados por um problema inesperado nas interfaces dos dispositivos utilizados pelos eleitores.

Uma forma comum de reduzir as falhas por fontes indirectas consiste em reduzir o acoplamento entre os diversos componentes do sistema de votação electrónica, seja ao nível do hardware (utilizando hardware diferente para funções diferentes, como sejam a verificação dos votantes e a entrega dos votos), software (evitando a utilização de pacotes de software que suportam simultaneamente várias funções) ou das comunicações (por exemplo restringindo o período em que as máquinas de voto comunicam com servidores centrais).

Note-se no entanto que não há registos significativos de falhas de sistema em sistemas de votação electrónica. Larsen³⁰ refere um problema na Noruega, em 1993, que originou uma crise parlamentar que durou um mês. Nos EUA, um relatório de representantes do partido Democrata³¹ identificou um conjunto numeroso de irregularidades que cumulativamente afectaram centenas de milhar de votos nas eleições presidenciais do Ohio em 2004.

³⁰ Larsen, K. (1999). Voting technology implementation, *Communications of the ACM* 42(12).

³¹ House Judiciary Committee Democratic Staff (2005). *Preserving Democracy: What Went Wrong in Ohio*.

ERRO HUMANO

Pedro Antunes e Filipe Simões

A questão do erro humano em sistemas de votação electrónica tem sido muito pouco discutida pela comunidade. No entanto estão disponíveis dados científicos que evidenciam que este é um aspecto crítico dos sistemas de votação electrónica. Um dos estudos mais conhecidos é o da Caltech/MIT^{32 33} que analisou e estimou a perda de votos em diversas eleições nos EUA entre 1988 e 2000 devidos a erro humano. Um outro estudo seminal nesta área foi conduzido por Susan King Roth³⁴ nos EUA e permitiu identificar diversos factores humanos que influenciam os resultados eleitorais, designadamente por os eleitores acabarem por votar em candidatos que não pretendiam seleccionar.

Um caso concreto e muito discutido de erro humano em sistemas de votação electrónica foi o das eleições para a presidência Americana de 2000, onde se admite que o desenho dos boletins de votação utilizados no estado da Flórida terá influenciado decisivamente o resultado eleitoral^{35 36 37}.

Na discussão deste problema iremos recorrer ao modelo proposto por Reason³⁸ que classifica o erro humano em três categorias:

- Lapsos e deslizes

Erros resultantes de falhas na execução (deslizes) ou memorização (lapsos) de uma acção ou uma sequência de acções.

- Enganos relacionados com procedimentos

Deficiências ou falhas cognitivas na selecção ou na aplicação de um plano de acção.

- Enganos relacionados com conhecimento

³² Caltech/MIT Voting Technology Project (2001). Voting: What Is, What Could Be.

³³ Caltech/MIT Voting Technology Project (2001). Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment.

³⁴ Susan King Roth (1998). Disenfranchised by design: voting systems and the election process, *Information Design Journal* (9)1.

³⁵ Alan, M Dershowitz (2005). *Supreme Injustice*, Oxford University Press.

³⁶ Tomz M., Houweling R. (2003). How Does Voting Equipment Affect the Racial Gap in Voided Ballots?, *American Journal of Political Science*, 47(1).

³⁷ Walter R. Mebane Jr. (2004). The Wrong Man is President! Overvotes in the 2000 Presidential Election in Florida, *Perspectives on Politics*, 2(3).

³⁸ Reason, J. (1990). *Human Error*, Cambridge University Press.

Deficiências ou falhas cognitivas na identificação ou resolução de um problema e na definição de um plano de acção.

Lapsos e deslizes

A lista de potenciais lapsos e deslizes é muito grande, pelo que apenas apresentamos aqui alguns dos casos mais representativos.

Voto “ao lado”

O fenómeno do voto ao lado consiste, basicamente, no eleitor seleccionar uma opção de voto que está próxima daquela que efectivamente pretendia. Trata-se de um tipo de erro que tem sido recentemente estudado e que ocorre entre 0,5 a 3% das vezes³⁹.

Confirmações de voto

A confirmação de voto é realizada pelo eleitor após ter seleccionado um ou vários candidatos (no caso de se realizarem diversas eleições em simultâneo) e corresponde normalmente a uma acção cognitiva de verificação dos dados introduzidos e a uma acção motora de confirmação desses dados por pressão num botão.

A confirmação de dados pode dar origem a um lapso, caso o eleitor se apresse a confirmar o seu voto sem realmente se assegurar da sua intenção. Ou ainda se simplesmente activar o processo de confirmação de voto não intencionalmente (carregando sem querer no botão de confirmação).

Há estudos de usabilidade que indicam que um grande número de utilizadores seleccionam a opção “sim” sem sequer lerem a questão⁴⁰, pelo que a técnica de pedir a confirmação não é eficaz na mitigação deste risco.

Outras técnicas comuns de mitigação deste risco, como a reversão das operações (*undo*) não podem ser adoptadas pois questionam a integridade dos votos.

³⁹ T. Selker, J. Goler, L. Wilde (2005). Who does better with a big interface? Improving Voting Performance of Reading Disabled Voters. MIT/Caltech Voting Technology Project.

⁴⁰ Zurko, M.E., Kaufman, C., Spanbauer, K., Bassett, C. (2002). Did you ever have to make up your mind? What Notes users do when faced with a security decision, Proceedings of 18th Annual Computer Security Applications Conference, IEEE Computer Society.

Este tipo de risco pode ser prevenido através da realização de estudos de usabilidade dos dispositivos que interagem com os votantes.

Operações da mesa de voto

As operações que envolvem a mesa de voto no controlo do funcionamento das máquinas de voto podem originar deslizes. Um exemplo deste tipo de deslize, que foi detectado na auditoria realizada nas eleições Europeias de 2004⁴¹, foi a autorização de um eleitor que não correspondia ao que se apresentou na mesa, porque o membro da mesa seleccionou com o rato o eleitor que estava na posição acima do caderno eleitoral.

Uma forma de prevenir este tipo de risco consiste em desenvolver um modelo mental simples e claro do funcionamento da mesa de voto. A mitigação também é possível, dando ao operador maior flexibilidade na selecção dos eleitores que já votaram, mas tem de ser combinada com mecanismos de registo desse tipo de operações, de forma a garantir a autenticidade e singularidade do voto, e a auditabilidade do sistema.

Enganos relacionados com procedimentos

Se algum dos procedimentos exigidos para o normal funcionamento do sistema de votação electrónica não for cumprido, seja por esquecimento, desleixo, simples incompetência ou desconhecimento, aumenta-se o risco de as propriedades inerentes à democracia serem violadas. Apresentam-se alguns exemplos deste tipo de riscos.

Enganos nos procedimentos de abertura e fecho do processo de votação

Podem ocorrer enganos na abertura e no fecho do processo de votação. Exemplos deste tipo de ocorrência são a não inicialização dos dispositivos e respectivos contadores, a não selagem dos dispositivos no fecho do processo de votação, ou a não impressão dos registos de contagem.

⁴¹ Pedro Antunes, Nuno Neves, Luís Carriço, Paulo Veríssimo, Rui Rocha Pinto, Filipe Simões (2004). Projecto de Avaliação de Sistemas de Votação Electrónica – Resultados da Auditoria.

Diversos estudos sobre a operação de sistemas socio-técnicos indicam que a incidência deste tipo de enganos é elevada⁴², por razões cognitivas, sendo aconselhável desenvolver no sistema de votação electrónica mecanismos de controlo dos procedimentos de abertura e fecho do processo.

Enganos nos procedimentos de operação

O processo de votação envolve diversos procedimentos que devem ser realizados pelos membros oficiais, que incluem a verificação da autenticidade do eleitor e singularidade do voto, autorização para votar, confirmação ou não de que o eleitor realmente votou.

Podem ocorrer enganos na selecção desses procedimentos derivados da não aplicação dos procedimentos correctos ou aplicação errada dos procedimentos correctos.

Este tipo de enganos está associado a sobrecarga de informação (e.g., demasiados eleitores processados em simultâneo, demasiado ruído), rigidez dos procedimentos, ou equívocalidade dos procedimentos.

Como forma de prevenção, é necessário garantir uma adequada formação dos operadores e realizar estudos de usabilidade que conduzam à redução da sobrecarga de informação.

As técnicas de mitigação deste tipo de risco centram-se normalmente na possibilidade de reverter operações.

Enganos nos procedimentos de tratamento de excepções

O processo eleitoral, pela sua complexidade, está sujeito à ocorrência de eventos não previstos ou de eventos que, estando previstos, fogem ao padrão normal.

É natural a existência de procedimentos de emergência para fazer face à ocorrência destas excepções. Por exemplo, utilizando a votação tradicional em papel para resolver um problema de falha de energia ou falha de um componente ou dispositivo.

No entanto, a selecção e aplicação dos procedimentos adequados para fazer face a essas excepções está sujeita a enganos. Este tipo de risco pode ser prevenido através da formação dos operadores e desenvolvimento de manuais de operação com incidência sobre o tratamento de excepções.

⁴² Reason, J. (1997) *Managing the Risks of Organizational Accidents*. England, Ashgate Publishing.

Enganos relacionados com conhecimento

Violação de procedimentos de segurança

Esta categoria engloba violações intencionais directamente relacionadas com os procedimentos de segurança do processo eleitoral como, por exemplo, a selagem de dispositivos ou o controlo de acesso aos dispositivos.

O estudo da operação de sistemas socio-técnicos indica que, mesmo em sistemas de elevado risco e com procedimentos de segurança muito estritos, como a produção de energia nuclear ou a pilotagem de aviões, ocorrem violações intencionais⁴³.

As violações intencionais são normalmente realizadas por motivos de optimização de esforço e estão directamente associadas a diversas limitações cognitivas dos operadores, como por exemplo a excessiva confiança, complacência ou simplificação da realidade.

Um aspecto importante a considerar no desenvolvimento de mecanismos de prevenção deste tipo de riscos é o desenvolvimento de uma cultura de segurança.

Violação de procedimentos de operação

Corresponde a enganos intencionais directamente relacionados com os procedimentos de votação, normalmente realizados por motivos de optimização de esforço. Dois exemplos são a não verificação do direito de voto de um eleitor ou a não confirmação de que o eleitor realmente votou.

De novo, este tipo de risco está directamente associado à excessiva confiança, complacência ou simplificação da realidade.

Enganos relacionados com o modelo mental do operador

Michael Duffy⁴⁴ descreve uma situação em que uma votante se dirigiu à máquina de voto, percorreu as diversas opções de voto, sem no entanto escolher qualquer candidato, e foi

⁴³ Perrow, C. (1999). *Normal Accidents, Living with High-Risk Technologies*. Princeton, New Jersey, Princeton University Press.

respondendo afirmativamente a todas as interrogações do sistema. Depois, dirigiu-se à mesa de voto indicando que já tinha experimentado a máquina e portanto desejava votar. No entanto, tal já não era possível pois o sistema tinha interpretado o teste inicial como um voto. Este exemplo ilustra um engano gerado pela incompatibilidade entre o modelo mental do operador e o modelo de funcionamento do sistema.

⁴⁴ Duffy, M. (2006). Can This Machine Be TRUSTED? *Time*, 168(19).

RISCOS DE SABOTAGEM

Pedro Antunes e Filipe Simões

Como riscos de sabotagem agrupamos os potenciais actos provocados por um atacante que tem como objectivo influenciar ou impedir o correcto desenrolar do processo eleitoral.

Negação de Serviço

A negação de serviço ocorre quando um atacante consegue tornar indisponível um serviço do sistema através de solicitações sucessivas que levam à exaustão dos recursos desse serviço.

O componente do sistema de votação electrónica mais crítico é naturalmente o de contagem dos votos, pois está no caminho crítico de todo o processo de votação. No caso dos sistemas de votação que utilizam a infraestrutura Internet, os servidores de acesso ao sistema também estão especialmente sujeitos a este tipo de sabotagem.

A técnica mais comum de prevenção e mitigação deste risco consiste na utilização de componentes redundantes.

Intercepção

Os riscos de intercepção estão associados à capacidade de um atacante interceptar os votos que viajam pela rede de comunicação de dados. Todos os componentes do sistema de votação electrónica estão sujeitos a este tipo de risco, que questiona duas propriedades inerentes à democracia: o Anonimato e a Integridade dos Votos.

Uma forma comum de prevenir a intercepção é a utilização de redes privadas de comunicação de dados, como por exemplo a rede do Ministério da Justiça.

Os mecanismos de mitigação deste tipo de risco tendem a ser muito complexos, pois podem colidir com as propriedades inerentes à democracia, das quais se destaca o Anonimato.

Mascaramento

O mascaramento é um tipo de sabotagem onde um atacante simula uma identidade oficial da organização, oferecendo componentes e serviços que tentam captar informação

vital do sistema de votação electrónica, como sejam as credenciais dos votantes ou os próprios votos.

Este risco é especialmente relevante nos sistemas de votação que usam a infraestrutura Internet.

Código malicioso

Este tipo de risco ocorre quando um pedaço de código malicioso, previamente inserido no sistema de votação electrónica, permite eliminar ou alterar um voto, identificar quem e como alguém votou, votar por substituição de alguém, ou mesmo manipular os resultados de uma votação.

Este tipo de risco tem uma natureza diferente dos anteriores, pois está associado a uma sabotagem realizada a partir do “interior” do sistema de votação electrónica, podendo ocorrer nas fases de desenvolvimento de software, preparação ou operação do sistema.

Uma forma de prevenir este tipo de riscos consiste em auditar todos os componentes do sistema de votação electrónica em todas as suas fases de desenvolvimento e selar esses componentes antes do início do processo de votação.

Vírus e Cavalos de Tróia

Os ataques por vírus e Cavalos de Tróia são muito comuns e estão associados a vulnerabilidades dos sistemas operativos e das aplicações informáticas.

Normalmente o atacante consegue alojar no sistema pedaços de software com a capacidade para se esconderem, sobreviverem longos períodos de tempo, eventualmente adormecidos, e que após acordarem podem invadir outros sistemas.

Existem diversas formas de prevenção deste tipo de riscos, das quais se destacam os vulgares anti-vírus e a re-instalação completa dos sistemas operativos a partir de fontes limpas imediatamente antes do processo de votação.

Deve no entanto notar-se que os anti-vírus, pela sua própria natureza, são apenas capazes de prevenir vírus conhecidos, pelo que não são adequados para sistemas de votação electrónica.

Uma forma de prevenção mais eficaz consiste na utilização de sistemas operativos especificamente desenvolvidos para sistemas de votação electrónica.

Uma forma de mitigação deste risco consiste em diversificar a origem, natureza e funcionalidade dos sistemas e dispositivos utilizados nos processos eleitorais.

Acessos não autorizados ao hardware

O acesso não autorizado a dispositivos físicos, como o ecrã, o teclado e rato, ou interfaces para dispositivos periféricos (e.g, portas série, USB, *firewire*) podem permitir a um atacante quebrar o anonimato ou privacidade do voto. Exemplos concretos são a leitura dos movimentos do rato ou da pressão das teclas que permitem captar informação confidencial como palavras passe e sentido do voto.

Este tipo de riscos pode fundamentalmente ser mitigado através da auditoria aos sistemas de votação electrónica.

Acesso não autorizado ao software

Este tipo de risco tem uma natureza semelhante ao anterior, apesar de colocar desafios substancialmente diferentes. Ele está relacionado com vulnerabilidades do tipo engenharia social, onde os operadores são manipulados de forma a fornecer informação ou realizar operações indevidas, como seja a reinicialização de dispositivos.

ANÁLISE DE RISCOS

Carlos J. Costa e Pedro Antunes

Se os sistemas de votação electrónica apresentam muitos benefícios, também trazem riscos adicionais. Como já vimos, o processo eleitoral pode falhar devido a falhas de componentes, erro humano e sabotagem. Estes riscos adicionais são inerentes à dependência quer da tecnologia quer das pessoas. O resultado é que o desenvolvimento de sistemas de votação electrónica requer um esforço significativo de gestão de riscos em toda a fase de desenvolvimento de software, com particular incidência na fase de teste dos sistemas.

Em seguida iremos proceder a uma análise de risco dos sistemas de votação electrónica focando em dois tipos de sistemas bem característicos:

- Sistema de votação electrónica utilizando máquinas de registo directo instaladas em recintos fechados e interligadas através de uma rede privada de dados;
- Sistema de votação electrónica utilizando a infraestrutura Internet para comunicação de dados.

A tabela seguinte apresenta uma análise de riscos do primeiro tipo de sistemas. São identificados o risco, a sua probabilidade e consequência. Como é habitual em análise de riscos, apresentam-se ainda algumas medidas de gestão de riscos.

Risco	Consequência	Probabilidade	Gestão
Sistema de votação electrónica utilizando máquinas de registo directo			
Falhas de componentes (hardware)	Podem causar perdas de votos localizadas	Muito provável - Este tipo de falhas é comum neste tipo de sistemas	Utilização de equipamento redundante. Utilização de procedimentos alternativos.
Falhas de componentes (software)	Podem causar perdas de votos localizadas, ou comprometer todo o sistema se uma única tecnologia for utilizada	Muito provável - Este tipo de falhas é comum neste tipo de sistemas	Utilização de equipamento redundante. Utilização de procedimentos alternativos. Utilização de tecnologias diversificadas.
Falhas de modo comum, proximidade ou fontes indirectas	Podem causar perdas de votos localizadas	Provável	Utilização de equipamento redundante. Utilização de procedimentos alternativos.
Falta de familiaridade dos utilizadores com o sistema (lapsos, deslizes, enganos)	Insatisfação e baixa participação no processo eleitoral	Muito provável	Fornecer simuladores de votação. Treinar pessoas para treinarem os utilizadores. Controlar a qualidade dos manuais de operação.
Violações de procedimentos de operação	Podem causar falhas de sistema localizadas	Muito provável - Este tipo de violações é muito comum	Fortes sanções legais sobre quem viola os procedimentos do sistema.
Negação de serviço, interceptação, mascaramento	Podem causar falhas de sistema localizadas	Muito pouco provável, considerando que o recinto é controlado	Controlo do recinto. Controlo da segurança da rede.
Código malicioso	Compromete todo o sistema	Provável - Este tipo de ataques é comum em ambientes organizacionais	Controlo estrito sobre os componentes do sistema e dos recursos humanos aplicados no seu desenvolvimento. Fortes sanções legais sobre quem viola o sistema.

Vírus e Cavalos de Tróia	Compromete todo o sistema	Improvável - Apesar de teoricamente possível	A detecção é muito difícil, especialmente quando são utilizadas técnicas de ofuscamento de código. A adopção de código livre e a certificação de código ajudam a gerir este risco.
Acessos não autorizados ao hardware ou software	Podem causar falhas de sistema ou perdas de votos localizadas	Improvável - Apesar de teoricamente possível	Selar todos os acessos ao hardware e software.

A tabela seguinte apresenta uma análise de riscos para os sistemas de votação electrónica utilizando a infraestrutura Internet.

Risco	Consequência	Probabilidade	Gestão
Sistema de votação electrónica utilizando a infraestrutura Internet			
Falhas de componentes (hardware)	Podem causar perdas de votos localizadas	Muito provável - Este tipo de falhas é comum	Permitir voto reversível.
Falhas de componentes (software)	Podem causar perdas de votos localizadas, ou comprometer todo o sistema se uma única tecnologia for utilizada	Muito provável - Este tipo de falhas é comum neste tipo de sistemas	Permitir voto reversível. Utilização de tecnologias diversificadas.
Falta de familiaridade dos utilizadores com o sistema (lapsos, deslizes, enganos)	Insatisfação e baixa participação no processo eleitoral	Muito provável	Fornecer simuladores de votação. Treinar pessoas para treinarem os utilizadores. Controlar a qualidade dos manuais de operação.
Negação de serviço, interceptação, mascaramento	Podem causar falhas de sistema localizadas	Provável, considerando que a Internet é pouco segura	Controlar este tipo de risco é relativamente difícil.
Código malicioso	Compromete todo o sistema	Provável - Este tipo de ataques é comum em ambientes organizacionais	Controlo estrito sobre os componentes do sistema e dos recursos humanos aplicados no seu desenvolvimento. Fortes sanções legais sobre quem viola o sistema.
Vírus e Cavalos de Tróia	Compromete todo o sistema	Provável, considerando que a Internet é pouco segura	A detecção é muito difícil, especialmente quando são utilizadas técnicas de ofuscamento de código. A adopção de código livre e a certificação de código ajudam a gerir este risco.
Acessos não autorizados ao software	Podem causar falhas de sistema ou perdas de votos localizadas	Provável, considerando que a Internet é pouco segura	Selar todos os acessos ao software.

A tabela seguinte apresenta uma análise de diversos riscos que se aplicam a ambos os sistemas.

Risco	Consequência	Probabilidade	Gestão
Ambos os sistemas			
Falta de acesso ao código fonte	Reduz o papel dos testes e auditorias ao sistema	Muito provável	Realizar testes de caixa negra.
Falta de padrões de certificação	Reduz o papel dos testes e auditorias ao sistema	Muito provável	Desenvolver padrões de certificação (processo muito lento).
Falta de controlo da configuração	Alterações no último minuto podem causar falhas de sistema localizadas	Muito provável - Os problemas de controlo da configuração são bem conhecidos	Utilizar assinaturas em todos os componentes de software. Fortes sanções legais sobre quem viola o procedimento.

PERSPECTIVA TÉCNICO-JURÍDICA

João Ferreira Dias e Domingos Magalhães

Neste capítulo iremos proceder a uma análise dos sistemas de votação electrónica do ponto de vista técnico-jurídico, focando em primeiro lugar no seu enquadramento no espaço europeu e em seguida no contexto nacional.

Organizações Internacionais

Conselho da Europa (COE)

Sobre a votação electrónica é incontornável a Recomendação (2004)II de 30/9 do Conselho de Ministros do Conselho da Europa (COE), designadamente os seus apêndices: I, sobre Padrões legais; II, sobre Padrões Operacionais; e III, sobre Requisitos Técnicos.

Nesta recomendação, que resultou de um longo processo de consenso que decorreu em 2003 e 2004, o COE reafirmou a necessidade de observância dos princípios do sufrágio universal, igual, livre e secreto por parte dos sistemas de votação electrónica.

Mais recentemente, em reunião de 23-24/11/2006, o COE decidiu: reafirmar a validade da Rec(2004)II (tendo agendado novo debate dentro de 2 anos); insistir na pertinência do conceito do “voto reversível” (ou voto sucessivo); sublinhar a indispensabilidade de reforçar a confiança dos eleitores nos sistemas de votação electrónica; afirmar o interesse em desenvolvimentos “open software” que, em alguns países, já tem um peso elevado; melhorar o sítio do COE nesta área, disponibilizando recursos e um repositório de “boas práticas”.

União Europeia

Em relação aos sistemas de votação electrónica, a posição da Comissão Europeia (Pergunta n.º 74 de Proinsias De Rossa (H-0208/4)), é a seguinte:

- Não há indicações que conduzam à conclusão de que a utilização dos sistemas de votação electrónica comprometa, só por si e de algum modo, o carácter universal, directo, secreto e livre das eleições.
- A votação electrónica pode ser compatível com esses princípios eleitorais básicos, desde que as normas operacionais e técnicas sejam de molde a garanti-los.

- O uso da tecnologia nos vários sistemas de votação, incluindo os sistemas de votação electrónica, faz parte de procedimentos eleitorais cuja regulamentação é da responsabilidade dos Estados-Membros.

No âmbito da iniciativa “e-Ten” decorre desde 2000 o projecto “e-poll” que envolve a França, a Itália e a Polónia para a realização de testes de voto electrónico presencial usando redes privadas virtuais sobre Internet. Foi desenvolvido um protótipo para utilização em assembleias de voto sob o conceito “votar em qualquer lado”. O fim do projecto ocorrerá em 2009 (eleição do Parlamento Europeu) com a realização de um grande piloto abrangendo 3,5 milhões de cidadãos nos três países acima referidos.

Quadro do sistema eleitoral em Portugal

Dos sistemas de votação tradicionais

Em Portugal, o poder político é exercido pelo povo através do sufrágio universal, igual, directo, secreto, periódico e livre, cf. o artº 10, n.º.1 (Sufrágio universal e partidos políticos) da Constituição da República Portuguesa (CRP).

Outros preceitos constitucionais relevantes são: o artº 12.º (Princípio da universalidade), o artº 13.º (Princípio da igualdade), o artº 49.º (Direito de sufrágio), o artº 113 (Princípios gerais de direito eleitoral) o artº 121.º (Eleição do Presidente da República), o artº 149.º (Assembleia da República - Círculos eleitorais), o artº 226.º (Leis eleitorais das Regiões Autónomas), e o artº 235 (Autarquias locais).

Pelas suas implicações para os futuros sistemas de votação electrónica merecem relevância os seguintes preceitos constitucionais:

- Artº 10, n.º.1: O povo exerce o poder político através do sufrágio universal, igual, directo, secreto e periódico, do referendo e das demais formas previstas na Constituição;
- Artº 49.º n.º.1: Têm direito de sufrágio todos os cidadãos maiores de dezoito anos, ressalvadas as incapacidades previstas na lei geral;
- Artº 49.º n.º.2: O exercício do direito de sufrágio é pessoal e constitui um dever cívico;
- Artº 113: O sufrágio directo, secreto e periódico constitui a regra geral de designação dos titulares dos órgãos electivos da soberania, das regiões autónomas e do poder local.

Os diversos tipos de sufrágio são regulados por diplomas específicos:

- Lei 14/79 de 16/5⁴⁵ - Lei eleitoral para a Assembleia da República;
- DL 319-A/76 de 3/5⁴⁶ - Lei eleitoral para a Presidência da República;
- Lei Orgânica n.º 1/2001 de 14/8⁴⁷ - Lei eleitoral dos órgãos das Autarquias Locais;
- Lei 14/87 de 29/4 - Lei eleitoral para o Parlamento Europeu.

O sistema de votação tradicional, em vigor em Portugal, respeita a observância destes princípios eleitorais básicos. A Lei 13/99 de 22/3 (Lei do Recenseamento Eleitoral) estabelece o regime jurídico do recenseamento eleitoral.

Entre nós, de acordo com a lei eleitoral, o direito de sufrágio é exercido através do voto pessoal e presencial e a recolha e o apuramento são manuais. Em regra, o procedimento é o seguinte: o eleitor, no dia da votação e dentro de um determinado horário, dirige-se à assembleia de voto que corresponde à respectiva inscrição para o recenseamento; identifica-se junto das pessoas que compõe a mesa de voto; recebe um boletim em papel; exerce o seu direito de voto numa câmara de voto e, finalmente, introduz o boletim em que exerceu o referido direito numa urna.

No caso da eleição para o Presidente da República, o art.º 121.º da CRP determina:

- O Presidente da República é eleito por sufrágio universal, directo e secreto dos cidadãos portugueses eleitores recenseados no território nacional, bem como dos cidadãos portugueses residentes no estrangeiro (nos termos do número seguinte);
- A lei regula o exercício do direito de voto dos cidadãos portugueses residentes no estrangeiro, devendo ter em conta a existência de laços de efectiva ligação à comunidade nacional;

⁴⁵ Com as alterações introduzidas pela Lei 8/81 de 15/6; Lei 28/82 de 15/11; Lei 14-A/85 de 10/7; DL 55/88 de 26/2; Lei 5/89 de 17/3; Lei 18/90 de 24/7; Lei 31/91 de 20/7; Lei 55/91 de 10/8; Lei 72/93 de 30/11; Lei 10/95 de 7/4; Lei 35/95 de 18/8; Lei Orgânica 1/99 de 22 Junho; Lei Orgânica 2/2001 de 25 Agosto.

⁴⁶ Com as alterações introduzidas pelo DL 377-A/76 de 19/5; DL 445-A/76 de 4/6; DL 456-A/76 de 8/6; DL 472-A/76 de 15/6; DL 472-B/76 de 15/6; DL 495-A/76 de 24/6; Lei 69/78 de 3/11; Lei 45/80 de 4/12; Resolução 83/81 de 23/4; Lei 8/81 de 15/6; Lei 28/82 de 15/11; Lei 143/85 de 26/11; DL 55/88 de 26/2; Lei 31/91 de 20/7; Lei 72/93 de 30/11; Lei 11/95 de 22/4; Lei 35/95 de 18/8; Lei 110/97 de 16/9; Lei 13/99 de 22/3; Lei Orgânica 3/2000 de 24/8; Lei Orgânica 2/2001 de 25/8; Lei Orgânica 4/2005 de 8/9; Lei Orgânica 5/2005 de 8/9.

⁴⁷ Com as alterações introduzidas pela Declaração de Rectificação 20-A/2001 de 12/10; Lei Orgânica 5-A/2001 de 26/11; Acórdão TC 243/2002 de 25/6; Lei Orgânica 3/2005 de 29/8.

- O direito de voto no território nacional é exercido presencialmente (o mesmo sucedendo no estrangeiro, após a alteração constante da Lei Orgânica nº 3/200, de 24-Agosto).

O conceito de voto antecipado reporta-se a determinados grupos de eleitores como os citados a seguir da Lei eleitoral do Presidente da República, DL 319-A/76 de 3/5, art. 70.º-A (voto antecipado):

I. Podem votar antecipadamente:

- Os militares que no dia da realização da eleição estejam impedidos de se deslocar à assembleia de voto por imperativo inadiável de exercício das suas funções;
 - Os agentes de forças e serviços, que exerçam funções de segurança interna nos termos da lei e que se encontrem em situação análoga à prevista na alínea anterior;
 - Os trabalhadores marítimos e aeronáuticos, bem como os ferroviários e os rodoviários de longo curso que, por força da sua actividade profissional, se encontrem presumivelmente embarcados ou deslocados no dia da realização da eleição;
 - Os eleitores que por motivo de doença se encontrem internados ou presumivelmente internados em estabelecimento hospitalar e impossibilitados de se deslocar à assembleia de voto;
 - Os eleitores que se encontrem presos e não privados de direitos políticos;
 - Os membros que representem oficialmente selecções nacionais, organizadas por federações desportivas dotadas de estatuto de utilidade pública desportiva, e se encontrem deslocados no estrangeiro, em competições desportivas, no dia da realização da eleição.
2. Podem ainda votar antecipadamente os seguintes eleitores recenseados no território nacional e deslocados no estrangeiro:
- Militares, agentes militarizados e civis integrados em operações de manutenção de paz, cooperação técnico-militar ou equiparadas;
 - Médicos, enfermeiros e outros cidadãos integrados em missões humanitárias, como tal reconhecidas pelo Ministério dos Negócios Estrangeiros;
 - Investigadores e bolseiros em instituições universitárias ou equiparadas, como tal reconhecidas pelo ministério competente;
 - Estudantes de escolas superiores, ao abrigo de programas de intercâmbio.
3. Podem ainda votar antecipadamente os cidadãos eleitores cônjuges ou equiparados, parentes ou afins que vivam com os eleitores mencionados no número anterior.

Na Eleição para a Assembleia da República, o respectivo processo eleitoral prevê o voto por correspondência para os eleitores inscritos no estrangeiro nos círculos da Europa e de fora da Europa.

O DL 95C/76 de 30/1⁴⁸ estabelece a organização do processo eleitoral no estrangeiro e regula o voto por correspondência.

Os meios técnicos que têm sido usados na implementação do sistema eleitoral, tradicional ou electrónico, são da competência interna do Estado português.

A utilização da informática também mereceu dignidade constitucional expressa na CRP artº 35 (utilização da informática), que se transcreve:

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei;
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente;
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis;
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei;
5. É proibida a atribuição de um número nacional único aos cidadãos;
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional;
7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.

Também merecem menções a regulamentação e a actividade da Comissão Nacional de Protecção de Dados⁴⁹.

⁴⁸ Com as alterações introduzidas pela Lei 10/95 de 7/4.

⁴⁹ www.cnpd.pt.

Quadro para o voto electrónico em Portugal

No que respeita a Portugal, a resolução do Conselho de Ministros n.º.135/2002 de 20 de Novembro criou, na dependência da Presidência do Conselho de Ministros, a Unidade de Missão Inovação e Conhecimento (UMIC), com a tarefa de propor uma estratégia detalhada de desenvolvimento da sociedade da informação e governo electrónico no nosso país para o período 2003/2006, os planos de acção para a sua operacionalidade, bem como a monitorização da respectiva execução.

Em Junho de 2003, o Conselho de Ministros aprovou um conjunto de documentos estratégicos para a sociedade de informação desenvolvidos sob coordenação directa da UMIC.

Entre esses documentos estratégicos, interessa-nos em particular, o Plano de Acção para a Sociedade de Informação, publicado em anexo à Resolução do Conselho de Ministros n.º. 107/2003.

Nesse documento, pode ler-se, a propósito do voto electrónico presencial, o que a seguir se transcreve:

“A simplificação e modernização do processo de votação surgem cada vez mais, como uma forma bastante eficaz de melhorar o conforto dos cidadãos e de atingir os segmentos mais abstencionistas. Especialmente quando esses segmentos são maioritariamente constituídos pela camada mais jovem da população e esta regista a mais elevada taxa de utilização de TIC [Tecnologias de Informação e Comunicação].

O objectivo estabelecido para o «Voto electrónico presencial» é testar este método de voto electrónico [...] nas próximas eleições europeias e generalizá-lo nas próximas eleições legislativas [...] O boletim de voto e a urna são substituídos por um terminal electrónico (com teclado, touch screen ou pointer) que permite ao eleitor indicar o seu sentido de voto. Adicionalmente, o eleitor pode aceder a informação adicional sobre os candidatos e os partidos e organizações políticas que o apoiam, permitindo uma votação mais informada e esclarecida por parte dos cidadãos.

Os votos não são transmitidos em tempo real para um repositório comum de dados, mas sim mantidos nas secções de voto até ao final do acto, sendo então transferidos e totalizados os resultados finais em poucos segundos [...]

Só numa fase mais adiantada de desenvolvimento, este sistema de votação irá oferecer conveniência e flexibilidade adicional aos cidadãos eleitores através das possibilidade da votação através de uma qualquer secção de voto (independentemente do local de residência) e da rapidez da contagem dos votos (apuramento em tempo real), bem como redução dos custos do processo eleitoral.”

Em conformidade com as referidas orientações, foram desenvolvidas diversas experiências de voto electrónico não vinculativo.

Entretanto, o Decreto-Lei n.º 16/2005 de 18 de Janeiro, veio criar a UMIC - Agência para a Sociedade de Conhecimento, I.P. (UMIC).

A UMIC, “tem como missão o planeamento, a coordenação e o desenvolvimento de projectos nas áreas da sociedade da informação e governo electrónico” (art. 4º). As suas atribuições são, designadamente, “aproveitar as potencialidades das TIC [...] para aumentar a participação dos cidadãos nos actos eleitorais” (art. 5º, alínea f)). Para o efeito, “sucede nas atribuições e competências, bem como nas universalidades dos direitos e obrigações legais e contratuais da Unidade de Missão Inovação e Conhecimento (art. 17º, nº1)”.

Não existem outras referências jurídicas que tenham que ver directamente com a votação electrónica, sendo de salientar a sua omissão no programa do actual governo, que parece na prática estar mais interessado na questão da mobilidade, “votar em qualquer lado”, do que na questão do voto à distância.

Sobre a legislação a produzir em Portugal

O conteúdo concreto da legislação a produzir no nosso país depende, em primeiro lugar, das soluções técnicas que se pretendam ver implementadas no terreno.

Admitindo que se trata de voto electrónico não presencial ou remoto, o respectivo articulado deverá colher os ensinamentos da doutrina e do direito constituído dos países da União Europeia e de outros que já legislaram sobre o assunto.

Nesse sentido, será vantajoso, numa perspectiva comparada, recorrer à análise dos ordenamentos legislativos eleitorais em vigor na Suíça e na Estónia. Por último, importa referir que em Espanha a Lei Orgânica do Regime Eleitoral Geral estará a ser adaptada aos sistemas de votação electrónica.

De resto, sem legislação da Assembleia da República sobre esta matéria, o voto electrónico nunca poderá passar da fase experimental, desde logo porque as normas legais das eleições políticas terão de ser alteradas de modo a que a votação electrónica se mostre conforme com algumas das regras de direito eleitoral, como entre outros são:

- A actual exigência do voto presencial (artº. 79 nº.3 da Lei 14/79 de 16/5, na actual redacção, e artº.70º nº.1 da Lei 319/76 de 3/5);
- A pessoalidade do voto (nº.2 do artº.70 da Lei 319/76 de 3/5);
- Os requisitos de exercício do voto (artº.83 da Lei 14/79 de 16/5 e artº.75 da Lei 319/76 de 3/5);

- O local de exercício de voto (artº.84 da Lei 14/79 de 16/5 e artº.76 da Lei 319/76 de 3/5);
- A presença de não eleitores no local da votação (artº.93 da Lei 14/79 de 16/5 e artº.84 da Lei 319/76 de 3/5);
- Os requisitos dos boletins de voto (artº.95 da Lei 14/79 de 16/5 e artº.86 da Lei 319/76 de 3/5).

Convirá ter ainda presente a envolvente resultante da introdução do cartão do cidadão e a intenção governamental de introduzir a inscrição automática dos cidadãos no caderno eleitoral (a exemplo de que sucede em Espanha e França há já vários anos) da freguesia de residência constante da base de dados da identificação civil do Ministério da Justiça.

A inclusão automática dos cidadãos no caderno eleitoral irá, previsivelmente, elevar os níveis de abstenção que se verificam no país, dado ser reconhecido que a faixa dos 18 aos 24 anos de idade é aquela onde se verificam as maiores taxas de não inscrição no recenseamento eleitoral.

Por outro lado, a introdução do voto em mobilidade (“votar em qualquer lado”) acarretará uma camada adicional de complexidade ao sistema.

ARQUITECTURAS

André Zúquete, Paulo Ferreira, Filipe Simões e Pedro Antunes

Neste capítulo apresentamos uma breve panorâmica, fundamentalmente centrada em aspectos arquitecturais, sobre os sistemas de votação electrónica mais importantes propostos pela comunidade científica.

Sistema proposto por Fujioka, et al.⁵⁰

É o sistema seminal na área da votação electrónica e que serviu de base a muitos outros que se seguiram. Apresenta um conjunto de componentes bastante abrangente, cobrindo a maioria das fases do processo eleitoral:

- *Preparation* - Nesta fase o votante preenche o boletim de voto. Este componente compõe uma mensagem onde o voto segue oculto, assina-a digitalmente e envia-a para o *Administrator*;
- *Administrator* - Por sua vez, o *Administrator* assina também a mensagem, que contém o voto oculto, e devolve-a ao votante;
- *Voting* - Através deste componente o votante recebe novamente o boletim de voto, mas agora devidamente assinado pelo *Administrator*, e envia-o para o *Counter*;
- *Counter* - O *Counter* lista publicamente os boletins de voto recebidos (sem no entanto divulgar o seu conteúdo);
- *Opening* - Através deste componente o votante envia, de forma anónima, a chave pública que permite decifrar o seu voto;
- *Counter* - Finalmente, este componente contabiliza e anuncia os resultados.

Sistema FOO⁵¹

⁵⁰ Fujioka, A., Okamoto, T., Ohta, K., (1993). A Practical Voting Scheme for Large scale Elections, NTT Network Information Systems Laboratories, Nippon Telegraph and Telephone Corporation, 1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03, Japan.

⁵¹ <http://www.cs.washington.edu/homes/mausam/evote/tsldoo8.htm> , acedido em Setembro de 2006.

É um sistema também proposto por Fujioka et al., e por isso mesmo reflecte uma funcionalidade muito semelhante à anterior, onde podemos apenas referir que alguns componentes assumem outra designação:

- *Validator* - Componente que verifica a autenticidade do boletim de voto;
- *Tallier* - Componente que contabiliza e anuncia os resultados.

Sistema EVOX⁵²

É um sistema igualmente baseado na arquitectura proposta por Fujioka et al., mas que apresenta novos componentes, abrangendo uma fase de pré-votação e também o processo de envio/recepção de mensagens utilizando canais anónimos:

- *Election Commission* - Numa fase anterior à votação propriamente dita, mas que faz parte do processo eleitoral, este componente realiza o pré-registo dos votantes e procede à criação dos boletins de voto;
- *Registrar* - Ainda numa fase anterior à votação propriamente dita, o *Registrar* tem a função de elaborar as listas de votantes e distribuir palavras passe de acesso ao sistema;
- *Voting* - Na fase de votação, o votante preenche o boletim, assina-o e envia-o para o *Admin*. Depois de receber o voto do *Admin* e verificar a sua assinatura, o boletim é enviado para o *Anon*;
- *Admin* - Verifica a autenticidade do voto e reenvia-o para o votante;
- *Anon* - Este componente destina-se a tornar anónimo o canal de entrega do voto;
- *Counter* - O *Counter* conta e apresenta os resultados da votação;
- *Confirmation* - Finalmente, através deste componente, cada votante pode confirmar que o seu voto foi entregue e contabilizado.

Sistema Sensus⁵³

⁵² Prakash, A., Mausam, (1999). Electronic Voting System, <http://theory.lcs.mit.edu/~cis/voting/protocol/index.html> , acedido em Setembro de 2006.

⁵³ Cranor, Lorrie F., Cytron, Ron K., (SD). Sensus: A Security-Conscious Electronic Polling System for the Internet, Public Policy Research, AT&T Labs Research, Department of Computer Science, Washington University in St. Louis.

O sistema Sensus foi sugerido por Lorrie Cranor e Ron Cytron na sequência do trabalho realizado por Fujioka et al. Inicialmente pensado para reproduzir a votação por correio tradicional, veio a revelar-se suficientemente flexível para permitir outros tipos de votação menos tradicionais⁵⁴. O Sensus é um sistema que apresenta três componentes essenciais:

- *Registrar* - Responsável pelo registo dos votantes para cada eleição;
- *Validator* - Tem como função verificar o registo do votante e assegurar que um votante vota apenas uma vez;
- *Pollster*, - Actua como um agente de votação, que apresenta os boletins de voto a cada votante e coleciona esses votos, sendo ainda responsável pelas operações de cifra e entrega do voto;
- *Tallier* - que coleciona e contabiliza os votos, sendo também responsável pela apresentação de resultados.

Sistema REVS⁵⁵

O sistema REVS assume a prévia existência de uma lista de eleitores já registados e preocupa-se apenas com o processo eleitoral a partir deste ponto. É um dos dois sistemas aqui apresentados que introduz um componente independente responsável pela anonimização do voto. É ainda um sistema que aposta numa arquitectura baseada na replicação de componentes, tendo em vista aumentar a tolerância a falhas.

O REVS utiliza uma arquitectura com cinco componentes:

- *Ballot Distributor* - Assegura a distribuição dos boletins pelos votantes e é responsável pela configuração das chaves e assinaturas envolvidas no processo;
- *Administrator* - Assegura que só os boletins assinados são válidos;
- *Anonymizer* - Torna o voto anónimo, ocultando o endereço da máquina (IP) onde o votante exerceu o seu direito e ocultando ainda a hora em que ocorreu a votação;
- *Voter Engine* - Executa a votação propriamente dita;

⁵⁴ Cranor, Lorrie F., (1995). Can declared strategy voting be an effective instrument for group decision-making?, Tech. Rep. WUCS-95-04, Washington University Department of Computer Science, St. Louis.

⁵⁵ Joaquim, R., Zúquete, A., Ferreira, P., (2003). REVS, A Robust Electronic Voting System, Proceedings of IADIS International Conference e-Society.

- *Counter* - Verifica a validade dos votos (através das assinaturas), elimina a repetição de votos e calcula os resultados.

Sistema proposto por Kofler, et al.⁵⁶

É um sistema que separa a fase de registo do votante da fase de votação propriamente dita (a fase em que se deposita o voto):

- *Registration* - A fase de registo permite o registo de votantes durante um período anterior ao dia da eleição;
- *Trust Center* - Verifica as credenciais dos votantes e autoriza a votação;
- *Ballot Box* - A fase de votação é composta pelo componente *Ballot Box*, que também acumula os votos.

Oasis Election⁵⁷

O sistema Oasis propõe um conjunto de componentes que abrangem a fase de pré-votação e pós-votação:

- *Candidates* - Responsável pela designação dos candidatos e constituição das listas;
- *Voters* - Coordena o registo de votantes, a interligação entre as bases de dados e as comunicações aos votantes;
- *Voting* - Gere os pedidos de autenticação dos votantes e respectivas respostas, selecção dos candidatos, o depósito dos votos e a respectiva confirmação pelos eleitores;
- *Results* - Procede à contagem dos votos;
- *Audit* - Componente que pretende exercer algum tipo de verificação sobre o número de boletins entregues, inutilizados e não usados.

⁵⁶ Kofler, R., Krimmer, R., Prosser, A., (2002). *Electronic Voting: Algorithmic and Implementation Issues*, Department Production Management, Vienna University for Business Administration and Economics.

⁵⁷ Borrás, J., (2002). *Overview of the work on e-voting technical standards*, Office of e-Envoy, Cabinet Office, UK Government.

Cybervote⁵⁸

Trata-se de um sistema sugerido num relatório sobre requisitos para um protótipo de votação electrónica apresentado à Comissão Europeia por um conjunto de quatro organizações (EADS Systems & Defence Electronics, NOKIA Research Centre, K. U. Leuven Research & Development e British Telecommunications).

Este sistema apresenta os seguintes componentes:

- *Client Repository* - Que contém toda a informação sobre os dispositivos que permitem aos votantes exercerem esse direito;
- *Registration Server* - Tem como função registar os votantes;
- *Vote Server* - É o responsável pela recepção dos votos, após confirmação de autorização de votação de cada votante;
- *Tabulation* - Proceda à contagem, verificação e apresentação dos resultados;
- *Audit and Validation* - Componente responsável pela verificação do processo de votação e pela gestão dos registos do sistema.

Quadro resumo

	Fujioka, et al.	EVOX	Sensus	REVS	Kofler, et al.	Oasis	Cyber-vote
Pré-registo		election commission				candidates	client repository
Registo		registrar	registrar		registration	voters	registration server
Validação	administration	admin	validator	administrator	trust center	voting	vote server
Anonimização		anon		anonymizer			
Votação	preparation voting	voter	pollster	voter engine	ballot box	voting	vote server

⁵⁸ Cybervote, (2002). Report on mock-ups of architectures and overall system architecture, CYBERVOTE:WP2:D7/V2:2001 VI.O.

Contagem	counting	counter	tallier	counter		results	tabulation
Verificação	collecting opening	confirmation				audit	audit and validation

Como se pode observar no quadro acima, os sistemas EVOX, OASIS e Cybervote possuem um componente que opera numa fase ainda anterior ao processo de votação (anterior mesmo à fase de registo do votante), chamada de pré-registo. Nessa fase, no sistema EVOX são elaborados os boletins de voto, no sistema OASIS faz-se a gestão de candidatos, e no Cybervote é gerida a informação acerca dos dispositivos que irão permitir aos votantes exercer o seu voto.

Relativamente à fase de registo dos votantes, apenas os sistemas propostos por Fujioka et al. e REVS partem do princípio de que a lista de eleitores já existe. Em todos os restantes se prevê o registo de votantes.

A validação do votante é tida em conta por todos os sistemas aqui apresentados, no entanto Fujioka et al., Zúquete et al. e Kofler et al. sugerem que tal validação deve ser efectuada à parte da componente de votação, enquanto que os outros sistemas aglomeram as duas fases no mesmo processo.

Ao separar estas operações fundamentais para o processo eleitoral, os sistemas conseguem maior independência e previsivelmente maior segurança. Ou seja, caso ocorra algum problema numa destas operações, será mais fácil isolar e mitigar o seu impacto.

O sistema REVS trata da anonimização do voto num componente independente e completa essa importante função com a capacidade muito específica de encobrir a origem e data dos votos. De notar que o sistema EVOX também se refere à anonimização de canais através de um componente específico mas com um papel mais restrito e dependente. Ainda que os outros sistemas se refiram também à anonimização, esta fase é incluída no processo de tratamento do voto durante a fase de votação.

A fase de votação é uma fase que parece consensual em todos os sistemas, enquanto que só o sistema sugerido por Kofler et al. não se refere à fase de contagem do voto.

A fase de verificação apresentada por estes sistemas pode ser considerada como uma primeira abordagem à auditoria do processo eleitoral num sistema de votação electrónica. No entanto, os componentes apresentados pelos sistemas em análise limitam-se a verificações após o processo ter decorrido, salvaguardando o caso da Cybervote, conforme se descreve mais à frente.

Mas, regra geral, apenas após ter ocorrido a votação, estes sistemas demonstram alguma preocupação com a questão da verificação do número de boletins usados e não usados ou inutilizados, ou com o facto de um votante ter votado e o seu voto poder não ter sido contado.

As propriedades dos sistemas de votação electrónica que são alvo de alguma verificação responsabilizam muitas vezes apenas os próprios votantes, mesmo que de forma muito limitada, por causa da garantia de algumas propriedades, em particular a da não coercibilidade.

Sistemas como o de Fujioka et al. e EVOX, referem-se à fase de verificação como sendo da responsabilidade dos próprios, através da confirmação/validação final de que os votos foram depositados.

O sistema OASIS pretende dar mais algumas garantias ao processo, desde que os membros oficiais da eleição sejam capazes de verificar que o número de boletins depositados nas urnas, mais o número de boletins inutilizados, mais os boletins não usados seja igual ao número de boletins disponibilizados; fornecendo também um mecanismo de recontagem dos votos, no caso dos resultados serem contestados; e ainda permitindo a observadores alguma vigilância sobre todo o processo.

É no entanto de realçar que o sistema sugerido pela Cybervote já refere uma verificação mais abrangente, em três segmentos: a segurança, os registos e questionários.

ARQUITECTURA DE REFERÊNCIA

Filipe Simões e Pedro Antunes

Procedemos anteriormente a uma descrição breve de diversos sistemas de votação electrónica, focando em particular nas arquitecturas propostas. Dessa descrição pode-se inferir uma arquitectura genérica, independente dos sistemas concretos, e que sirva de referencial para a comparação de funcionalidades, discussão sobre segurança e auditoria ou mesmo sugestão de inovações.

Iremos neste capítulo propor uma arquitectura de referência para sistemas de votação electrónica.

Partimos ainda do pressuposto de que a gestão do risco de um sistema de votação electrónica será tanto mais eficaz quanto maior for a granularidade da sua arquitectura. Podemos utilizar como medida da granularidade a contagem simples de componentes definidos pela arquitectura.

Assim, a arquitectura de referência que propomos tenta identificar o maior número de componentes de entre o conjunto de sistemas de votação electrónica anteriormente apresentados. A análise do quadro resumo dos sistemas de votação electrónica existentes (ver capítulo anterior) permite imediatamente inferir que a arquitectura de referência será fundamentalmente baseada no sistema EVOX, já que é este o sistema que apresenta maior quantidade de componentes.

Por outro lado, deve ainda ser observado que o sistema EVOX cobre as diversas fases do processo eleitoral que vão desde o pré-registo até à fase de contagem, incluindo ainda a fase de verificação do voto pelos eleitores.

A arquitectura de referência é a que se apresenta na tabela seguinte, na qual se apresentam ainda as diversas fases do processo eleitoral que foram consideradas.

Fases do processo	Componentes
Pré-registo	Geração de listas de votantes
	Preparação de boletins de voto
Registo	Servidor de registo de eleitores
	Servidor de credenciais
Validação	Servidor de validação de eleitores (credenciais e direito de voto)
Votação	Disponibilização de boletins
	Contagem parcial
	Cifra de boletins
Anonimização	Anonimização
Contagem / apresentação de resultados	Contagem final
	Divulgação de resultados

Na fase de pré-registo, os potenciais eleitores podem fazer uma “pré-inscrição” para a votação, através do componente de *geração de listas de votantes*. O componente de *preparação de boletins* compõe os boletins de voto de acordo com as especificações do acto eleitoral.

Na fase de registo, o componente *servidor de registo de eleitores* terá como função identificar o potencial eleitor e autorizar o seu registo no sistema. Após autorizar o registo do eleitor, o componente *servidor de credenciais* entrega as respectivas credenciais ao eleitor para que este possa mais tarde vir a exercer o seu direito de voto, caso seja essa a sua intenção.

Na fase de validação, é o componente *servidor de validação de eleitores* que verifica as credenciais do eleitor e ainda o direito de voto, para não permitir uma segunda votação por parte do mesmo indivíduo⁵⁹.

A fase de votação é iniciada com a apresentação do boletim de voto ao eleitor pelo componente de *disponibilização de boletins*. Note-se que a confirmação das opções de voto do eleitor pode ser realizada por este componente.

O componente de *contagem parcial* destina-se a recolher o boletim de voto e dar ao eleitor a informação de que o seu voto foi contabilizado até esta fase. Este componente pode ainda oferecer mecanismos de confirmação do voto pelo eleitor.

O componente de *cifra de boletins* cifra os boletins de voto antes de estes serem entregues para anonimização. O componente de *anonimização* procede à anonimização dos boletins de voto de forma a garantir que estes não possam ser relacionados com os votantes.

Na fase de contagem e divulgação de resultados, o componente de *contagem final* procede à contagem dos votos. Finalmente, o componente de *divulgação de resultados* apresenta as contagens finais às entidades oficiais e ao público em geral.

⁵⁹ O conceito de voto reversível implica algumas alterações nesta funcionalidade, dado que requer uma interação com o componente de contagem para permitir que vários votos possam ser submetidos mas apenas um seja contabilizado.

PERSPECTIVA SOBRE O VOTO PELA INTERNET

Pedro Antunes

A primeira autorização legal para votar pela rede de comunicação de dados Internet terá sido dada nos EUA, quando o estado do Texas permitiu que o astronauta David Wolf votasse por correio electrónico, utilizando um computador portátil, para as eleições do Texas de 1997, quando este se encontrava ao serviço da estação espacial Russa Mir⁶⁰.

Com a disseminação da Internet surgiu o interesse em alargar o processo de votação, de maneira a que os utilizadores possam enviar o seu voto a partir de um qualquer computador com acesso à Internet.

A conveniência é considerada o aspecto mais favorável ao uso da Internet⁶¹. Numa sociedade de maior comodismo, o facto de se obrigar à presença física dos eleitores nos locais de voto num horário fixo leva à falta de participação. Como mostram os dados da abstenção da Califórnia, os níveis de abstenção são crescentes e atingem valores preocupantes. Em 1996, 100 milhões de cidadãos dos EUA elegíveis para votar preferiram não o fazer.

A votação pela Internet vem maximizar a conveniência e acesso dos eleitores, permitindo o acto eleitoral virtualmente em qualquer local que tenha acesso à Internet, sendo extremamente atractivo poder exercer esse direito em casa, emprego ou biblioteca. Nas experiências realizadas em diversos países, também é sobre este modelo que estão a incidir as pressões políticas e sociais.

Por outro lado, um sistema de votação pela Internet implicaria um menor esforço financeiro, logístico e humano no processo eleitoral. Finalmente, diversas experiências realizadas nos EUA e Reino Unido indicam alguma aceitação desta tecnologia, em particular dos jovens eleitores. Este são, no essencial, os aspectos positivos a considerar nos sistemas de votação pela Internet.

O uso da Internet como plataforma de suporte a um sistema de votação electrónica representa um risco substancial à integridade do sistema, uma vez que se torna prati-

⁶⁰ Baer, W. (2001). Signing Initiative Petitions Online: Possibilities, Problems and Prospects. Public Policy Institute of California.

⁶¹ Dictson, D., Ray, D. (2000). The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections. White Paper. SecurePoll.com.

camente impossível ter um controlo oficial da plataforma e do ambiente físico. Segundo a definição de Ford e Baum⁶² podemos definir a Internet como sendo:

“...uma entidade extraterritorial, não controlada nem controlável por qualquer governo ou organização, mas em vez disso, que opera exclusivamente numa base de mútua cooperação. A Internet pode melhor ser descrita como caos controlado.”

O conceito perfeitamente adequado de entidade extraterritorial levanta grandes preocupações, na medida em que as eleições se referem a uma território bem definido e com uma soberania própria, o que pressupõe o controlo de todas as variáveis envolvidas no processo eleitoral. Assim, esta limitação pode permitir interferências nos resultados das votações, e a tecnologia actual não se apresenta em condições de resolver completamente este problema.

Uma solução que tem sido experimentada⁶³ consiste em utilizar uma estrutura do tipo cliente-servidor onde o software cliente (por exemplo, uma *Applet Java*) é carregado na máquina cliente a partir do servidor e depois estabelece uma comunicação segura com o servidor. No entanto, esta solução está sujeita a problemas bem conhecidos, como por exemplo, quebras na ligação, demoras no carregamento do software cliente ou insuficiência de recursos do lado cliente.

O que acontece se os eleitores não tiverem acesso ao sistema de votação, por o serviço não estar disponível? Voltariam a tentar? Uma vez? Duas? Se não tivessem sucesso, deslocar-se-iam para o seu local de voto?

Um sistema bem desenhado deveria ser capaz de suportar a carga de tráfego gerada pelas eleições sem problemas. No entanto, mesmo grandes empresas dedicadas ao comércio electrónico como a eBay, sofrem interrupções quando o tráfego ultrapassa a capacidade dos seus servidores, levando à interrupção dos seus serviços, que por vezes dura dias. Os fornecedores de serviços eleitorais podem sofrer das mesmas vulnerabilidades.

Em algumas situações estes estrangulamentos da rede, em termos de tráfego e sobrecarga dos servidores, são devidos a ataques do tipo Negação de Serviço⁶⁴ (DoS - *Denial of Service*) e Negação de Serviço Distribuída (*Distributed DoS*)⁶⁵.

Estes dois tipos de ataque são semelhantes, à excepção de que no primeiro os atacantes assumem o controlo de uma determinada máquina (normalmente através de Cavalos de Tróia), que irá depois atacar o serviço, enquanto no segundo caso os atacantes apoderam-se de um conjunto de máquinas para realizar um ataque sincronizado ao serviço.

⁶² Ford, W., Baum, M. (1997). *Secure Electronic Commerce*. Prentice-Hall.

⁶³ Gerck, E. (2001). *Internet Voting System Requirements*. The Bell, 1(7). November.

⁶⁴ Ver capítulo dedicado aos riscos de sabotagem.

⁶⁵ Veríssimo, P., Rodrigues L. (2001). *Distributed Systems for System Architects*. Kluwer Academic Publishers.

Devido ao facto de ser praticamente ilimitado o número de máquinas possíveis de controlar pelos atacantes neste tipo de ataque, a Negação de Serviço torna-se uma ameaça bastante perigosa. Por exemplo, ainda não existem formas de evitar (tendo em conta as constantes descobertas de vulnerabilidades nos sistemas operativos mais comuns) ou interromper um ataque deste tipo em curso sem interromper a ligação e parar os serviços.

Como, utilizando a Internet, pode ser possível garantir que apenas os eleitores autorizados votam?

Existem já alguns mecanismos que podem servir de base para garantir a elegibilidade e autenticidade:

- Palavra-chave (ou PIN - *Personal Identification Number*), para garantir a autenticação do eleitor;
- Assinatura digital, que garante a origem do voto;
- Cartão inteligente (*Smart Card*) e respectivo leitor;
- Identificação bio-métrica.

O nível mais básico de segurança utilizado hoje na Internet é a palavra-chave. No entanto, ocorrem inevitavelmente situações em que os eleitores esquecem as palavras-chave, ficando impedidos de votar, ou as palavras-chave são roubadas, podendo originar votos não desejados.

A tecnologia de assinatura digital está a começar a ser aceite como principal dispositivo de segurança para os sistemas de votação pela Internet⁶⁶. Alguns Estados federados dos EUA já autorizaram as assinaturas digitais e, inclusive, existem alguns que já as regulamentaram. Contudo, o seu uso parece ser mais orientado para o comércio electrónico. A California Internet Task Force⁶⁷ recomenda que as assinaturas digitais em eleições apenas sejam introduzidas quando os eleitores estiverem já habituados ao seu uso corrente nas relações com a administração pública.

Uma vantagem do uso de assinaturas digitais é a existência de uma terceira entidade responsável pela emissão de assinaturas. Esta entidade independente pode garantir simultaneamente a identidade e o anonimato do eleitor.

Outro mecanismo de segurança que está a ser testado na votação pela Internet é o cartão inteligente. Um cartão inteligente emitido para cada eleitor pode ser usado em qualquer computador que tenha um leitor. Os cartões podem ser pré-programados com os boletins de voto e enviados por correio para os eleitores. O leitor de cartões iria funcionar como o

⁶⁶ Dictson, D., Ray, D. (2000). The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections. White Paper. SecurePoll.com.

⁶⁷ California Internet Task Force (2000). Final Report. California Secretary of State.

dispositivo de votação e a Internet seria apenas utilizada para transmitir o voto. Contudo, um sistema deste tipo ainda continua vulnerável a ataques na Internet, assim como à já antiga ameaça de roubo de correspondência.

A última geração de mecanismos de segurança na Internet utiliza identificadores bio-métricos, reconhecimento de voz, impressão digital ou leitura da retina.

Os identificadores bio-métricos são menos vulneráveis que os outros dispositivos de segurança, mas não são infalíveis.

Existe ainda uma preocupação adicional sobre os identificadores bio-métricos: a privacidade. Muitos cidadãos e países resistem por exemplo à recolha sistemática de impressões digitais. Sem qualquer tipo de controlo das companhias que oferecem sistemas bio-métricos, a votação pela Internet que usa este tipo de tecnologia pode oferecer oportunidades de abuso.

Esta é, com certeza, a questão mais delicada relativamente ao voto pela Internet. Como garantir que os votos não podem ser modificados, forjados ou eliminados num ambiente que é vulnerável em pelo menos três pontos: o servidor, o cliente e a rede de comunicação de dados?⁶⁸

Relativamente à rede, uma forma de atacar a integridade dos votos é a Intercepção⁶⁹, uma técnica que permite capturar o tráfego de pacotes na rede, alterá-los e de seguida voltar a colocá-los na rede, na maioria das vezes sem que esta operação seja detectada. No âmbito de um sistema de votação pela Internet, isto significa que o eleitor após ter efectuado o seu voto pode não ter garantias de que ele não seja alterado. De salientar que actualmente este tipo de ataques são controláveis, nomeadamente recorrendo a técnicas de criptografia.

Refira-se, a propósito da cifra de dados, o debate sobre até que ponto as instituições governamentais podem ter acesso às chaves que permitem reverter uma cifra. Essa possibilidade legal coloca em risco o anonimato do voto.

Relativamente ao cliente, deve ser considerada a possibilidade de um ataque do tipo Cavalo de Tróia, em que um software malicioso se instala no sistema operativo do cliente, podendo espiar, modificar ou eliminar o voto do eleitor. Este tipo de ataque é extremamente insidioso, pois não é resolvido pelos mecanismos criptográficos e de auten-

⁶⁸ Aviel Rubin (2002). Security Considerations for Electronic Voting. Communications of ACM 45(12).

⁶⁹ Ver secção dedicada aos riscos de sabotagem.

tação do eleitor⁷⁰. A California Internet Task Force recomenda diversas medidas para detectar ou evitar este tipo de ataques:

- Re-instalar o sistema operativo e aplicações de votação antes de votar;
- Utilizar equipamento seguro adicional, ligado ao computador pessoal destinado a executar a aplicação de votação;
- Utilizar um sistema operativo seguro;
- Utilizar informação adicional, obtida por meios não informáticos, necessária ao processo de votação;
- Permitir ao eleitor enviar votos de teste, indiferenciáveis do voto real, para o sistema de contagem centralizada. Esta é uma técnica curiosa de segurança por ofuscação.

Qualquer uma destas técnicas apresenta significativos impactos no custo, complexidade e conveniência na utilização do sistema de votação electrónica.

No que se refere ao servidor, deve ser considerada a possibilidade de, pela via do mascaramento, sítios fantasmas desviarem os eleitores, que não se apercebem de que o seu voto não está a ser enviado para as autoridades legítimas⁷¹. Uma vez o voto capturado, ele pode ser falsificado e usado na eleição real a favor de um dos candidatos, de forma não facilmente detectável.

Note-se que os tipos de ataque aqui referidos podem ganhar extrema importância se os sistemas forem uniformizados, pois uma grande variedade de equipamentos e protocolos proporciona maior segurança numa eleição geral.

Um grande sistema de votação, por exemplo a nível nacional, é também um enorme e apetecível alvo para potenciais ataques.

Finalmente, deve ser referido que uma das formas de reduzir o risco de ataques é fechar o código fonte utilizado pelo sistema de votação. No entanto, esta aproximação colide com os requisitos de Certificabilidade e Auditabilidade.

Uma técnica que tem sido utilizada para fornecer Auditabilidade nos sistemas de votação pela Internet consiste em associar o nome do eleitor ao seu voto, devidamente cifrado. Esta técnica não garante o Anonimato do voto, pois não é possível garantir que a chave

⁷⁰ Internet Policy Institute (2001). Report of the National Workshop on Internet Voting: Issues and Research Agenda. Internet Policy Institute.

⁷¹ Rubin, A. (2001). Security Considerations for Electronic Voting Over the Internet. 29th Research Conference on Communication, Information and Internet Policy (TPRC2001). October.

não será quebrada. Esta técnica também levanta algumas questões legais: como garantir o anonimato mesmo perante uma ordem legal para quebrar a chave?

Uma forma de garantir o Anonimato em sistemas de votação pela Internet consiste em recorrer a uma entidade independente que se interponha entre o eleitor e o sistema de contagem centralizado. Este mecanismo está no entanto sujeito aos problemas de Integridade do Sistema e Integridade dos Votos já referidos, sendo ainda de considerar um risco acrescido de falta de disponibilidade do sistema.

O voto pela Internet parece ainda levantar um problema incontornável: como garantir a Privacidade e Não Coercibilidade de um eleitor fora de um recinto controlado?

Refira-se, no entanto, que o mesmo problema ocorre com a votação por carta que é no entanto aceite em diversos países, incluindo Portugal (apenas para residentes no estrangeiro). Este problema tem sido aceite porque o número de votantes é geralmente reduzido, não influenciando os resultados eleitorais. Esse entendimento poderá no entanto mudar se o voto remoto for adoptado em grande escala.

Um outro problema levantado na votação pela Internet tem a ver com a diversidade de ambientes computacionais (sistemas operativos, ecrãs de computador, resoluções gráficas) inerente à arquitectura da Internet. Neste cenário, é possível que um boletim de voto apareça aos utilizadores de formas diferentes, o que pode quebrar a equidade dos diferentes candidatos.

Finalmente, um problema interessante que tem também sido levantado relativamente ao voto pela Internet questiona a legitimidade e as motivações de um votante que realiza esse acto em qualquer local e ocasião, eventualmente de forma pouco ponderada ou mesmo irreflectida, enquanto por exemplo joga no seu computador.

REVS – UM PROTOCOLO ROBUSTO DE VOTAÇÃO ELECTRÓNICA PELA INTERNET

André Zúquete, Paulo Ferreira e Rui Joaquim

Existem muitos protocolos para efectuar votações electrónicas, mas só um número reduzido deles foi realmente posto em prática. Uma razão para esta disparidade é o facto de os protocolos considerarem apenas requisitos do processo de votação e não problemas colocados pelo universo real de utilização desses protocolos, tal como tolerância a falhas. Os sistemas de votação pela Internet, em particular, levantam ainda inúmeros problemas operacionais que entravam actualmente o seu uso generalizado^{72 73}. Do ponto de vista técnico estes problemas são de três tipos:

- A arquitectura funcional da Internet não possui mecanismos de segurança e tolerância a falhas necessários à correcta execução da maioria dos protocolos de votação;
- Muitos protocolos de votação usam pressupostos acerca do ambiente de execução que são difíceis de assegurar em cenários reais, tais como: (1) os computadores usadas pelos clientes são confiáveis, no sentido em que o seu sistema opera como um intermediário de confiança; (2) os servidores que controlam a eleição não podem falhar, ficar incomunicáveis ou perverter o protocolo; e (3) o protocolo não é perturbado por falhas de comunicações ou de máquinas;
- Os protocolos podem ser atacados directa ou indirectamente, no primeiro caso com o intuito de controlar a contagem final, no segundo com o intuito de impedir a sua realização. Pode ainda existir coacção dos votantes se o local de voto não for controlado por agentes oficiais.

O REVS⁷⁴ é um protocolo de votação pela Internet que foi concebido para resolver alguns destes problemas. Em particular, é suportado por diversos servidores replicados, o que permite tolerar algumas falhas de comunicação e de máquinas, e mantém um estado distribuído que permite recuperar de interrupções no protocolo de votação. Cada votante mantém um estado local, num suporte de armazenamento não-volátil móvel, que lhe permite parar e retomar o processo de votação noutra altura e noutro local. Cada ser-

⁷² The Caltech/MIT Voting Technology Project (2001). Voting: What is What Could Be. Caltech/MIT.

⁷³ California Internet Voting Task Force (2000). A report on the feasibility of internet voting.

⁷⁴ R. Joaquim, A. Zúquete, and P. Ferreira (2003). REVS A Robust Electronic Voting System. In IADIS International Conference e-Society.

vidor, por si só, não consegue personificar nenhum votante autorizado nem consegue interagir de forma incorrecta com os votantes sem que tal seja detectado. O conluio entre servidores para realizar actividades de sabotagem (por exemplo, votar em nome de quem não votou) é contrariado até um certo grau que é parametrizável pelas entidades reguladoras da eleição.

Tecnicamente o REVS é um sistema de votação electrónica que utiliza assinaturas às cegas e que deriva do sistema proposto por DuRette⁷⁵, o qual por sua vez deriva do EVOX, já discutido no capítulo relativo às arquitecturas. Ambos os sistemas anteriores são muito sensíveis a falhas na comunicação ou nos servidores, o que se procurou resolver com o REVS. Para além disso, o REVS possui um mecanismo de autenticação de votantes mais robusto que impede a sua personificação pelos servidores do sistema mas que não será aqui descrito.

O primeiro protótipo do REVS foi ensaiado em Maio de 2003 para a recolha de avaliações pedagógicas no Instituto Superior Técnico (IST). Para esse fim foi preparada uma sala de voto com vários computadores cliente devidamente preparados; foi também fornecido software para que os votantes pudessem participar a partir de qualquer outro computador. A votação foi controlada por 5 servidores fornecidos e geridos por entidades com interesses disjuntos: dois serviços informáticos (CIIST e RNL), dois departamentos (Engenharia Civil e Matemática) e ainda a Associação de Estudantes (AEIST). Como boletins de voto usou-se texto em formato XML, assinado para garantir a sua correcção. Este é carregado dinamicamente pelos computadores cliente reproduzindo o aspecto dos originais em papel. Os computadores clientes foram capazes de verificar o correcto preenchimento dos boletins através de informação contida nos mesmos, o que evitou votos nulos.

Análise dos protocolos existentes

Os protocolos de votação electrónica baseiam-se, grosso modo, em três tecnologias distintas: assinaturas às cegas^{76 77}, mix-nets⁷⁸ e cifras homomórficas⁷⁹. Cada uma destas tec-

⁷⁵ B. DuRette (1999). Multiple Administrators for Electronic Voting. Bs.C. thesis.

⁷⁶ L. Cranor and R. Cytron (1997). Sensus: A security-conscious electronic polling system for the Internet. In Proceedings of the Hawaii International Conference on System Sciences, Wailea, Hawaii, USA.

nologias tem prós e contras, mas as assinaturas às cegas permitem sistemas mais flexíveis, suportando qualquer tipo de boletim de voto, e mais eficientes que as demais, o que ditou a sua selecção para o REVS.

De forma simplificada, uma assinatura às cegas é igual a uma assinatura digital mas o assinante não consegue associar a sua assinatura com o que assinou. Desta maneira é possível garantir a inalterabilidade de dados - os dados assinados, neste caso os votos - sem que o assinante tenha que os conhecer. A geração de assinaturas digitais segue o seguinte processo: (1) os dados a assinar são ocultados (alterados com um valor secreto, dito factor de ocultação) e enviados para o assinante; (2) o assinante produz e devolve a assinatura desses dados, dita assinatura às cegas; e (3) a assinatura é alterada pelo requerente removendo o factor de ocultação. No final deste processo os dados estão assinados digitalmente de forma normal mas o assinante não só não os conhece como não consegue relacionar a assinatura às cegas que produziu com a que dela deriva após a remoção do factor de ocultação.

O protocolo de referência baseado em assinaturas às cegas, conhecido como FOO, inspirou dois sistemas reais de votação electrónica - Sensus e EVOX. Todos estes sistemas foram já anteriormente discutidos (ver capítulo dedicado às arquitecturas).

O EVOX foi posteriormente melhorado de forma a eliminar um serviço plenipotenciário capaz de interferir fraudulentamente com o protocolo, dando origem ao EVOX *Managed Administrator*⁸⁰ (EVOX-MA daqui em diante). O melhoramento introduzido pelo EVOX-MA consistiu em separar a verificação da Integridade do Voto por N servidores, dos quais $t \leq N$ têm de funcionar correctamente para produzir um voto válido. A verificação do Direito de Voto continuou a ser gerida por um único servidor.

Eis um resumo do funcionamento do EVOX-MA: (1) o votante obtém um boletim de voto do *Manager*, preenche-o e (2) contacta $t \leq N$ *Administrators* para que estes assinem cegamente o boletim preenchido, (3) envia as t assinaturas para serem assinadas cegamente pelo *Manager*, que o faz se e só se o votante estiver autorizado a participar na eleição. No fim deste processo o votante envia para um *Counter* o seu boletim juntamente com todas as assinaturas obtidas, fazendo esse envio através de um *Anonymizer* que garante o anonimato do votante perante o *Counter*.

⁷⁷ A. Fujioka, T. Okamoto, and K. Ohta (1992). A Practical Secret Voting Scheme for Large Scale Elections. In Advances in Cryptology AUSCRYPT 92 Proceedings (LNCS 718), Queensland, Australia.

⁷⁸ D. Chaum (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Comm. of the ACM*, 24(2).

⁷⁹ O. Baudron, P. A. Fouque, D. Pointcheval, G. Poupard, and J. Stern (2001). Practical Multi-Candidate Election System. In Proceedings of the 20th ACM Symposium on Principles of Distributed Computing.

⁸⁰ B. DuRette (1999). Multiple Administrators for Electronic Voting. Bs.C. thesis.

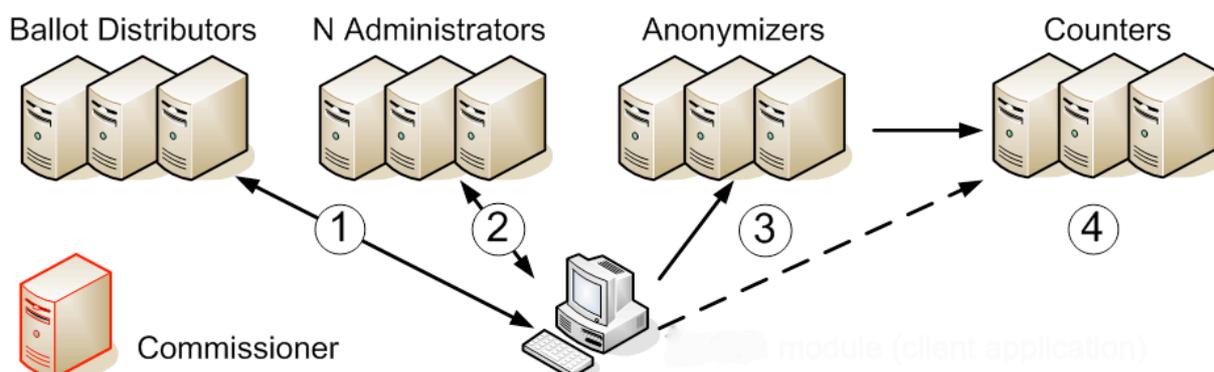
O valor de t controla o grau de conluio que é necessário que exista entre *Administrators* para, em conjunto com o *Manager*, poderem sabotar a eleição. No entanto, o EVOX-MA utiliza a mesma senha por utilizador em todos estes servidores, o que permite um grau de conluio efectivamente menor para chegar aos mesmos fins fraudulentos.

Em termos de tolerância a falhas o EVOX-MA tem vários problemas. A arquitectura possui um ponto singular de falha no *Manager* (a proposta contempla apenas a replicação de *Anonymizers* e *Counters*). Como este servidor é responsável pela distribuição de boletins e autorização do Direito de Voto, qualquer falha do mesmo bloqueia infalivelmente o processo eleitoral. Para além disso, este servidor é um ponto de estrangulamento do sistema se se considerarem eleições em larga escala. Finalmente, a perda de respostas de mais de $N-t$ dos *Administrators* ou do *Manager* é fatal para o votante, ficando daí em diante impedido de votar.

No REVS procurou-se resolver todos estes problemas, como se verá de seguida. O REVS é uma evolução do EVOX-MA que permite tolerar falhas de máquinas e comunicações e, desse modo, assegurar uma maior disponibilidade do sistema de votação sobre a Internet. Para além disso, o REVS possui um mecanismo de autenticação de votantes mais seguro que o seu antecessor, o que torna mais difícil a personificação de votantes por grupos de servidores do sistema.

Arquitectura do REVS

O REVS utiliza 5 tipos de servidores que suportam várias eleições em simultâneo: *Commissioner*, *Ballot Distributor*, *Administrator*, *Anonymizer* e *Counter*. Existe ainda um componente, o Módulo Eleitor, que é usada pelos votantes para participarem em eleições e que esconde as complexidades do protocolo (por exemplo, a obtenção de assinaturas às cegas).



O *Commissioner* existe para tratar queixas de votantes ou servidores. Para além disso, é ainda responsável por preparar eleições, gerar e manter secretas as chaves das eleições,

assinar o boletim de voto para garantir a sua correcção e definir os parâmetros operacionais da eleição (endereços e chaves públicas dos servidores, número t de assinaturas requeridas, etc.).

O *Ballot Distributor* distribui dados, preparados e assinados pelo *Commissioner*, pelos votantes: eleições activas e respectivos boletins de voto e parâmetros operacionais. Usou-se um servidor dedicado, que pode ser livremente replicado para melhorar o desempenho e a disponibilidade, por ser uma operação de transferência de dados potencialmente intensa.

Os N *Administrators* garantem o Direito de Voto. Um voto só é válido para a contagem final se possuir um número mínimo de t assinaturas de diferentes *Administrators* e as assinaturas só são concedidas uma vez a cada votante autorizado. Se $t > N/2$ então cada votante só pode gerar um voto válido.

Os *Anonymizers* garantem o anonimato dos computadores dos votantes perante os *Counters* e baralham a ordem dos votos recebidos e retransmitidos para impedir análises temporais. Cada votante pode usar um número arbitrário de *Anonymizers*.

Os *Counters* acumulam e validam votos submetidos pelos votantes através dos *Anonymizers*. Para a contagem final são agrupados os votos de todos os *Counters* e eliminados os votos repetidos (cada voto possui um identificador único gerado aleatoriamente pelo votante). Qualquer entidade com acesso aos votos acumulados pelos *Counters* pode efectuar a contagem final, o que é desejável para aumentar a confiança no resultado eleitoral.

Os votos entregues aos *Counters* são cifrados com uma chave pública da eleição, gerada pelo *Commissioner*. Só após o fim da eleição é que a correspondente chave privada é divulgada de modo a permitir a contagem final. Caso seja desejável, os votos podem ser entregues em claro aos *Counters*, o que permite um apuramento em tempo real dos resultados eleitorais. Haverá, decerto, certas eleições onde tal poderá ter interesse.

O REVS suporta ainda configurações sem pontos singulares de falha, uma vez que usa N *Administrators* e permite uma replicação livre dos demais servidores. O sistema tolera também até $N-t$ falhas de *Administrators*; se num dado instante o número de falhas for superior o sistema fica temporariamente incapaz de gerar votos válidos.

Processo eleitoral no REVS

O processo eleitoral é constituído por três fases: a preparação da eleição (criação de cadernos eleitorais, recolha dos elementos de identificação dos votantes autorizados, etc.), a realização da eleição, onde os eleitores expressam a sua opinião, e o apuramento dos resultados.

A realização da eleição possui três grandes passos, geridos pelo Módulo Eleitor:

1. Distribuição de boletins. O votante contacta um dos *Ballot Distributors* para pedir os elementos relativos a uma eleição - boletim, chave pública e configuração operacional - que são devolvidos assinados pelo *Commissioner*. Tal acontece em duas fases: primeiro o votante fornece a sua identificação e recebe a lista de eleições em que pode participar; em seguida pede os elementos relativos a uma dessas eleições.
2. Criação de um voto válido. O votante expressa a sua opinião no boletim obtido e “entrega-o” para ser assinado às cegas pelos *Administrators*. Antes da primeira assinatura o Módulo Eleitor cria e acrescenta ao boletim um identificador único, após o que envia o resumo do boletim, ocultado, para t *Administrators* para ser assinado. Antes desse envio o votante pode, e deve, guardar o estado do boletim num suporte não volátil para permitir a repetição do processo em caso de falha (porque a repetição implica a reutilização do mesmo voto, do seu identificador único e dos factores de ocultação usados). Esta salvaguarda, dependendo de como o sistema for usado, pode ter implicações com garantias de não coacção.

Quando um *Administrator* recebe um pedido de assinatura verifica se o mesmo vem de um votante autorizado, autentica-o e devolve a assinatura requerida do resumo ocultado. Essa assinatura é guardada para mais tarde ser devolvida caso o mesmo votante torne a requerê-la (o que pode acontecer caso tenham ocorrido falhas), o que é relevante para garantir o Direito de Voto.

As assinaturas recebidas pelo votante são transformadas, anulando o efeito da ocultação, revelando uma assinatura convencional de um *Administrator* sobre o resumo original do boletim de voto. Esta assinatura final pode ser validada por qualquer entidade, inclusive o votante, mas o *Administrator* que lhe deu origem não consegue relacioná-la com qualquer das assinaturas que produziu sobre resumos ocultados (o que garante o Anonimato).

Se o votante receber assinaturas inválidas, tal pode impedi-lo de produzir um voto válido, devendo reclamar junto do *Commissioner*. São suficientes $N-t+1$ *Administrators* em conluio para impedir alguém de votar devolvendo assinaturas inválidas. Este problema pode ser minorado baixando tanto quanto possível o valor de t . Se t for igual a $N/2+1$ então o grau de conluio necessário para fabricar ou negar votos é igual.

3. Entrega do voto. Depois de obtidas t assinaturas o voto está válido e pode ser entregue aos *Counters* através dos *Anonymizers*. O voto é constituído pelo boletim preenchido e pelas assinaturas dos *Administrators*, tudo cifrado com a chave pública da eleição e cifra híbrida. Este voto não pode ser inspeccionado antes da eleição terminar, porque está cifrado, nem pode ser alterado sem que tal invalide todas as assinaturas, o que o tornaria automaticamente inválido. Assim, muito embora os *Anonymizers* e os *Counters* possam “perder” votos, não o podem fazer de maneira a controlar

o resultado final da eleição. Por outro lado, o votante pode enviar uma cópia do seu voto para diversos *Counters*, pelo que a “perda” de uma dessas cópias pode ser facilmente tolerada.

O apuramento dos resultados só acontece depois de terminado o prazo estipulado para a eleição. Para esse apuramento o *Commissioner* revela a chave pública da eleição, que permite verificar todos os votos entregues a todos os *Counters*. Todas as entidades com acesso à totalidade dos votos nos *Counters* podem, então, proceder ao apuramento de resultados. Nesse apuramento devem ser usados apenas os votos não repetidos com t assinaturas válidas de *Administrators*. Qualquer votante pode realizar esse apuramento e verificar se o seu voto, que possui um identificador único copiado para um dispositivo de salvaguarda no passo 2, foi ou não incluído no mesmo. Se o voto tiver sido perdido o votante poderá eventualmente enviá-lo anonimamente ao *Commissioner* para que este o inclua na contagem final.

Para terminar, os *Administrators* publicam a lista de todas as assinaturas que produziram e para quem as produziram. Esta lista permite verificar se o conjunto de votos considerados no apuramento final é superior ao número de pessoas que efectivamente votaram, o que, a acontecer, revela uma fraude.

Avaliação do sistema REVS

A segurança do REVS tem de ser avaliada tendo em conta alguns pressupostos base, os quais são seguidamente apresentados. Dados esses pressupostos, consegue-se provar que o REVS garante as propriedades inerentes à democracia. Os pressupostos são os seguintes:

- Os algoritmos criptográficos usados são difíceis de violar. No REVS usam-se três algoritmos diferentes: (1) cifras assimétricas, para gerir assinaturas normais e às cegas e para cifrar chaves simétricas aleatórias usadas na cifra de votos entregues (cifra híbrida); (2) cifras simétricas para cifrar votos entregues; e (3) algoritmos de síntese para calcular todos os resumos necessários. Na prática usaram-se os algoritmos RSA, DES-triplo e SHA-1, respectivamente, para os quais não existem vulnerabilidades significativas conhecidas.
- As comunicações são autenticadas, i.e., os votantes têm garantias que falam com os servidores certos e que os dados não são alterados em trânsito. Na prática usaram-se canais seguros SSL/TLS⁸¹ e os servidores autenticam-se com a sua chave pública perante o Módulo Eleitor. Os servidores, os computadores dos votantes e as máquinas em geral

⁸¹ T. Dierks and C. Allen (1999). The TLS Protocol: Version 1.0, RFC 2246.

envolvidas na interligação entre os primeiros e os segundos, não são vulneráveis a vários tipos de sabotagem, tais como Negação de Serviço ou infecção com Vírus.

- Os *Anonymizers* são honestos e operam correctamente.
- O número mínimo de assinaturas de *Administrators* requeridas, t , é superior a $N/2$.
- O votante guarda os elementos críticos da sua participação (boletim preenchido, identificador único e factores de ocultação) no início do passo 2 do protocolo de votação.
- O identificador único de cada voto é efectivamente único e não associável a um votante. Na prática cada Módulo Eleitor gera um valor aleatório de 160 bits, que é virtualmente único, e ninguém consegue associar esses identificadores a votantes concretos.

Dados estes pressupostos, prova-se que o REVS possui as seguintes propriedades inerentes à democracia:

Integridade do Voto

Nenhum voto pode ser alterado com sucesso porque tal invalida as assinaturas dos *Administrators* que lhe estão afectas. Cada votante pode verificar se o seu voto está entre os publicados pelos *Counters* e, caso não esteja, pode reenviá-lo através do *Commissioner*. A eliminação de um voto é potencialmente complexa porque pode implicar a sua remoção de vários *Counters*. A validação universal de todos os votos reunidos pelos *Counters* impede a contagem de votos inválidos. Consequentemente, a Integridade do Voto é garantida.

Direito de Voto

Cada votante só pode votar uma vez porque $t > N/2$, logo cada votante só pode gerar um voto válido (que precisa de t assinaturas). Os votantes autorizados podem exercer o seu direito desde que estejam disponíveis t *Administrators* e um par *Anonymizer/Counter*. A perda de assinaturas pode ser tolerada porque os *Administrators* guardam-nas e reenviam-nas quando solicitado. Consequentemente, o Direito de Voto é garantido se o sistema não exceder um limite de falhas (configurável) e se o votante não alterar o seu voto (boletim preenchido e identificador único) durante o processo.

Anonimato

Os pressupostos antes referidas garantem a impossibilidade de associação entre votos e votantes - porque as assinaturas às cegas não permitem que o assinante relacione uma sua

assinatura de um valor ocultado com uma sua assinatura do valor original, o identificador único é gerado de forma aleatória pelo votante e os *Anonymizers* não associam computadores a votos.

Não-Coercibilidade

A Não-Coercibilidade não é, à partida, garantida pelo protocolo, se se desejar tolerância a falhas (porque o votante guarda dados críticos num suporte não-volátil móvel). No entanto, este aspecto está muito dependente das condições de controlo físico do suporte não-volátil. Por exemplo, se o suporte físico ficar à guarda de uma entidade oficial e for destruído após um prazo para apresentação de reclamações, então consegue-se garantir a Não-Coercibilidade.

Relativamente às propriedades inerentes aos sistemas de votação electrónica, temos a considerar:

Verificabilidade

Qualquer sujeito pode efectuar a contagem final, bastando para tal possuir a chave privada da eleição e as chaves públicas dos *Administrators* (todas disponibilizadas pelo *Commissioner*) e o somatório de todos os votos recolhidos pelos *Counters*. Cada votante pode também, como já vimos antes, verificar se o seu voto foi contado.

Detectabilidade

Esta característica depende do valor de t . Cada *Administrator* deverá estar afecto a um grupo de interesses e, tanto quanto possível, deverá ser o mais próximo possível de t para minimizar a possibilidade de falsificação de votos ou a marginalização de votantes. Também quanto maior for t maior é a sensibilidade do sistema a falhas, pelo que importa escolher valores de t e N que garantam minimamente a improbabilidade de conluio e assegurem alguma tolerância a falhas.

Disponibilidade

O sistema garante disponibilidade desde que possua um conjunto mínimo de servidores activos: um *Ballot Distributor*, t *Administrators*, e um par *Anonymizer/Counter*.

Recuperabilidade

O votante pode recuperar de interrupções no protocolo de votação, a partir do passo 2 do mesmo, desde que guarde e reutilize informação crítica para gerar o voto: o identificador único e os factores de ocultação. O boletim de voto preenchido não precisa de ser guardado porque o votante pode repetir o seu preenchimento.

Há ainda que referir um pormenor relevante do REVS que o distingue de outros sistemas de votação electrónica comerciais: o seu funcionamento interno é conhecido e o seu código pode ser divulgado para avaliação pública, o que permite detectar se tem erros ou funcionalidades escondidas. Este aspecto é muito importante para que os utilizadores do sistema possam ter confiança no seu funcionamento.

Experiência

Em Maio de 2003 realizou-se um teste ao REVS no IST, onde foi utilizado para dar suporte ao inquérito pedagógico semestral aos alunos. Escolheram-se dois cursos do IST para realizar a experiência, Licenciatura em Engenharia Informática e de Computadores e Licenciatura em Engenharia do Território.

O inquérito era constituído por 57 perguntas de diversos tipos, escolha múltipla (1 de n), múltipla escolha (m de n) e perguntas de resposta livre. A grande diferença dos inquéritos electrónicos em relação aos tradicionais em papel, além da verificação da correcção das respostas, foi a possibilidade de personalização dos mesmos, ou seja, como se sabia as disciplinas nas quais os alunos estavam inscritos, quando um aluno pedia um inquérito ele já estava pré-preenchido com a informação relativa ao curso, à disciplina e aos professores da mesma.

Nesta experiência participaram cinco entidades do IST. Para uma máxima disponibilidade foram instalados todos os servidores nos cinco computadores cedidos: *Ballot Distributor*, *Administrator*, *Anonymizer* e *Counter*. Na configuração utilizada era requerido que os inquéritos tivessem a assinatura de pelo menos 3 *Administrators* para que fossem considerados válidos.

Durante as duas semanas em que durou a votação houve, como seria de esperar, alguns problemas. O mais grave impossibilitou o uso de um dos computadores durante toda a experiência. Como a configuração inicial tolerava falhas simultâneas em dois computadores, durante a votação efectivamente tolerou-se apenas a falha de mais um computador. Outros problemas menos graves e temporários foram: a base de dados de um dos computadores parou de 3 em 3 dias e um sistema de ficheiros de outro computador falhou. Como estas últimas falhas não ocorreram em simultâneo conseguiu-se uma disponibilidade de 100%.

Na fase de validação e contagem dos votos detectou-se um erro de concretização que afectou uma pequena percentagem dos votos - o sistema era sensível ao conjunto de

caracteres por omissão da plataforma Java, que variava de computador para computador. No entanto, foi possível recuperar os inquéritos afectados e juntá-los à contagem final.

Comparando o processo de inquérito usando o REVS com o tradicional baseado em papel, conseguiu-se garantir um maior controlo do Direito do Voto (porque o sistema controla rigorosamente quem pode votar, enquanto no anterior tal não acontecia) mas desapareceu um tipo particular de Anonimato que anteriormente existia: anteriormente não se sabia se um dado aluno tinha sequer votado, o que não é possível com o REVS. Finalmente, o REVS permitiu maior rapidez no apuramento dos resultados finais, menos votos nulos (efectivamente nenhum, após a correcção do erro acima referido) e uma redução considerável do custo de realização dos inquéritos pedagógicos, tanto em termos de material como de horas de trabalho.

MOBILEREVS - UM SISTEMA DE VOTAÇÃO ELECTRÓNICA PARA DISPOSITIVOS MÓVEIS

Paulo Ferreira e Rui Joaquim

O objectivo do projecto MobileREVS consistiu em desenhar e implementar um sistema de votação electrónica baseado em dispositivos móveis, em particular, telemóveis. O sistema em causa respeita um conjunto de requisitos bastante exigentes dadas as especificidades dos processos de votação e dos dispositivos utilizados.

O MobileREVS pode ser utilizado em diversos contextos, quer a nível particular quer a nível da sociedade em geral. Alguns dos principais exemplos da utilização deste sistema são:

- Eleições - O sistema pode ser utilizado na concretização mais flexível dos direitos cívicos de cada indivíduo, ao usufruírem do seu direito de voto em qualquer lugar. O MobileREVS pode ser uma alternativa muito forte no combate às taxas de abstenção nas eleições legislativas, autárquicas e presidenciais, entre outras. Mais do que permitir que um indivíduo vote sem necessitar de sair de casa, permite que o voto seja exercido mesmo quando se encontra em movimento.
- Sondagens - Os organismos estatísticos podem efectuar sondagens através deste sistema. É claramente um ponto positivo na redução de custos operacionais. O processo ganha na rapidez de execução da sondagem e, principalmente, na capacidade mais fina da verificação de resultados em tempo real.
- Referendos - Os referendos (públicos ou privados) para decisão de diversos assuntos da sociedade podem também ser efectuados de forma rápida usando o MobileREVS.

O MobileREVS implementa as fases usuais de um processo de votação (registo, validação, recolha, verificação, contagem) assim como as propriedades requeridas para um sistema de votação electrónico.

O MobileREVS constitui uma adaptação do REVS para permitir a votação a partir de dispositivos móveis. A votação é realizada via rede telefónica móvel, nomeadamente GPRS/UMTS, fazendo uso das capacidades do próprio telemóvel. Como vimos no capítulo anterior, o REVS foi desenhado para ambientes distribuídos sujeitos a falhas, nomeadamente a Internet. O REVS também lida com falhas em cenários do mundo real, como falhas nas máquinas ou na comunicação, o que pode levar a interrupções no protocolo, permitindo assim um processo de voto seguro mesmo nesses ambientes. O MobileREVS herda assim todas estas características.

Requisitos específicos

Para que os sistemas de votação electrónica possam ser utilizados sem receio, são necessários protocolos que satisfaçam as propriedades patentes em praticamente todas as eleições. Deste modo, e à semelhança do REVS, o MobileREVS cumpre igualmente todas as propriedades inerentes à democracia.

No entanto, e apesar dos dois sistemas assentarem em ambientes distribuídos, os seus ambientes de execução são substancialmente diferentes. Enquanto que o REVS foi desenhado para clientes com computadores pessoais ligado à rede fixa, o MobileREVS foi desenhado para ambientes móveis. Tal facto traduz-se na introdução de novos requisitos:

- Mobilidade - Todos os serviços são oferecidos de igual modo em comparação a um local de votação fixo. As limitações da rede móvel (e.g., falta de rede) são as únicas restrições impostas;
- Espaço ocupado pela aplicação - Tendo em conta o facto do espaço disponível na memória dos telemóveis ser um recurso limitado, o espaço ocupado pela aplicação deve ser minimizado;
- Desempenho - A pouca capacidade de processamento dos telemóveis impõe um cuidado acrescido no desenvolvimento de aplicações para o mesmo, pois a realização de operações pesadas (e.g., funções criptográficas) pode levar ao aparente bloqueio da interface do utilizador;
- Consumo de energia - A bateria é outra das limitações impostas a ter em conta; com efeito, a sua exaustão pode implicar uma interrupção involuntária do processo de votação;
- Custos associados - O serviço de comunicações GPRS/UMTS providenciado pelos operadores de telecomunicações móveis é taxado em função do volume de tráfego trocado na rede. Como tal, a quantidade de dados trocados na rede deve ser minimizada, para que os custos associados não se tornem um problema na utilização do sistema.

Desafios técnicos

Embora alguns dos requisitos acima mencionados sejam de fácil resolução, outros necessitam de cuidados acrescidos. Isto para que, na prática, o processo de votação não

termine com uma série de erros impossíveis de recuperar, ou mesmo erros que não sejam sequer detectados.

Durante uma eleição são gerados inúmeros dados sensíveis que têm que atravessar meios de comunicação controlados por terceiros. Consequentemente, tornam-se acessíveis a intervenientes mal intencionados, sendo objecto de ataque e de abuso. Assim, é necessário recorrer a técnicas criptográficas que permitam garantir a segurança do sistema.

Em relação ao protocolo do REVS, o principal problema levantado para a sua migração para ambientes móveis prende-se com o cumprimento da propriedade de Anonimato. Esta propriedade pode ser satisfeita recorrendo a várias técnicas criptográficas; no entanto, são escassas as que são oferecidas pelas bibliotecas base existentes nos dispositivos móveis (e.g., da plataforma Java 2 *Micro Edition* - J2ME). Assim, é necessário recorrer ao uso de bibliotecas externas às oferecidas de base.

Um dos requisitos das aplicações com interface utilizador é que mantenham a sua interface sempre disponível de modo a responder a qualquer pedido do utilizador. No entanto, a troca de mensagens na rede com servidores ou a realização de operações de cifra cujo processamento é potencialmente demorado podem levar ao bloqueio da interface. Este problema advém da fraca capacidade de processamento dos telemóveis. Como tal, a solução passa pelo uso de vários fios de execução (*threads*) que impeçam o bloqueio da interface durante a realização de operações de processamento intensivo.

Embora hoje em dia os telemóveis de gama alta já recorram a cartões de memória, esta continua a ser um recurso muito limitado nestes dispositivos. Como tal, o espaço ocupado pela aplicação desenvolvida deverá ser minimizado, de modo a poder abranger o maior número possível de dispositivos.

Arquitectura e processo de votação

Tendo em conta a arquitectura do sistema REVS⁸², a arquitectura do sistema MobileREVS manteve-se semelhante. Seguidamente apresentamos de forma resumida os aspectos mais relevantes do sistema REVS de modo a facilitar a posterior descrição do MobileREVS. A arquitectura do REVS considera quatro tipos de servidores: *Ballot Distributor*, *Administrators*, *Anonymizers* e *Counters*. Iremos considerar ainda: um Módulo Eleitor, que é usado pelos eleitores para suportar as suas votações; e um módulo para preparar a eleição, o *Commissioner*.

A função de cada um dos módulos é a seguinte:

⁸² R. Joaquim, A. Zúquete and P. Ferreira (2003). REVS - A Robust Electronic Voting System. IADIS International Journal of WWW/Internet. Vol. 1, N. 2.

- *Commissioner* – É o módulo usado para preparar a eleição: registar os eleitores, definir as configurações operacionais (par de chaves da eleição, boletim, endereços e chaves públicas dos servidores, número de assinaturas requeridas, etc.). O *Commissioner* assina todos os dados relativos à eleição de modo a que qualquer pessoa possa verificar a sua autenticidade;
- *Ballot Distributor* – É responsável pela distribuição dos dados definidos pelo *Commissioner*: boletins e configurações operacionais. Toda a informação distribuída por este servidor tem de ser assinada pelo *Commissioner*, entidade de confiança dos eleitores. Como tal, podem haver vários *Ballot Distributors*, aumentando assim a eficiência e providenciando tolerância a falhas. Deste modo é aumentada a robustez do processo de distribuição de boletins;
- *Administrators* – São as entidades responsáveis pela validação dos votos. Um voto apenas é aceite na contagem final caso tenha a assinatura de N *Administrators* diferentes, em que N representa uma maioria dos *Administrators*. O eleitor utiliza palavras-passe diferentes para se autenticar perante cada *Administrator*, não permitindo assim que estes personifiquem o eleitor;
- *Anonymizer* – Este módulo tem a responsabilidade de providenciar o Anonimato, não permitindo que o *Counter* associe um boletim de voto a um eleitor. O *Anonymizer* baralha e retém temporariamente os votos, protegendo a identidade dos eleitores;
- *Counter* – Verifica a validade de cada boletim certificando-se que estão presentes todas as assinaturas requeridas dos *Administrators*. Os eleitores enviam os seus votos para os *Counters*, através dos *Anonymizers*, cifrados com a chave pública da eleição, prevenindo que estes possam interpretar os votos durante o processo eleitoral;
- Módulo Eleitor – É o módulo usado pelo eleitor para participar na eleição, executando todas as interações necessárias com os servidores.

No REVS os *Ballot Distributors*, os *Anonymizers* e os *Counters* podem ser replicados. A replicação é útil para evitar pontos únicos de falha que comprometam a realização do protocolo. Os *Administrators* requerem especial atenção pois cada boletim de voto deve ser assinado por uma maioria destes de modo a que o boletim seja considerado válido.

O protocolo REVS está dividido em três passos:

- Distribuição de boletins (1) – O eleitor contacta um *Ballot Distributor* e providencia o seu número de eleitor para receber uma lista de eleições que estão a decorrer e nas quais ele pode participar. Seguidamente o eleitor requer um boletim ao *Ballot Distributor*, indicando-lhe a eleição escolhida;
- Assinatura de boletins (2) – Após o eleitor expressar o seu voto, é criado um resumo do mesmo ao qual é aplicado um factor de cegamento. Enviado depois para $t > N/2$ dos

Administrators, juntamente com as palavras-passe respectivas, de modo a obter as suas assinaturas. Cada *Administrator* após receber o pedido do eleitor verifica se ainda não assinou um voto para o mesmo eleitor. Em caso negativo, este assina-o e devolve-o ao eleitor, guardando-o; em caso positivo, apenas devolve ao eleitor o voto previamente assinado;

- Submissão de boletins (3) – Neste passo o eleitor constrói um pacote do qual faz parte o seu voto, as assinaturas e um conjunto de bits que identificam a submissão do voto por parte de um eleitor. Nesta altura o Módulo Eleitor pode guardar esta informação em memória segura melhorando assim o desempenho do sistema. Seguidamente, o pacote é cifrado com uma chave de sessão juntamente com a chave da eleição e submetido através dos *Anonymizers*. Cada eleitor pode submeter o seu voto as vezes que achar necessário até se sentir confiante que o voto chegou ao seu destino.

Tal como foi referido, cada eleitor pode submeter o seu voto as vezes que entender, para qualquer um dos *Counters*. Portanto, diferentes *Counters* podem ter diferentes conjuntos de votos no final da eleição, e esses conjuntos podem conter votos repetidos. Para solucionar este problema é escolhido um Contador Mestre, que possui acesso aos restantes *Counters*. O Contador Mestre obtém a contagem final depois de juntar os votos de todos os *Counters*, eliminando os repetidos.

No final da eleição todos os *Counters* publicam os pacotes recebidos e os *Administrators* os boletins assinados. Deste modo, cada eleitor pode então verificar se o seu voto foi tido em conta para a eleição. Caso isso não tenha acontecido, este pode reclamar apresentando anonimamente o pacote previamente guardado no acto da submissão de boletins.

Módulo Eleitor

Obviamente, no MobileREVS o módulo de interacção do cliente com o restante sistema (denominado Módulo Eleitor) foi substituído por um telemóvel, tendo havido uma reavaliação da funcionalidade suportada por este. Em particular, foi necessário avaliar que operações de segurança podem ser suportadas pelo telemóvel.

O Módulo Eleitor foi desenvolvido para a plataforma J2ME. A comunicação com os servidores REVS é realizada exclusivamente através de RMI (*Remote Method Invocation*). Porém, o RMI ainda não está presente de raiz nas máquinas virtuais J2ME, ficando apenas disponível através da utilização da *Optional Package* com o mesmo nome⁸³. Actualmente, esta *Optional Package* não está presente em todos os telemóveis dos dife-

⁸³ JSR75 PDA Profile for the J2ME Platform. Java Community Process.

rentes fabricantes, ficando nalguns casos inviabilizada a comunicação directa entre o Módulo Eleitor e os servidores.

Para solucionar este problema optou-se pela criação de *proxies* para os servidores. Os *proxies* permitem criar um nível de indirectão que torna transparente no sistema os diferentes tipos de comunicação usados entre o Módulo Eleitor e os servidores. No fundo estes *proxies* não são mais do que *servlets*, i.e. pequenas aplicações Web em Java que se executam nos servidores Web interpretando os pedidos que lhe são direccionados e gerando as respostas adequadas.

Desta forma, cada servidor Web passa a conter um *servlet* diferente. Cada *servlet* é responsável por interpretar o pedido HTTP/HTTPS do Módulo Eleitor e transformá-lo num pedido RMI equivalente para o servidor J2SE respectivo. Para garantir a segurança nas comunicações os *servlets* devem estar localizados no mesmo servidor Web de cada servidor J2SE respectivo do REVS. Assim, a comunicação entre o *servlet* e o servidor J2SE encontra-se protegida sempre que se assumir que o servidor Web é, no seu todo, seguro.

Manteve-se o protocolo original do REVS, descrito anteriormente, com as respectivas adaptações para a nova arquitectura, assegurando-se a manutenção das características e propriedades originais. A comunicação entre o telemóvel e os servidores passa, então, a ser mediada pelos *servlets*, que permitem traduzir os pedidos HTTP/HTTPS em pedidos RMI equivalentes para os servidores. Ao mesmo tempo, os *servlets* permitem adaptar algumas das estruturas de dados de J2ME para J2SE, e vice-versa, dadas as limitações existentes da máquina virtual para telemóveis.

O Módulo Eleitor do MobileREVS decompõe-se estruturalmente em diversos módulos de código com diferentes finalidades: o módulo aplicação, o módulo apresentação, o módulo domínio, o módulo comunicação, e o módulo armazenamento.

O módulo aplicação define o comportamento do Módulo Eleitor durante as várias etapas do processo de votação. É nele que está programada toda a lógica funcional e onde é mantido o estado do processo de votação.

O módulo apresentação efectua o tratamento da interface do utilizador para o sistema, realizando a apresentação dos diversos elementos gráficos e interpretando os comandos do utilizador. No módulo domínio são representados os objectos manipulados pelo módulo aplicação, evidenciando as ligações e restrições entre os mesmos. Através deste módulo, o Módulo Eleitor é capaz de criar uma representação abstracta dos objectos, e.g. boletins de voto, e do estado do sistema.

O módulo comunicação permite ao módulo aplicação abstrair-se das características e idiosincrasias da comunicação, tratando dos aspectos mais específicos da comunicação realizada entre o Módulo Eleitor e os servidores. Finalmente, o módulo armazenamento oferece uma interface simples para o armazenamento persistente de dados no telemóvel, lidando internamente com os pormenores que daí advêm.

Esta modularização tem o objectivo principal de tornar o código reutilizável e fácil de modificar (por exemplo, alterar a maneira como a apresentação dos boletins é realizada ao utilizador sem afectar o restante código).

Processo de votação

Conforme indicado anteriormente, o módulo aplicação define o comportamento do Módulo Eleitor durante o processo de votação. De seguida é apresentado em detalhe o fluxo normal desse processo e são contempladas as excepções ao mesmo.

Na óptica do eleitor o processo de votação decompõe-se em três etapas essenciais: (1) a escolha de uma eleição em que ele pode participar; (2) o preenchimento do respectivo boletim de voto; e (3) a submissão do seu voto. Opcionalmente, na etapa de submissão do voto, o sistema possibilita o armazenamento do voto para continuação diferida do processo noutra altura (seja por falhas na comunicação ou para o eleitor se sentir mais seguro de que o seu voto foi entregue).

Assim que iniciada, a aplicação apresenta ao utilizador um formulário para a sua autenticação. O utilizador deverá fornecer o seu identificador de eleitor e a palavra-passe correspondente. Ao contrário do REVS, não é possibilitada a introdução conjunta de um PIN, facilitando a utilização da aplicação pelo eleitor. Optou-se antes pela utilização de uma palavra-passe com um número mínimo de 8 caracteres, de modo a reforçar a segurança da autenticação.

Os dados serão, então, enviados para um *Ballot Distributor* que efectuará a autenticação do eleitor. Se os dados em causa estiverem correctos, o utilizador tem a possibilidade de interagir com o sistema para votação. O utilizador também tem a capacidade de definir algumas opções de configuração da utilização do sistema nesta etapa.

Inicialmente são apresentadas as eleições disponíveis, i.e., as eleições em que o eleitor pode participar, fornecidas por um dos *Ballot Distributors* na interacção anteriormente referida. Assim que o utilizador escolher uma das eleições possíveis, o Módulo Eleitor verifica se já existe uma sessão armazenada no telemóvel para essa eleição. Entenda-se por sessão o estado que pode ser armazenado pelo utilizador durante uma eleição em que este participa. Se já existir uma sessão armazenada, é dada a possibilidade de enviar novamente o mesmo voto (não é possível alterá-lo). Caso não exista nenhuma sessão armazenada, a aplicação requer ao *Ballot Distributor* o boletim de voto da eleição escolhida, que é então apresentado ao utilizador. Juntamente com o boletim são fornecidas as configurações necessárias do sistema (endereços dos vários servidores, chave pública da eleição, chaves públicas dos *Administrators*, etc.).

Depois do utilizador preencher o boletim, ele terá de confirmar as suas respostas antes de as submeter. Nesta etapa o utilizador pode rever as suas respostas e detectar eventuais erros, tendo a possibilidade de efectuar correcções.

Logo após a confirmação das respostas do utilizador, o sistema está pronto para submeter o seu voto. Nesta etapa é verificada a opção de personalização relativa ao armazenamento da sessão. Por omissão, a opção está configurada para guardar a sessão, mas o utilizador também tem a possibilidade de nunca a guardar ou que lhe seja perguntado sobre o que fazer. Posteriormente, o voto é enviado aos *Administrators* para ser assinado. Se não for possível comunicar com t deles o processo de votação é interrompido neste ponto, oferecendo a possibilidade ao utilizador de efectuar uma nova tentativa ou armazenar o voto, caso ainda não o tenha feito, para poder continuar a votação noutra altura.

Aquando do sucesso da comunicação com os *Administrators* a sessão será actualizada se tiver sido guardada anteriormente. Note-se que caso o utilizador esteja a efectuar a continuação diferida de uma sessão esta será sempre actualizada. Posteriormente, o voto é submetido para os *Anonymizers/Counters*. Mais uma vez poderão existir problemas na comunicação. Nesse caso o utilizador será avisado da situação de erro e ser-lhe-ão oferecidas as possibilidades de tentar novamente a comunicação ou armazenar a sessão, se ainda não o tiver feito, para completar a votação noutra altura.

Assim que o processo de votação for bem sucedido o utilizador é informado da sua correcta conclusão. Neste instante, o utilizador poderá escolher entre participar noutra eleição disponível ou abandonar a aplicação.

Criptografia

O MobileREVS utiliza um conjunto de algoritmos criptográficos da biblioteca *Bouncy Castle (Light Edition)* para assegurar as propriedades de Integridade dos Votos e Anonimato. A escolha da utilização desta biblioteca no Módulo Eleitor deveu-se a duas razões: (1) a implementação raiz do J2ME não oferece nenhuma destas funcionalidades; e (2) as alternativas são escassas, e o seu acesso é muito limitado.

As assinaturas do MobileREVS são realizadas utilizando chaves RSA de 1024 bits e um resumo SHA-1 (160 bits). Para cifra simétrica é utilizado o 3DES. A cifra do pacote a enviar utiliza, assim, uma combinação híbrida RSA-3DES, ou seja, os dados são cifrados com 3DES e a chave simétrica é cifrada com RSA. Foi no entanto necessário implementar um módulo para suportar as assinaturas às cegas, módulo este que mais tarde foi incorporado na biblioteca *Bouncy Castle*.

Comunicação

Genericamente existem três meios de comunicação usados pelos telemóveis. São eles o SMS (*Short Message Service*), o WAP (*Wireless Application Protocol*) e o GPRS (*General Packet Radio Service*), ou UMTS (*Universal Mobile Telecommunications System*) no caso das redes móveis de terceira geração. A utilização do GPRS/UMTS como meio de comunicação para o sistema MobileREVS foi determinada com base na adequação do mesmo para os propósitos do sistema.

O SMS e o WAP revelam-se dois meios de comunicação visivelmente desajustados para o MobileREVS. Por um lado, ambos têm baixas taxas de transferência e latências elevadas, algo que no caso do MobileREVS não é aceitável dada a troca de quantidades elevadas de dados. Por outro lado, são meios de comunicação muito inflexíveis neste contexto. O SMS exige uma sintaxe de escrita de mensagens. O WAP exige a alocação permanente de recursos ponto-a-ponto enquanto a ligação está activa. Além disso, a utilização destes meios de comunicação teria custos impraticáveis no ambiente real das operadoras de telecomunicações móveis: (1) através do SMS seria preciso trocar muitas mensagens, dado o limite máximo de 160 caracteres por mensagem; e (2) o serviço WAP é cobrado por tempo de utilização, ao invés do volume de dados como acontece em GPRS/UMTS.

O GPRS/UMTS tem vindo a ser utilizado mais frequentemente como meio de acesso à Internet e troca de dados a partir de dispositivos móveis, apresentando custos cada vez mais reduzidos. Com base nos argumentos apresentados, a escolha do meio de comunicação usado recaiu sobre o GPRS/UMTS.

Relativamente ao protocolo de comunicação usado, foi escolhido o HTTP/HTTPS. Apesar de existirem diversos tipos de ligação disponibilizados pelo MIDP 2.0 (HTTP/HTTPS, *sockets*, *datagrams*) a utilização de HTTP/HTTPS oferece algumas vantagens: (1) portabilidade, dada a menor dependência das redes de comunicação utilizadas; (2) gestão automática de ligações; (3) encapsulamento de qualquer tipo de dados, através de MIME (*Multipurpose Internet Mail Extensions*); e (4) facilidade de integração com os servidores actuais. Além disso, a utilização de HTTP oferece ainda a vantagem adicional da compatibilidade, dado que este é o único tipo de ligação que deve ser obrigatoriamente disponibilizado pelos fabricantes de telemóveis.

Visto que o desenvolvimento do sistema assenta sobre a versão 2.0 do MIDP, escolheu-se utilizar o protocolo HTTP/HTTPS, de forma a possibilitar a criação de canais seguros entre o telemóvel e os servidores, sempre que tal for possível.

Tratamento dos boletins de voto

De acordo com o protocolo do MobileREVS, o *Ballot Distributor* envia um boletim de voto para o cliente com uma estrutura XML. Como tal, torna-se imperativo que o Módulo Eleitor seja capaz de processar esta meta-linguagem, mapeando o boletim num objecto de domínio. De maneira a cumprir esta tarefa é necessário: (1) utilizar um dos processadores de XML existentes; ou (2) produzir um processador específico para a aplicação.

A produção de um processador específico apenas faria sentido para a optimização dos recursos consumidos pela aplicação. Visto que actualmente já existem diversos processadores disponíveis, que foram desenhados com esta finalidade, optou-se pela utilização de um processador existente⁸⁴.

O processamento de XML é uma tarefa que, tradicionalmente, consome bastantes recursos. Os telemóveis são dispositivos de processamento lento e com memória escassa. Além disso, alguns telemóveis limitam o tamanho máximo dos MIDlets, tornando-se importante minimizar o espaço ocupado pelos mesmos. Pretende-se, portanto, que o processador utilizado seja simultaneamente eficiente e compacto, ocupando a menor quantidade de espaço possível em memória.

As técnicas de processamento de XML estão ligadas com os três tipos fundamentais de processadores. Os aspectos que diferenciam a sua escolha são: (1) o modo como se pretende que a aplicação se comporte no processamento dos documentos; e (2) o tipo de documentos que se pretende manipular.

Um processador de modelos interpreta todo um documento XML e cria uma representação do mesmo em memória. Um processador sequencial interpreta sequencialmente um documento XML. À medida que várias partes são encontradas, o processador informa a aplicação. Um processador guiado interpreta pequenas porções do documento de cada vez. A interpretação é guiada pela aplicação, que requer repetidamente o pedaço seguinte.

Ao criar uma representação de um documento XML inteiro em memória, o processador de modelos é o que utiliza mais memória em execução. Claramente, esta solução não se adequa ao desenvolvimento de aplicações para telemóveis pelas restrições referidas anteriormente.

⁸⁴ Jonathan Knudsen (2002). Parsing XML in J2ME.

A grande diferença entre os restantes métodos reside no ponto de controlo da tarefa de processamento. No processador sequencial o controlo está a cargo do processador, que informa a aplicação sempre que tem nova informação; no processador guiado o controlo é da aplicação, que requer explicitamente as partes seguintes do documento.

Desta maneira é possível verificar que o processador guiado é o tipo mais adequado para os MIDlets. Ao permitir que a aplicação detenha o controlo da tarefa de processamento do XML, esta pode ser desenvolvida de maneira a manter em memória apenas a parte com que está a lidar no momento. Quando mais nada tiver a fazer com essa parte pode libertá-la da memória e passar à seguinte.

Actualmente existem alguns processadores Java específicos para dispositivos de recursos limitados, como é o caso dos telemóveis. A tabela seguinte resume as principais características de cada um deles.

Nome	Tipo	Tamanho (KB)	Integração MIDP
ASXMLP 020308	sequencial, modelo	6	sim
kXML 2.2	guiado	11	sim
kXML 1.2	guiado	16	sim
MinML 1.7	sequencial	14	possível
NanoXML 1.6.4	modelo	10	possível
TinyXML 0.7	modelo	12	possível
Xparse-J 1.1	modelo	6	sim

A coluna “Tipo” indica o tipo de processador de acordo com o que foi indicado anteriormente. O tamanho representa o espaço ocupado pelas classes do processador, que corresponde a uma aproximação do aumento do tamanho total da aplicação que as utilize. A coluna “Integração MIDP” indica a facilidade com que o processador pode ser integrado num MIDlet. Embora três dos processadores não possam ser directamente utilizáveis pelos MIDlets apenas são precisas simples modificações para que tal passe a ser possível.

Conforme foi determinado, o processador ideal para colmatar as limitações impostas pelos telemóveis aos MIDlets deve ser do tipo guiado. De acordo com a tabela apenas o kXML⁸⁵ é deste tipo, pelo que foi o escolhido para o desenvolvimento do projecto.

Armazenamento

Durante o processo de votação o utilizador tem a capacidade de armazenar o seu voto, algo que lhe permitirá retomar o processo de votação numa outra altura. Como tal, é necessário recorrer a mecanismos que efectuem armazenamento persistente.

O armazenamento persistente pode ser efectuado em dois tipos de memória: (1) na memória interna do telemóvel; ou (2) num cartão de memória, instalado no telemóvel. A principal vantagem do armazenamento do voto ser feito num cartão de memória é a capacidade do eleitor poder retomar a votação a partir de outros telemóveis.

No J2ME existem bibliotecas que permitem lidar com o armazenamento de dados nestes dois tipos de memória. O *Record Management Store* (RMS) oferece uma interface para os MIDlets armazenarem os seus dados na memória do telemóvel. Esta biblioteca é oferecida no perfil MIDP do telemóvel, encontrando-se presente em qualquer implementação J2ME. Por outro lado, o acesso aos cartões de memória está condicionado pela presença da *Optional Package* FileConnection, do pacote PDA *Optional Packages*, dependendo assim do fabricante de cada telemóvel. No entanto, já existe uma boa quantidade de telemóveis a implementar esta *Optional Package*.

Perante os factores apresentados, a decisão recaiu sobre a utilização do RMS para o armazenamento do voto. A utilização da *Optional Package* FileConnection é uma outra possibilidade, podendo ser incluída numa versão posterior do MobileREVS.

Avaliação das propriedades

Iremos agora avaliar se as propriedades do REVS continuam a ser respeitadas no sistema MobileREVS.

Integridade do Voto

Em primeiro lugar, um voto não pode ser alterado pois isso iria invalidar a assinatura de todos os *Administrators*. Segundo, a eliminação de um dos votos dos *Counters* não é uma tarefa trivial, visto que eles podem estar em qualquer servidor e seria necessário eliminar

⁸⁵ kXML: Open Source XML Pull Parser API. <http://kxml.sourceforge.net/>

o voto de todos eles. Para além disso, é sempre possível ao utilizador efectuar nova submissão caso tenha o voto guardado de forma persistente. Em terceiro lugar, tendo em conta que as assinaturas são publicadas com os votos e podem ser verificadas por qualquer pessoa, é muito pouco provável que um voto inválido faça parte da contagem final.

Direito de voto

A um eleitor apenas pode ser concedida uma assinatura para uma determinada eleição caso este tenha sido incluído na lista de eleitores da mesma. Cada eleitor só pode votar uma vez em cada eleição pois o seu voto apenas é considerado na contagem final caso tenha a assinatura da maioria dos *Administrators* ($t > n/2$). Assim garante-se que um eleitor não pode adquirir mais do que um voto válido. A obtenção de resultados parciais no MobileREVS só é possível com o conluio da autoridade eleitoral, que possui a chave da eleição, e dos *Anonymizers* ou *Counters*, que possuem os votos cifrados. Assim, se a autoridade eleitoral e pelo menos t *Administrators* forem honestos todos os aspectos relacionados com o direito de voto são garantidos.

Anonimato

A única forma de uma autoridade eleitoral conseguir ligar um eleitor a um voto é através de um conluio entre os *Administrators*, *Anonymizers* e *Counters*. Enquanto os *Anonymizers* se mantiverem honestos é impossível estabelecer qualquer ligação temporal entre o momento da assinatura dos votos e a sua submissão aos *Counters* e, como tal, o Anonimato é garantido.

Verificabilidade

A contagem final dos votos pode ser feita por qualquer pessoa através da verificação das assinaturas nos votos e da sua soma. Cada eleitor pode verificar se o seu voto está correcto, e assume que os outros votos também estão correctos devido à assinatura que eles têm.

Disponibilidade

Visto que todos os servidores podem ser replicados, o MobileREVS não tem um ponto de falha único. O sistema está disponível enquanto houver um conjunto mínimo de servidores a funcionar correctamente. Esse conjunto mínimo é constituído por um *Ballot Distributor*, t *Administrators*, e um par *Anonymizer/Counter*.

Recuperabilidade

O eleitor pode recuperar de uma interrupção desde que mantenha em memória os dados do voto.

Integridade do Sistema

No MobileREVS nenhuma autoridade eleitoral consegue corromper, sozinha, as propriedades do sistema de votação electrónica. No entanto, a questão do conluio merece especial atenção. Num conjunto de N *Administrators* e t assinaturas requeridas é necessário o conluio de $N - t + 1$ *Administrators* para impedir um eleitor de votar, ou seja, à medida que t aumenta torna-se mais fácil impedir o processo de votação. Por outro lado, para simular um voto válido por parte dos *Administrators* é necessária a cooperação de t deles, o que se torna mais difícil à medida que t aumenta. Como tal, é necessário um balanceamento ponderado sobre os valores de N e t .

Avaliação dos requisitos

Nesta secção são avaliados diversos requisitos considerados para o MobileREVS, considerando em particular os aspectos relacionados com a utilização de dispositivos móveis.

Mobilidade e falhas de energia

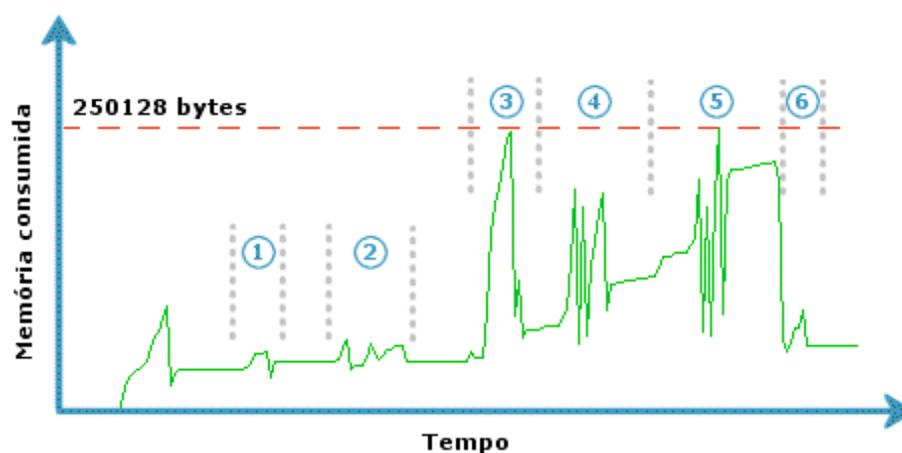
Em caso de falha na rede móvel ou falhas de energia (e.g., bateria descarregada) o eleitor pode recuperar o estado do seu voto se o tiver salvaguardado previamente. A opção de guardar o voto (juntamente com todas as informações do seu estado) está activada por omissão.

O estado do voto é salvaguardado em três partes distintas: (1) após o preenchimento do boletim, evitando assim que o utilizador o tenha de voltar a preencher; (2) após obter as assinaturas, quer perfaça o total de assinaturas requeridas ou não, evitando posteriores comunicações desnecessárias com os *Administrators* já contactados; e, finalmente, (3) no final do processo de votação, assinalando a submissão com sucesso do voto.

Memória

O espaço total ocupado pelo Módulo Eleitor, aplicação a ser instalada no telemóvel, é de 139 KB. Este é um tamanho considerado admissível visto estar na média de outras aplicações para telemóveis.

Relativamente à memória consumida durante a execução da aplicação, esta vai variando consoante a fase do protocolo de votação do MobileREVS. Tendo em conta que o consumo de memória não depende do dispositivo móvel, optou-se por recorrer à ferramenta



de monitorização de memória do *Wireless Toolkit 2.2* para a analisar.

A figura acima representa a evolução da utilização da memória volátil durante um processo de votação com duas assinaturas requeridas e um par *Anonymizer/Counter*. As etapas assinaladas na figura são descritas em seguida:

1. Contacto com o *Ballot Distributor* para obtenção da lista de eleições;
2. Contacto com o *Ballot Distributor* para obtenção do boletim de voto;
3. Preparação da votação;
4. Obtenção de uma assinatura junto do 1º *Administrator*;
5. Obtenção de outra assinatura junto do 2º *Administrator*;
6. Submissão do voto para o par *Anonymizer/Counter*.

De acordo com a figura, a memória volátil consumida pela aplicação não sofre variação significativa durante o contacto com o *Ballot Distributor* (1 e 2). Posteriormente, observa-se uma subida abrupta do consumo, até atingir o seu ponto máximo (3) de aproximadamente 250 KB, situação que ocorre logo após a preparação da votação e antes do

envio do voto aos *Administrators*. Por preparação da votação entende-se a geração do pacote de votação e dos factores de cegamento.

Para cada *Administrator* envolvido no processo de votação assiste-se a um incremento significativo da memória volátil consumida do telemóvel (4 e 5). Esta situação acontece no momento da resposta de cada um, visto serem retidas todas as assinaturas em memória volátil até ser possível armazená-las em memória persistente. Uma alternativa possível poderia passar pelo armazenamento imediato de cada assinatura, logo após a sua recepção. Porém, os acessos às funções de armazenamento persistente induziriam um atraso significativo no processo. Além disso, a memória volátil consumida pela aplicação em situações mais comuns de configuração do sistema (no exemplo foram usados dois *Administrators*) é relativamente baixa dados os limites dos telemóveis actuais. No caso do Nokia 6600, por exemplo, são disponibilizados 3 MB de memória volátil para as aplicações Java⁸⁶.

No final, depois de armazenados de forma persistente, o voto e as assinaturas dos *Administrators* são enviados aos pares *Anonymizers/Counters* (6). Analisando agora a utilização da memória persistente, esta também apresenta variações significativas. A tabela abaixo revela o espaço ocupado em memória persistente pelo voto, nas fases do processo de votação onde é possível salvaguardá-lo.

# assinaturas requeridas	Memória persistente consumida (bytes)		
	após preenchimento do boletim	após obtenção das assinaturas	após submissão do voto
1	768	511	511
2	1110	654	654
3	1452	799	799
4	1794	934	934

Como se pode verificar, o valor máximo da memória persistente utilizada atinge-se na primeira salvaguarda do voto, ou seja, após o preenchimento do boletim. Neste instante é armazenada toda a informação relativa ao estado da votação. Porém, assim que as assinaturas requeridas são obtidas, alguma desta informação (e.g. os factores de cegamento) deixa de ser necessária, não sendo armazenada em memória. É este facto que justifica a diminuição do espaço ocupado persistentemente pelo voto à medida que o processo de votação se aproxima do fim.

⁸⁶ Nokia 6600 Device Details (2003). Forum Nokia. June 16, 2003.

Tendo em conta a memória disponível nos telemóveis de hoje em dia, bem como a crescente utilização de cartões de memória, os valores apresentados na tabela não constituem um factor limitativo na utilização do sistema.

Desempenho

O desempenho é outro dos factores críticos do sistema. Conforme foi referido anteriormente, o protocolo de votação exige a cifra de dados, a assinatura dos *Administrators*, comunicações remotas, entre outras operações de poder computacional elevado.

Na tabela seguinte são apresentados os tempos de execução das diferentes etapas de um processo de votação para os telemóveis Nokia 6600 e Sony Ericsson P900. É usada como referência uma eleição com dois *Administrators*, um *Counter* e um boletim de voto com 1 KB. Os valores da tabela expressam-se em milisegundos.

Telemóvel	# assinaturas requeridas	Distributor		Administrator	Anonymizer/Counter	Total
		Lista de eleições	Obtenção do boletim	Assinatura	Submissão	
Nokia 6600	1	196	281	18510	16500	35487
	2	212	515	28953	16266	45946
Sony Ericsson P900	1	32	46	8016	7985	16079
	2	16	47	10281	6890	17234

Existe uma diferença significativa entre os valores obtidos nos dois telemóveis, justificada pelas diferentes características do hardware de cada um. O Sony Ericsson P900 possui maior poder computacional que o Nokia 6600, facto que permite que a realização das operações de votação seja mais rápida.

Por outro lado, é possível verificar que o aumento do número de assinaturas requeridas não incute um aumento proporcional do tempo de execução da fase de obtenção de assinaturas. Ou seja, de acordo com a tabela, duas assinaturas são obtidas em menor tempo que o dobro da obtenção de uma. Este desempenho deve-se à utilização de *threads* para comunicação simultânea com os *Administrators*.

Comunicações

O tráfego de dados em comunicações remotas é um dos factores mais importantes para os utilizadores de aplicações móveis, já que são normalmente taxados pelos operadores de

telecomunicações. Para avaliar este requisito configurou-se uma eleição de referência composta por um boletim de voto com 1 KB, um único *Counter* e exigindo a assinatura de dois *Administrators*. Os resultados estão expressos na tabela seguinte, em termos de dados enviados e recebidos.

Servidor	Etapa	Dados enviados (bytes)	Dados recebidos (bytes)
Distributor	Lista de eleições	29	103
	Obtenção do boletim	33	1490
Administrator	1ª Assinatura	164	134
	2ª Assinatura	164	134
Anonymizer / Counter	Submissão	576	2
		966	1863
TOTAL		2829	

O tráfego total do processo de votação, para a eleição acima referida, foi de aproximadamente 2,8 KB. Na comunicação com o *Ballot Distributor* os dados recebidos são variáveis, dependendo do número de eleições disponíveis e do tamanho do boletim de voto. O mesmo acontece com a comunicação com os *Anonymizers/Counters*, onde a quantidade de dados varia com o tamanho do boletim. Relativamente aos *Administrators*, são trocados 298 bytes por cada assinatura requerida. Estes dados não variam com o tamanho do boletim de voto, já que apenas é enviado um resumo do voto (tamanho fixo).

Em suma, a quantidade de dados trocados varia com o tamanho do boletim de voto, o número de assinaturas requeridas e o número total de *Administrators* e *Anonymizers/Counters*.

Tendo em conta as tarifas actuais dos operadores de telecomunicações móveis portugueses, os custos associados ao tráfego gerado no sistema são bastante aceitáveis. O custo da transferência de dados é taxado aos conjuntos de 10 KB de informação, de acordo com os seguintes valores:

- TMN: 0,005€/KB
- Vodafone: 0,0024€/KB
- Optimus: 0,0025€/KB

Para a eleição de referência indicada anteriormente, com dois *Administrators*, onde são transferidos 2,83 KB de dados, tem-se um custo associado entre 0,024€ (Vodafone) e

0,05€ (TMN), visto não se ter ultrapassado o limite de 10 KB de informação. Rapidamente se conclui que em termos monetários o custo da comunicação via GPRS/UMTS é comportável, não se tornando um entrave à utilização do sistema.

SUPORTE À MOBILIDADE DOS VOTANTES⁸⁷

André Zúquete

Os sistemas de votação electrónica via Internet são apelativos por diversas razões, umas das quais é a mobilidade dos votantes. Os sistemas baseados em papel normalmente obrigam os votantes a deslocar-se a locais de voto específicos. Mas através da Internet os votantes podem contactar os servidores eleitorais praticamente a partir de qualquer ponto no mundo. Contudo, as máquinas usadas pelos votantes para expressar e submeter o seu voto têm de ser confiáveis. Nomeadamente, essas máquinas não deverão ser capazes de obter as credenciais usadas pelos votantes para a sua autenticação, divulgar o sentido de voto para além dos servidores eleitorais, nem interferir de forma perniciosa com o processo de votação.

O desenvolvimento de aplicações cliente confiáveis de apoio à votação via Internet sobre sistemas operativos banais e generalistas, como o Windows, Linux ou MacOS, é difícil. A complexidade destes sistemas operativos e o seu grau de liberdade em termos de configuração e capacidades instaladas torna praticamente impossível a tarefa de assegurar a confiança no funcionamento de uma aplicação local de apoio ao voto através da Internet. Consequentemente, algumas componentes críticas das aplicações cliente de apoio ao voto pela Internet devem ser instaladas em ambientes computacionais restritos, capazes de providenciar o que normalmente se designa como *Trusted Computing Base* (TCB), ou seja, um ambiente computacional confiável.

Neste sentido, foi estudado o desenvolvimento de uma aplicação cliente confiável de apoio à votação via Internet para uma TCB formada por um cartão inteligente (*smartcard*) e um terminal FINREAD. Este terminal permite proteger a entrada de dados do votante – códigos de identidade ou de autenticação e escolhas relativas ao voto – e algumas saídas de dados – apresentação do boletim de voto ao votante e apresentação das suas escolhas relativas ao voto. O cartão inteligente fornece protecção para as credenciais de autenticação do votante – pares de chaves criptográficas assimétricas e assinaturas digitais efectuadas pelo votante no decurso do seu processo de votação – e permite efectuar a validação de assinaturas digitais, criadas por uma autoridade eleitoral bem conhecida, dos dados relativos à eleição recebidos dos servidores eleitorais através da Internet – boletim de voto, elementos de localização e identidade dos servidores eleitorais. Esta TCB e um qualquer computador (PC) ligado à Internet permitem o desenvolvimento de uma apli-

⁸⁷ Este texto é um resumo de um artigo apresentado no Workshop WRAITS 2007: “An Intrusion-Tolerant e-Voting Client System”, André Zúquete, Carlos Costa and Miguel Romão, 1st Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS 2007), Lisboa, Portugal, Março de 2007.

cação cliente de apoio à votação via Internet que é tolerante a intrusões. A expressão “tolerância a intrusões” significa que as intrusões podem acontecer mas, no pior caso, apenas podem impedir a conclusão com êxito do processo de votação, mas não violar outras premissas do votante (privacidade, inalterabilidade do voto, etc.). O PC serve, à partida, para efectuar a ponte necessária entre a TCB e a Internet. Um PC comprometido, através de uma intrusão ou não, apenas poderá impedir a entrega ao servido eleitoral de um voto controlado pela TCB, o que configura um ataque do tipo Negação de Serviço (*Denial of Service*, DoS).

Para concretizar e testar a aplicação cliente sobre a TCB antes indicada usou-se o sistema REVS, já apresentado num capítulo anterior. Neste sistema a aplicação cliente, designada por Módulo Eleitor, é uma *Applet Java* que se executa num navegador (*browser*) e numa máquina virtual Java do PC usado pelo votante. Muito embora o nosso objectivo fosse apenas alterar a aplicação cliente do REVS para a mesma usar a TCB, na prática foi preciso alterar também algumas interacções com os servidores eleitorais para introduzir a autenticação dos votantes através de assinaturas digitais criadas com um cartão inteligente (originalmente o REVS usava senhas memorizáveis).

Vulnerabilidades do Módulo Eleitor do REVS

Como antes se referiu, o Módulo Eleitor é uma *Applet Java*. O Sistema do Votante é, assim, constituído pelo Módulo Eleitor, pela máquina virtual que o interpreta e pelo sistema operativo onde a máquina virtual se executa. O Sistema do Votante pode ser comprometido de diversas formas com o intuito de interferir com o anonimato e privacidade dos votantes e com a integridade dos votos no que diz respeito aos votos expressos localmente. Seguidamente apresentam-se algumas acções que podem ser efectuadas por um Sistema do Votante malicioso:

- Fornecer boletins de voto falsos ao votante e enviar votos falsos em vez do que o votante expressou. Tal constitui um risco para a Integridade dos Votos.
- Roubar as credenciais do votante - identidade e senha. Tal representa um risco de personificação do votante por terceiros com consequências no Direito de Voto.
- Uso para outros fins da identidade do votante e do seu voto. Tal representa um risco para o Anonimato e a Privacidade do voto.

Para evitar as acções maliciosas acima expressas o Sistema do Votante deverá usar a TCB para:

- Proteger as credenciais do votante – a chave pública do *Commissioner* – usada para validar a informação recebida dos *Ballot Distributors*.

- Proteger a entrada de dados relativa ao preenchimento do boletim de voto pelo votante.
- Proteger a identidade do votante e impedir o roubo das suas credenciais de autenticação.
- Proteger toda a informação crítica relativa ao processo de votação através do REVS, incluindo os factores de obscurecimento usados na obtenção de assinaturas às cegas.

Neste sentido, parte do Módulo Eleitor tem de migrar para a TCB, de forma a proteger a informação crítica de validação (por exemplo, a chave pública do *Commissioner*), operações de entrada/saída críticas do votante e todos os dados críticos, permanentes ou temporários, envolvidos no processo de votação do REVS.

Novo sistema do votante

Para concretizar a TCB escolheu-se um sistema constituído por um cartão inteligente e por um leitor específico, um dispositivo FINREAD. Estes dois componentes são descritos em seguida. Existem outros trabalhos envolvendo o uso de cartões inteligentes para suportar votações electrónicas^{88 89 90}. Neles o cartão inteligente é usado fundamentalmente para efectuar cálculos com a chave privada do votante num ambiente seguro e pessoal. Neste trabalho deram-se vários passos em frente, porque se usou o cartão inteligente para guardar outros dados críticos, como a chave pública do *Commissioner* e valores criptográficos usados para produzir o voto. Para além disso, protegemos a interacção entre o votante e o cartão inteligente através de um terminal seguro de entrada/saída de dados com uma interface humano-computador – o dispositivo FINREAD. Tanto quando sabemos, esta foi a primeira vez que um dispositivo FINREAD foi usado para suportar sistemas usados por votantes.

Cartões inteligentes

⁸⁸ C.-B. Breunese, B. Jacobs, and M. Oostdijk (2002) Voting using Java Card smart cards: A case study.

⁸⁹ S. Canard and H. Siberty (2006) How to fit cryptographic e-voting into smart cards. In Frontiers in Electronic Elections (FEE 2006), Hamburg, Germany.

⁹⁰ J.-K. Jan and C.-C. Tai (1997) A Secure Electronic Voting Protocol with IC Cards. Journal of Systems and Software, 39(2).

Os cartões inteligentes fornecem um ambiente devidamente protegido para armazenar informação privada crítica, tais como chaves criptográficas⁹¹. Há várias formas de usar esta tecnologia⁹² mas quando a mesma é combinada com outras tecnologias de segurança, como a criptografia de chave pública e a biometria, é muito eficaz para efectuar um controlo de acesso robusto através de identificação pessoal e/ou autenticação⁹³.

Há vários tipos de cartões inteligentes mas os mais interessantes em termos de segurança para concretizar a TCB são os que possuem um microprocessador embebido capaz de executar internamente algoritmos criptográficos complexos, não precisando por isso de comunicar para o exterior os segredos que emprega nesses algoritmos. O recurso a este tipo de cartões, com capacidades criptográficas nativas protegidas por segredos pessoais (*Personal Identification Numbers*, PIN), permite aumentar a segurança dos sistemas que os usam. Nomeadamente, os cartões inteligentes são ideais para concretizar sistemas de autenticação com chaves assimétricas: a chave privada é mantida num sistema de armazenamento imune à penetração, e um segundo factor de autenticação, o PIN, tem de ser fornecido para autorizar o seu uso. Para além disso, aceleradores criptográficos internos fornecem operações criptográficas realizadas por hardware, tais como a geração de pares de chaves assimétricas e a geração e validação de assinaturas digitais. No protótipo da TCB usaram-se dois tipos de cartões com estas funcionalidades: *Schlumberger (Axalto) Cryptoflex* (16 KB) e *Javacard Cyberflex Egate* (32 KB).

Os sistemas de autenticação com chaves assimétricas são mais seguros que os sistemas baseados em senhas simétricas porque não existe partilha de segredos entre os interlocutores (o autenticador e a entidade que se autentica). A chave privada é usada para calcular uma assinatura de autenticação e apenas precisa de ser conhecida por um dos intervenientes na autenticação – a entidade que se autentica. Num processo típico de autenticação com chaves assimétricas, a entidade que se autentica assina algo que lhe é fornecido pelo autenticador com a sua chave privada e o autenticador valida essa assinatura com a chave pública do interlocutor, que a conhece de antemão ou a obtém no momento. Neste último caso, deverá obter não apenas a chave públicas mas um certificado da mesma, o qual permitirá validar a sua correcção. Importa referir, a este respeito, que o novo Cartão do Cidadão que está a ser gradualmente atribuído aos cidadãos Portugueses já possui esta funcionalidade, entre diversas outras fornecidas.

⁹¹ R. Marvie, M.-C. Pellegrini, O. Potonniée, and S. Jean (2000) Value-added Services: How to Benefit from Smart Cards. In Gemplus Developer Conf. (GDC 2000), Montpelier, France.

⁹² H. Gobioff, S. Smith, J. D. Tygar, and B. Yee (1996) Smart Cards in Hostile Environments. In 2nd USENIX Works. on Electronic Commerce, Oakland, USA.

⁹³ G. Hachez, F. Koeune, and J. Quisquater (2001) Biometrics, Access Control, Smart Cards: a Not So Simple Combination. Security Focus Magazine.

No âmbito do REVS, os *Administrators* são os servidores eleitorais que validam a identidade dos votantes e que os autorizam a votar. Assim, um votante prova a sua autenticidade perante os *Administrators* assinando os pedidos que lhes são enviados usando o cartão inteligente e a chave privada nele guardada. Para realizar essa assinatura é preciso autorizá-la, introduzindo o PIN correcto. Os *Administrators* verificam a autenticidade de um votante verificando a sua assinatura num pedido com a respectiva chave pública previamente guardada nas suas bases de dados. Estas bases de dados são criadas durante a fase de registo dos votantes, durante a qual os votantes indicam a respectiva chave pública apresentando o seu cartão inteligente.

No âmbito do REVS, os dados que são enviados num pedido efectuado a um *Administrator* correspondem a um resumo obscurecido do voto expresso pelo votante. Serão estes, portanto, os dados que deverão ser assinados pelo cartão antes de os enviar aos *Administrators* para obter sobre os mesmo uma assinatura às cegas. Contudo, um cartão inteligente assina os dados que lhe são apresentados desde que seja fornecido o PIN correcto, não tem qualquer capacidade de verificar se esses dados correspondem ou não às escolhas efectuadas pelo votante. Portanto, eles, por si só, não são capazes de impedir a adulteração de votos por um Sistema do Votante malicioso onde a componente que se executa no PC foi comprometida. Este problema é evitado através do uso do dispositivo FINREAD.

Dispositivo FINREAD

Como antes se explicou, o simples uso de um cartão inteligente não impede a possibilidade de adulteração dos votos pelo Sistema do Votante. Por exemplo, o Módulo Eleitor pode ser sabotado por um atacante de forma não detectável para o votante. Tal representa um potencial risco para garantia das propriedades inerentes à democracia.

Depois de analisar várias formas alternativas de assegurar uma interacção humano-máquina no Sistema do Votante, optou-se por retirar esta interacção da parte do sistema que se executa no PC e realizá-la através de um dispositivo seguro com capacidade de interacção com humanos. Depois de analisar vários dispositivos invioláveis, optámos pelo leitor FINREAD.

Consequentemente, a nossa TCB foi desenvolvida com base no leitor de cartões *CardMan Trust FINREAD* da Omnikey⁹⁴. Este é um leitor de cartões inteligente con-

⁹⁴ K. Schmid and H. Zeithofer (2003) FINREAD Whitepaper, Rev 1.0.

forme com as normas ISO 7816 e EMV 3.1.1⁹⁵ e que também segue as especificações FIN-



FINREAD⁹⁶. A figura abaixo apresenta o dispositivo FINREAD adoptado.

Uma plataforma FINREAD adopta e estende a tecnologia de *Applets Java*; num ambiente FINREAD as Applets chamam-se Finlets. Os dispositivos FINREAD possuem uma memória interna (1MB) capaz de hospedar diferentes Finlets e uma JVM para os interpretar. Quando um Finlet é interpretado no dispositivo, este opera no modo seguro, o qual assegura que qualquer acesso ao cartão é sempre mediado pelo Finlet. Caso contrário, o dispositivo opera em modo transparente, sendo neste modo equivalente a um leitor de cartões convencional.

O dispositivo FINREAD escolhido tem uma interface humano-máquina reduzida mas suficiente para suportar uma participação numa eleição. Ele possui um pequeno ecrã LCD, com 4 linhas de 20 caracteres cada, e um teclado de 16 teclas para introdução de dados. Os Finlets em execução no dispositivo controlam tanto as interações com o cartão como as interações com o votante através do ecrã e teclado próprios. Nomeadamente, as opções de voto são apresentadas pelo terminal do dispositivo e as escolhas do

⁹⁵ ISO/IEC 7816-4 (1995) Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4 : Interindustry commands for interchange.

⁹⁶ OMNIKEY (2005) FINREAD SDK Manual, VI.22.3.

votante são indicadas através do seu teclado, assim como o PIN para autorizar certas operações do cartão.

Funcionalidade

Considerou-se que o conjunto de dois dispositivos, um cartão inteligente e um leitor FINREAD, eram suficientes para concretizar uma TCB que fornecesse os níveis de segurança necessários para o Sistema do Votante do REVS. As funcionalidades prestadas por cada componente da TCB estão elencadas na tabela seguinte.

TCB	Funcionalidades	
Cartão inteligente	Armazenamento	Chave pública do <i>Commissioner</i>
		Par de chaves assimétricas do votante
		Dados temporários de cada voto (escolhas, factores de obscurecimento)
	Cálculo	Geração de valores aleatórios (factores de obscurecimento)
		Assinaturas digitais do votante
		Cálculo de resumos dos votos
Dispositivo FINREAD	Entradas/saídas	Apresentação do boletim, opções de voto e leitura de dados para o voto
		Leitura do PIN do cartão
	Armazenamento	Chaves públicas por eleição (dos <i>Administrators</i> , da eleição)
		Assinaturas dos <i>Administrators</i> por eleição
	Cálculo	Validação dos dados recebidos dos <i>Ballot Distributors</i> (assinados pelo <i>Commissioner</i>)
		Obscurecimento e desobscurecimento de dados trocados com os <i>Administrators</i>
		Validação das assinaturas às cegas dos <i>Administrators</i>
		Produção do pacote de submissão do voto

O cartão inteligente é usado para guardar dados sensíveis, tanto dados privados como dados que são críticos para retomar o processo de votação noutra lugar ou mais tarde caso aconteça alguma falha. A chave pública do *Commissioner* faz parte dos dados sensíveis, uma vez que é o ponto de partida para a validação de todos os dados recebidos dos servidores eleitorais. A chave assimétrica do votante e os factores de obscurecimento usados nas assinaturas às cegas são tanto privados como críticos. Estes dados críticos devem ser guardados em memória não volátil, tal como a de um cartão inteligente, para

retomar o processo de votação mais tarde se alguma falha ocorrer. O facto de armazenar estes dados no cartão inteligente permite ainda que o votante use qualquer outro dispositivo FINREAD para completar a sua participação eleitoral.

Pelo contrário, o dispositivo FINREAD apenas guarda dados temporários necessários para os cálculos locais inerentes ao processo eleitoral do REVS – as chaves públicas dos servidores eleitorais e as assinaturas válidas fornecidas pelos *Administrators*. Estes dados podem sempre ser obtidos caso se tenha de recuperar de uma falha que tenha ocorrido no processo de votação.

VOTAÇÃO ELECTRÓNICA NO BRASIL: REFLEXÕES

João Ferreira Dias

Introdução

A utilização da urna electrónica no Brasil iniciou-se em 1996 (eleições municipais) nos municípios com mais de 200 mil eleitores. Em 1998, o critério de eleitorado foi alterado, alcançando todos os municípios com mais de 40.500 eleitores. Em 2000, a rede eleitoral com 353.780 urnas electrónicas cobriu a 100% os 109.780.071 eleitores distribuídos por 5559 municípios.

Trata-se a todos os títulos de um sistema de grandes dimensões e complexidade organizacional, com grandes impactos na afluência às urnas, diminuição de votos nulos por erros, transparência e rapidez de contagem, contribuindo para a credibilidade da democracia brasileira.

A utilização de números para identificar os candidatos resultou de estudos que mostraram que o analfabetismo é compatível com a identificação de números. Afinal, o alfabeto utiliza telefones públicos cujo teclado é igual ao da urna electrónica. Para confirmar ou corrigir o voto, ele poderá ainda identificar as teclas através de cores. Acresce que ao indicar o número do candidato em que pretende votar o eleitor é confrontado com a fotografia do candidato ou o símbolo do partido correspondente e só então confirma a opção de voto.

A montagem e funcionamento de todo o sistema eleitoral, desde o desenvolvimento do software e instalação das urnas electrónicas, passando pelo processo eleitoral propriamente dito e culminando na contagem e divulgação dos resultados eleitorais é da responsabilidade da Justiça Eleitoral que é encimada pelo Tribunal Supremo Eleitoral (TSE). O TSE é a cúpula dum sistema judiciário específico e arborescente. Em cada Estado existem os Tribunais Regionais Eleitorais Estaduais (TRE) e diversas Juntas Eleitorais (JE), que integram os representantes dos partidos políticos.

A lei 9504/1997 de 30/9 (actualizada em 07/02/2002), estabelece as normas para as eleições.

Montagem do sistema eleitoral

O TSE tem aberto concursos únicos para o desenvolvimento de software e contratação de serviços técnicos para sua instalação nas urnas eleitorais. Pretende com isso assegurar uma maior eficácia e segurança limitando o número de intervenientes no processo técnico.

As especificações do software seguem o núcleo criado em 1996 e que vem sendo aperfeiçoado. O desenvolvimento é acompanhado pelo TSE (a parte final é efectuada nas suas instalações), cujos peritos têm de aprovar a versão provisória. O código fonte dessa versão provisória é apresentado aos partidos, ao Ministério Público e à Ordem dos Advogados para auditoria e avaliação e fica à disposição destes por 50 horas, 60 dias antes das eleições. Face às recomendações são efectuadas alterações, num processo iterativo que decorre nas instalações do TSE.

Após todos concordarem que o código fonte está correcto, gera-se o código objecto, com incorporação de rotinas adicionais. Essas rotinas destinam-se a garantir que se houver qualquer alteração na assinatura digital do código objecto a urna deixa de funcionar. O código objecto é cifrado no TSE, com os algoritmos MD5 e ASSINA (da Microbase) em máquina segura do TSE.

O código fonte e o código objecto são gravados em CD, lacrados⁹⁷ e assinados por todos os participantes (TSE e partidos), e guardados em cofre do TSE. São efectuadas gravações em CD do código objecto, que são distribuídas aos TRE. Todas as urnas executarão esse mesmo software de votação.

Nos TRE o software “gerador de Mídia” agrega em cartões de memória (*flash-cards*) o código objecto e os ficheiros de dados de cada urna electrónica. São gerados o cartão de memória de instalação (tabelas de partidos e candidatos concorrentes) e o cartão de memória da votação (tabelas de eleitores e secções) que, junto com a disquete em que são gravados os votos totalizados, são introduzidos na urna electrónica em dia e horário previamente designados pelos juízes eleitorais.

As urnas electrónicas são preparadas (inseminadas, segundo a terminologia própria) com cerca de uma semana de antecedência. Nessa ocasião, todas as informações constantes no meio de armazenamento interno são apagadas e são carregadas as seguintes informações através dos *flash-cards* previamente preparados: uma cópia do sistema de exploração na versão para a eleição; o software das eleições; tabelas de candidatos; municípios, zonas e dados dos eleitores de cada secção. Todas as informações carregadas na urna são identificadas pelas respectivas assinaturas digitais, garantindo a Integridade do Sistema e a Invulnerabilidade. O conjunto formado por todas as informações gravadas recebe também uma assinatura digital para assegurar a integridade deste conjunto. É também inicializado o registo de todas as ocorrências na urna (físico e lógico).

⁹⁷ RES 22.039/2005 de 4/8 - Sobre a fiscalização, auditoria, assinatura digital e lacração dos programas-fonte e programas-executáveis.

Após o encerramento da instalação, a urna recebe lacre físico em todos os dispositivos e portas de acesso, que evidencia que é Fisicamente Seguro e facilita a Detectabilidade de violações. Todos estes procedimentos podem ser acompanhados por fiscais e delegados dos partidos, sendo ainda cada urna lacrada e assinada por um representante do Ministério Público Eleitoral e pelo Juiz Eleitoral. Aos fiscais e delegados de partidos e coligações é garantida alguma fiscalização desse processo, sendo admitida a conferência por amostragem, em até 3% das máquinas⁹⁸.

A urna inseminada só realizará todas as operações no dia e hora pré-determinados. Caso seja ligada antes do dia da eleição, será apresentado um ecrã solicitando aguardar o dia e hora do início da eleição. Em caso de segunda volta ou repetição, não há nova inseminação mas apenas actualização das tabelas via cartões de memória, com reposição de lacre.

Os TRE e as Juntas Eleitorais credenciam as pessoas que operam o sistema e que recebem do TSE chaves de acesso pessoais e intransferíveis. As eventuais intervenções de manutenção técnica da urna eleitoral já inseminada requerem a aprovação e a presença do juiz eleitoral e a presença dos representantes dos partidos nas juntas eleitorais. O sistema de exploração tem mecanismos de segurança que relacionam os intervenientes com as operações realizadas.

A interface com o operador faz-se sempre através do subsistema de instalação e segurança (SIS). O SIS é um software, desenvolvido pela empresa Módulo, que interage com o sistema de exploração e permite uniformizar, assistir e controlar os acessos ao sistema, a instalação do software e dados, etc.

Arquitectura do sistema

A votação faz-se nas urnas electrónicas, que são micro-computadores dedicados. A concepção da urna foi efectuada por técnicos do Instituto Nacional de Pesquisas Espaciais (INPE) de São José dos Campos, da Aeronáutica e do Ministério do Exército, em conjunto com o TSE. As urnas utilizadas em 2000 foram produzidas pela Procomp, empresa nacional vencedora de licitação promovida pelo TSE. A empresa também foi responsável pela actualização em 1998 das urnas utilizadas em 1996, que foram produzidas pela Unisys.

A arquitectura da urna é similar à de um computador pessoal normal, mas sem disco rígido e com uma extensão da BIOS (*Basic Input/Output System*) com funções de segurança. O sistema de exploração multi-tarefa é o VirtuOS. A urna electrónica compreende os seguintes equipamentos: terminal do eleitor (urna propriamente dita); micro-terminal

⁹⁸ RES 20.563/2000.

para uso da mesa de voto (mais dois terminais de leitor apenas com as funções de teclado e ecrã).

A urna funciona ligada à rede de energia eléctrica (110 ou 220 Volts, sem necessidade de ajuste) e, na falta desta, possui uma bateria interna com capacidade de funcionamento para 12 horas no modelo 2000 e menos para os modelos anteriores. A urna também pode ser ligada a uma bateria de automóvel.

O micro-terminal é posicionado na mesa de voto no lugar do presidente, sendo constituído por um teclado numérico 0 a 9, teclas “CONFIRMA” e “CORRIGE”, visor de cristal líquido e luzes de sinalização que, quando acesas indicam: vermelho, a urna electrónica está a ser alimentada através de bateria interna ou externa; amarelo, a urna electrónica está a ser utilizada por um eleitor; verde, a urna está autorizada para a identificação e votação do próximo eleitor.

É no micro-terminal que o presidente da mesa de voto digita o número do eleitor e, confirmada a sua identidade, o autoriza a votar. É nele também que digitará a senha de encerramento da votação.

A urna (terminal do eleitor) compreende: um visor e um teclado similar ao de um telefone; uma impressora; um gravador de disquetes; um *flash-card* externo; um *flash-card* interno e portas USB.

Em cada tecla da urna está gravado o respectivo número em código internacional braile. O deficiente visual que não lê braile pode votar guiando-se pelo número 5, central, ressaltado no teclado através de uma pequena barra, logo abaixo do número, na própria tecla. As urnas electrónicas mais recentes (modelo 2000) já possuem um sistema de som, que permite ao deficiente visual a verificação e confirmação do voto.

O software da urna regista a identidade do votante e a votação mas não os relaciona (não há registo e há reutilização da área de memória RAM). Nas eleições de 2002, efectuaram-se em diversas secções os testes à impressão de recibos de votação, que funcionam como justificativo eleitoral (no Brasil o voto é obrigatório). Para quem está fora do seu domicílio eleitoral no dia da eleição, basta apresentar o Requerimento de Justificativa Eleitoral em qualquer local de votação (no mesmo horário da votação) e a ausência é justificada, na própria urna electrónica.

Os dados da votação presentes na urna são listados e registados sob cifra em disquetes. As disquetes são lidas no Transportador, software específico que está instalado num computador localizado no edifício da secção eleitoral e à guarda de um juiz eleitoral. O Transportador funciona numa plataforma clássica (do tipo Windows NT) e trata da leitura, cópia e cifra dos dados constantes nas disquetes gravadas pelas urnas electrónicas.

O Transportador transmite electronicamente, através da rede informática privada da Justiça Eleitoral, os dados cifrados das disquetes das urnas para os Totalizadores nos TRE, e

destes para o TSE. Os computadores que fazem a transmissão dos dados para o TRE estão programados para aceitar apenas a cifra utilizada nas urnas e só executam operações de leitura e transmissão. Se houver qualquer alteração nos dados da disquete, o Transportador não a aceitará.

Nos TRE, os dados são recebidos, decifrados e validados quanto à origem da secção emite e à integridade dos dados. Em seguida os resultados são agregados e registados numa base de dados para posterior divulgação e envio ao Transportador do TSE. Os partidos políticos podem realizar testes de Integridade do Sistema comparando os dados de cada secção disponíveis de forma impressa e em meio magnético.

A rede informática do TSE é uma rede WAN da Embratel. Durante o período de votação está fisicamente isolada, sem ligação com o exterior e sob intensa fiscalização e vigilância.

Processo de votação

As urnas são ligadas às 7h30 do dia da eleição. O pessoal da mesa eleitoral (mesários) compreende 6 convocados pelo TRE, dos quais um é o presidente da mesa. Após recepção, verificação de lacres e instalação do material é ligado o computador à electricidade (mas desligado de qualquer rede informática). Durante a inicialização são executados testes dos componentes básicos e verificada a consistência de todas as informações contidas na urna. O ecrã indicando a possibilidade de se iniciar a eleição é apresentado somente quando todos os testes indicam o seu perfeito funcionamento e as verificações confirmam a integridade da informação.

Em seguida o presidente da mesa emite a “zerésima” de cada urna. A “zerésima” é um documento impresso pela urna contendo a relação de todos os concorrentes eleitorais e provando que não há qualquer voto registado naquela urna.

A autorização para os eleitores votarem faz-se por identificação física face à lista dos eleitores. Uma vez autorizado pela mesa, o eleitor assina ou imprime a sua impressão digital na folha de votação e encaminha-se para a urna electrónica. Entretanto, o presidente da mesa digita o número do título do eleitor no micro-terminal, assim autorizando o eleitor a votar.

Para votar⁹⁹, o eleitor marca o número do candidato preferido. No ecrã, aparecem a foto, o número, nome e sigla do partido do candidato. Para votar em branco, aperta a tecla BRANCO. Para votar nulo, marca um número inexistente. Para confirmar a opção,

⁹⁹ Um simulador da urna electrónica está disponível em http://www.tse.gov.br/eleicoes/urna_eletronica/simulacao_votacao/UrnaApplet2.htm.

aperta a tecla verde CONFIRMA. Se quiser corrigir, aperta a tecla vermelha CORRIGE e repete o procedimento.

Uma vez terminada a votação a urna bloqueia, emitindo um rápido sinal sonoro e acendendo uma luz verde no micro-terminal. A mesa desbloqueia-a ao inserir a identificação de novo eleitor no micro-terminal.

Encerrada a votação, o presidente da mesa digita no micro-terminal a senha de encerramento da votação. Quando a senha de encerramento é confirmada, o terminal do eleitor imprime, automaticamente, uma primeira via do Boletim de Urna. Cada Boletim de Urna consigna a data da eleição, a identificação do município, da zona eleitoral e da secção eleitoral, o horário de encerramento da votação, o código de identificação da urna electrónica, o número de eleitores aptos, o número de votantes, os votos nominais para os cargos daquela eleição, os votos de legenda, os brancos e os nulos e a soma geral dos votos. Se a impressão estiver correcta, o presidente da mesa aperta a tecla CONFIRMA no terminal do eleitor para emissão de até 10 vias do Boletim de Urna. Todos os Boletins de Urna são rubricados pela mesa. Uma via do Boletim de Urna é afixada na entrada da secção eleitoral e as cópias são entregues aos representantes dos partidos.

Após as impressões dos Boletins de Urna, o presidente da mesa destrói o lacre do gravador de disquetes (todos os outros devem permanecer até trânsito em julgado da eleição) e grava em disquete os dados cifrados das tabelas, eleitores, e histórico de eventos. Em seguida repõe o lacre no leitor de disquetes e prepara a urna para ser recolhida. Essa disquete, devidamente identificada, acompanhada dos documentos da votação (caderno de folhas de votação, acta da eleição e três vias do Boletim de Urna), é encaminhada para a Junta Eleitoral local que, atestando a validade da votação, autoriza a transmissão dos dados do Transportador para o TRE. Esta transmissão de dados para o TRE é autorizada através de códigos aos quais somente o Juiz Eleitoral tem acesso e de contra-senhas fornecidas por um pequeno aparelho, que permanece em poder do Juiz. Essas contra-senhas mudam aleatoriamente a cada transmissão. Somente no computador do TRE os dados são decifrados e os votos totalizados. Se houver alguma interferência nas linhas de comunicação, o computador rejeita aquele Boletim de Urna.

Em caso de avaria no dia da votação utiliza-se uma urna sobressalente com transferência, fiscalizada pela mesa, da disquete e do cartão de memória. Em caso de avaria de todas as urnas sobressalentes, a votação faz-se pelo sistema tradicional em papel e urna (de lona). A apuração das urnas das secções eleitorais que passam à votação tradicional em papel tem de estar concluída no prazo máximo de até 5 dias, no primeiro turno, e de até 10 dias, no segundo turno eleitoral.

Em cada Estado Federal procede-se a uma votação paralela. No dia anterior ao da votação, cada TRE com a presença dos partidos selecciona aleatoriamente e recolhe duas urnas já instaladas nas secções eleitorais e que são substituídas. A seguir, com a presença dos partidos, procede-se a uma votação simulada de 500 boletins que ficam lacrados

numa urna simples (urna de lona). No dia da votação, a urna de lona é aberta e os votos são introduzidos nas duas urnas electrónicas. Os resultados devem ser iguais entre si e à da urna de lona.

Resultados de auditorias

Foram efectuadas diversas auditorias ao sistema, entre as quais a da UNICAMP¹⁰⁰ que concluiu:

“O Sistema eletrônico de votação implantado no Brasil a partir de 1996 é um sistema robusto, seguro e confiável atendendo todos os requisitos do sistema eleitoral brasileiro.

... conclui-se que o sistema eletrônico de votação atende às exigências fundamentais do processo eleitoral, ou seja, o respeito à expressão do voto do eleitor e a garantia do seu sigilo. Conclui-se também que a segurança e a confiabilidade do sistema podem ser aprimoradas.”

As recomendações da UNICAMP referem:

- Desenvolvimento dos programas de votação baseados em blocos estáveis e permanentes;
- Formalização do ciclo de desenvolvimento de software;
- Avaliação do código fonte (também) por especialistas independentes do TSE;
- Compilação e determinação de resumos criptográficos em sessão pública;
- Verificação pelos partidos dos resumos criptográficos instalados nas urnas inseminadas;
- Revisão do procedimento de preparação da urna para a segunda volta;
- Impressão do Boletim de Urna antes da cifra e gravação dos resultados em disquete;
- Substituição da cifra dos Boletins de Urna por assinaturas digitais;
- Colocação de mais lacres e a sua manutenção até 60 dias após o trânsito em julgado da eleição;
- A proibição de intervenções de manutenção de urnas no dia da eleição;
- A substituição de urnas só poder ser feita até às 17 horas do dia da votação.

¹⁰⁰ UNICAMP (2002). Avaliação do sistema informatizado de eleições.

De entre diversas outras auditorias merece relevo a que foi realizada em 2001 pelos peritos Evandro Luiz de Oliveira e Cláudio Andrade Rego, no município de S. Domingos no Estado de Goiás. Depois de terem assinalado diversas deficiências procedimentais, por vezes por incúria e desleixo, esses peritos apresentam algumas sugestões, de entre as quais:

- Adopção de mecanismos de impressão do voto, o qual pudesse ser observado pelo eleitor, sem qualquer contacto manual, propiciando a possibilidade de recontagem ou auditoria do processo de votação;
- Adopção de mecanismos de assinatura digital que possam ser verificados pelos representantes dos partidos, para que se garanta, numa possível auditoria, a origem e fidelidade dos programas e dados inseridos em cada uma das mais de 300 mil urnas do país;
- Adopção, em carácter obrigatório, de programas considerados como “software aberto” nos processos eleitorais, fazendo com que não exista a possibilidade de programas deixarem de ser verificados e auditados.

Reflexões

O sistema parece-nos atractivo, robusto, seguro e Confiável.

O sistema permitiu reduzir os votos nulos por erro na expressão do voto, a lentidão da contagem e a necessidade de acompanhamento dos deficientes visuais.

A Não-Coercibilidade é dada pela votação presencial, com presença de representantes dos partidos e sob controlo jurisdicional.

O Anonimato do voto, isto é a inexistência por qualquer forma da relação entre o votante e o seu voto, é garantido por diversas medidas, desde o escrutínio pelo TSE e pelos partidos do software eleitoral (que reutiliza a memória RAM) até ao controlo das intervenções de manutenção.

A Integridade dos Votos é garantida pelo escrutínio pelo TSE e pelos partidos do software eleitoral, pelo controlo das intervenções de manutenção (sendo pertinente a recomendação da Unicamp de impedir a manutenção no dia da eleição), a cifra dos dados e a sua transmissão numa rede privada, e a possibilidade de controlo a posteriori dos resultados por secção através dos Boletins de Urna, dos registos das disquetes e das bases de dados dos TRE e do TSE.

O sistema com facilidade poderá evoluir para uma interligação por rede informática desde que se garantam os requisitos acrescidos de segurança.

EXPERIÊNCIAS EUROPEIAS

João Ferreira Dias e Domingos Magalhães

A panorâmica que se segue é tributária das comunicações efectuadas na reunião do Conselho da Europa (COE) em Estrasburgo em 23-24/11/2006¹⁰¹.

Suíça

Mais de 80% dos eleitores recorre ao voto antecipado nas estações do correio, apenas 20% do eleitorado se apresenta nas assembleias de voto. Daí que o voto electrónico só terá interesse através da modalidade “à distância”, leia-se através da Internet, esperando-se que venha a substituir o voto postal.

Neste momento está concluída a fase de testes piloto em três cantões, prevendo-se no futuro o debate no Parlamento sobre o processo.

Para não introduzir discriminação relativamente aos residentes no estrangeiro, antes da extensão a estes, vai ser constituída uma base de dados nacional, agregando os registos respeitantes a cada cantão de origem. As medidas de segurança aplicadas ao voto postal foram transpostas para o voto electrónico, acrescidas do pedido da data de nascimento e o local de naturalidade. Entendem que para voto electrónico remoto não faz sentido o recibo em papel.

A Suíça segue de forma rigorosa a Rec(2004)11 do COE, sentindo como necessária a existência de mecanismos de certificação do voto.

Embora não haja movimentos ou correntes de opinião militantes contra a utilização do voto electrónico, a Suíça optou por uma estratégia “passo a passo”, de modo a construir aceitação e confiança duradouras. Foram recebidas, no entanto, numerosas críticas construtivas e pedidos de esclarecimento em contactos dos cidadãos com a administração cantonal.

As autoridades suíças esperam apenas um crescimento modesto da percentagem de votantes pela utilização do voto electrónico (aparentemente, aqueles que já utilizaram o voto electrónico mantiveram-se fieis ao canal nas eleições seguintes).

Estónia

¹⁰¹ <http://www.coe.int/democracy>.

A Estónia dispõe de bases de dados de eleitores e Bilhete de Identificação electrónico (processo iniciado há nove anos, tendo sido emitido em 2002 o primeiro e- "id_card"; actualmente a taxa de cobertura é na ordem dos 70% com assinatura digital).

Nas eleições de 2005, 80% dos eleitores podiam já votar pela Internet. No entanto, este canal foi apenas utilizado por 1% dos votantes. Um dos constrangimento foi a não utilização de diversos idiomas, uma vez que os 30% de falantes do russo não compreendiam as instruções em Estónio.

Os eleitores necessitaram de um leitor de cartões inteligentes e de descarregar software específico (*driver*) do sítio electrónico dos serviços de identificação. Os eleitores podiam votar sucessivamente pela Internet e ainda, no dia da eleição, presencialmente na Assembleia de voto.

Este procedimento de voto reversível, já existente em processos presenciais de diversos países nórdicos, funciona como garantia da liberdade das eleições. No entanto, apenas 30 votantes dos 9700 que exerceram o direito de voto pela Internet recorreram ao voto reversível.

O relatório do COE sobre a votação de 2005 está disponível na Internet¹⁰².

França

A França aplicou o voto electrónico aos residentes no estrangeiro, na eleição parcial de Junho de 2006, da Assemblée des Français à l'Etranger (AFE), mediante legislação de 2006¹⁰³.

O processo teve as fases seguintes:

- Pré-inscrição, em Abril-Maio 2006, específica para os que pretendiam votar pela Internet. Receberam uma carta da embaixada;
- Envio dos documentos e normas de compatibilidade dos equipamentos;
- Votação (não foi permitido repetir o voto como no caso da Estónia).

Em números aproximados, ter-se-ia cerca de 600 mil expatriados e destes 26 mil manifestaram interesse em votar pela Internet, tendo efectivamente votado 10 mil. O total de votantes, em todos os canais, terá sido cerca de 75 mil (valores semelhantes aos da eleição anterior em que não havia o canal Internet). Estes números mostram que será preciso melhorar a facilidade do processo se se pretender melhorar a participação com a uti-

¹⁰² www.coe.int/democracy.

¹⁰³ <http://www.assemblee-afe.fr>.

lização da Internet. O centro de atendimento de chamadas recebeu 17 mil pedidos de apoio - problemas de vírus, de *browser*, etc.

O processo correu sem falhas técnicas (os ataques foram facilmente repelidos e tinham a ver com tentativas de modificar o voto, ligação múltipla e intrusão repetida). Mostrou-se pesado para os eleitores (normas CNIL sobre anonimato e segredo do voto). Finalmente, teve um impacto fraco quanto ao número de votantes. Parece não ter evidenciado capacidade em atrair novos votantes (os que votaram através da Internet, eram elementos muito activos na eleição e, por isso, votariam de qualquer maneira). No entanto, poderá ter contribuído para estabilizar a percentagem de votantes. O projecto teve um custo elevado (total estimado de cerca de 2 milhões de euros), tendo sido escrupulosamente observadas as normas de contratação (concurso público).

Quanto à Rec(2004)II, mostraram-se de difícil operacionalização os pontos 12 (manipulação/pressão exterior) e 18 (verificação da transparência do processo). Os partidos representados na AFE podiam indicar especialistas informáticos. Foram expressas algumas reservas que não incidiram sobre o funcionamento do sistema.

Não estão previstos desenvolvimentos de voto electrónico para eleições políticas em França, sejam nacionais ou locais.

Suécia

O voto electrónico não tem assumido prioridade, entendendo a Suécia que não há ainda suficiente experiência e garantias de segurança para a adopção generalizada do processo. Também se receia a discriminação social (*digital divide*).

A Internet é usada localmente para apoio a consultas populares mas a votação decorre de forma tradicional, nas assembleias de voto.

Por outro lado, as elevadas percentagens de votantes e normas de voto sofisticadas, possibilidades de voto antecipado e mobilidade, proporcionando satisfação aos eleitores, desencorajam a aplicação do voto electrónico.

No entanto, há expectativas de que o futuro governo quererá testar novas ideias, é diferente do anterior e a questão poderá assumir uma natureza “ideológica”.

Holanda

A Holanda era um dos países mais avançados na utilização do voto electrónico. No entanto o problema recentemente havido com a utilização das máquinas de voto constituiu um duro golpe.

Desde há 30 anos, a Holanda vinha utilizando de modo generalizado máquinas de votar. Note-se que nas últimas eleições, apenas 10 municípios de pequena dimensão, em 487, recorreram a boletins de voto em papel.

A iniciativa da utilização de máquinas de votar pertenceu aos municípios, por razões diversas - poupança de papel, maior rapidez, influência dos computadores em ambiente de escritório, moda. A generalidade dos municípios utiliza máquinas alugadas ao fornecedor NEDAP, que fora dos períodos de votação as armazena em locais sob a sua responsabilidade. Amsterdão utilizou máquinas do fornecedor SDU.

Em Setembro de 2006, um grupo anti-máquinas de votar (“we don't trust voting computers” ou “wijvertrouwenstemcomputersniet”) conseguiu ter em sua posse diversas máquinas e mostrou num programa televisivo de grande audiência que aquelas são vulneráveis e podiam ser quebradas (*backing*). O problema tinha sobretudo a ver com a radiação emitida através dos ecrãs, que associada ao facto de a lei holandesa determinar que o anúncio de quem vota seja feito dentro e fora da assembleia de voto, permitia a uma distância de 15-20 metros captar o sentido de voto de quem votava.

O Ministério teve conhecimento das vulnerabilidades dos equipamentos SDU e, em 25/10/2006, foi forçado a retirar a autorização de utilização previamente concedida. Como as eleições eram em Novembro, apesar do recurso a máquinas cedidas por entidades alemãs, alguns municípios (22), incluindo Amsterdão, tiveram de voltar aos boletins em papel.

O novo processo de verificação e testes evidenciou por outro lado que as normas em vigor datavam já de 1997. Foi por isso criada uma comissão com uma forte componente técnica com vista a indicar o que fazer neste domínio.

Note-se que foram justamente máquinas deste fornecedor holandês (SDU) que a Irlanda comprou e que acabou por encaixotar de novo em resultado da intervenção de comunidades de activistas contra o uso de tecnologias electrónicas nos processos eleitorais.

Os inquéritos de opinião mostraram, no entanto, que a população holandesa continua a aceitar as máquinas de votar mesmo depois das vicissitudes apontadas.

O processo de votação no estrangeiro não foi afectado. O sistema utilizado em 2006 é diferente do de 2004 (Europeias em que votaram 4871 eleitores em cerca de 16.000 registados para votar pela Internet). Refira-se que o sistema foi concebido pela Autoridade de Gestão da Água (*RIES System*) e premiado pelas Nações Unidas em 2006.

Reino Unido

As próximas experiências com voto electrónico irão decorrer por iniciativa das autarquias locais, em eleições locais, nas eleições da área da “Grande Londres” e, eventualmente, nas eleições dos Parlamentos Regionais, do Parlamento Europeu, mas não em eleições nacionais.

A atenção está agora na utilização de códigos de barras, na verificação de assinaturas, na facilitação do acesso pelos eleitores, no aumento da eficiência administrativa (contagem de votos), na descentralização do voto (do tipo “em qualquer lugar”), na utilização de outros locais para assembleias de voto, diferentes dos tradicionais, como estações de transportes, centros comerciais, etc.

Há um grande enfoque nas questões de segurança (“perceptions first”). A expansão virá depois quando houver suficiente apoio político.

Noruega

A Noruega pretende introduzir o voto electrónico em ambiente remoto, mas não acha que seja possível, para já, arrancar em larga escala. Assim, deverá continuar a fase de avaliação e testes.

O país dispõe actualmente de contagem por leitura óptica e por isso a modalidade de voto electrónico na assembleia de voto parece desnecessária, uma vez que não se obtém maior rapidez no apuramento dos resultados.

A Noruega tenciona efectuar testes de voto electrónico em ambiente controlado, nas escolas secundárias, antes das eleições autárquicas (são muito populares porque em geral os resultados antecipam os das eleições reais).

O planeamento apontava para a introdução do voto electrónico em 2007. O relatório, em inglês, está disponível na Internet¹⁰⁴. Para fazer testes piloto não se torna necessário alterar a lei eleitoral. Só o será quando se passar à larga escala, cobrindo todo o país.

Nessa altura a Noruega admite a possibilidade de passar a adoptar a regra do voto sequencial.

Finlândia

Em 2004, o Ministro da Justiça, que tutela os serviços eleitorais, ordenou a aceleração dos trabalhos para a utilização generalizada do voto electrónico remoto, baseado na Internet e não em máquinas de voto dedicadas. No entanto, o voto electrónico apenas seria possível em locais controlados para o efeito. As razões apontadas eram: custo ele-

¹⁰⁴ <http://www.e-valg.dep.no>.

vado do voto antecipado, que é utilizado por cerca de 40% dos eleitores, facilidade e rapidez na contagem dos votos e divulgação dos resultados.

O projecto de lei entretanto elaborado, seguiu de perto a Rec(2004)11 do COE excepto para o voto em branco, que só seria possível com voto de papel. Foi seleccionada a empresa espanhola Sycti de Barcelona e decidida a utilização do voto electrónico em alguns municípios já nas eleições parlamentares de 2007. Não foi incluída a confirmação em papel.

No entanto, o Parlamento alterou o projecto e determinou que: o voto electrónico teria de contemplar a opção “voto em branco”; seria o Parlamento e não o Ministro da Justiça a decidir a expansão do voto electrónico; e que o teste piloto fosse adiado para 2008 nas eleições locais, em 3 municípios.

Assim a expansão só terá efeitos, eventualmente, em 2011 (eleição do Parlamento) porque não haverá tempo para alterar a lei para a eleição Europeia de 2009. As secções de voto estarão ligadas em rede ao registo central de eleitores e estarão também abertas no dia da eleição. A médio e longo prazo a expectativa será acabar com o boletim de voto em papel.

A Finlândia não considera reunidas as condições de segurança e outras para introduzir o voto electrónico remoto em qualquer lugar.

Alemanha

A Alemanha tem utilizado máquinas de votar. É preocupante saber que diversas verificações evidenciaram desvios entre os resultados fornecidos por máquinas de registo directo do voto e leitores ópticos e as recontagens manuais.

O conseqüente défice de confiança alimenta uma forte corrente de opinião que pretende abolir a utilização de máquinas de votação electrónica (petição no Parlamento com mais de 40 mil assinaturas).

Lituânia

A Lituânia apresentou uma abordagem inovadora ao voto electrónico por recorrer aos cartões bancários utilizados para operações na Internet (existem cerca de 600 mil clientes bancários com *idBank card* e que por isso dispõem de leitores de cartões).

Está previsto um teste piloto em data próxima mas não definida.

Áustria

Os cidadãos não são obrigados a dispor de Bilhete de Identidade, pelo que a utilização de cartões inteligentes abrange uma fracção relativamente reduzida da população.

Os cartões inteligentes, no entanto, respeitam a norma fixada pelo governo para a utilização em governo electrónico. Daí que os testes já efectuados tenham sido em eleições não políticas.

Síntese dos resultados das experiências europeias

Tendo em conta as diversas experiências podem-se retirar as seguintes ilações:

- A Recomendação (2004)II de 30/9 do COE tem-se revelado uma referência muito útil, quer ao desenvolvimento, quer à auditoria, de sistemas de votação electrónica;
- Existem contudo diversos riscos no voto electrónico, mesmo que presencial, tais como: riscos de viciação, e ou, manipulação do software; riscos de desvirtuação do voto, ainda que não intencionais e decorrentes de erros na concepção, definição e operação dos sistemas; riscos de intromissão na comunicação da informação;
- No voto electrónico remoto aos riscos anteriores acrescem outros riscos, tais como: manipulação propagandística nos mesmos meios electrónicos que são utilizados no exercício do direito de voto; risco de coercibilidade no momento de voto; risco de quebra de confidencialidade; risco de má utilização, distanciamento ou exclusão decorrente da iliteracia informática;
- No entanto e embora seja impossível garantir 100% de segurança, o voto electrónico presencial e o voto electrónico remoto têm-se revelado confiáveis e com vantagens de comodidade, custo e rapidez;
- O período de votação deve ser alargado e, se for não presencial, deve repartir-se em dois períodos sequenciais: primeiro de votação electrónica remota não presencial; depois de votação presencial;
- O princípio de liberdade de opção de voto no voto remoto parece poder ser garantido pela regra do voto reversível (voto sucessivo), incluindo o voto presencial num período posterior à votação electrónica;
- Nos países com diversidade linguística o sistema deve ser multilingue;
- Podem retirar-se ensinamentos do voto electrónico para tornar os processos tradicionais mais amigáveis e seguros;
- É necessário reforçar a investigação substantiva e continuada sobre este tema.

EXPERIÊNCIAS PORTUGUESAS DE 2004 E 2005

João Ferreira Dias e Domingos Magalhães

As primeiras experiências de voto electrónico presencial e não vinculativo foram efectuadas pelo então STAPE nas eleições para as autarquias locais, em 1997 (freguesia de São Sebastião da Pedreira, Lisboa) e 2001, nas assembleias de voto de Baião e Sobral de Monte Agraço¹⁰⁵.

Posteriormente, nas Eleições para o Parlamento Europeu (eleições europeias de 13/6/2004), realizou-se nova experiência de voto electrónico presencial e não vinculativo. Foram elaborados quatro Relatórios de Auditoria da referida experiência¹⁰⁶.

Nas Eleições para a Assembleia da República (eleições legislativas de 20/2/2005) foram feitas experiências de voto electrónico não vinculativo, abrangendo a opção presencial e não presencial (esta só para os cidadãos residentes no estrangeiro). A experiência foi objecto de um Relatório de Auditoria¹⁰⁷.

Nestes últimos testes foi explícita a intenção de vir a utilizar o voto electrónico não presencial como uma tentativa de encontrar uma forma alternativa ao voto por correspondência, já permitido para os eleitores inscritos nos círculos internacionais da Europa e de fora da Europa, que permitisse aumentar a participação nos actos eleitorais, dada a dispersão geográfica.

Entre os objectivos associados ao voto electrónico não presencial, este piloto pretendia:

- Simplificar o processo eleitoral dos eleitores portugueses recenseados no estrangeiro (desburocratizar e tornar o processo mais célere);
- Utilizar as tecnologias em serviços prestados a cidadãos portugueses recenseados no estrangeiro;
- Dar visibilidade, motivar e fortalecer relações com uma comunidade tendencialmente esquecida pela administração pública portuguesa;
- Facilitar a vida ao cidadão português recenseado no estrangeiro;
- Facilitar e incentivar o exercício do direito de voto do cidadão português recenseado no estrangeiro e a sua participação na democracia nacional;

¹⁰⁵ www.stape.pt/eleiref/ensaio.htm.

¹⁰⁶ www.votoelectronico.pt.

¹⁰⁷ Idem.

- Desenvolver plataformas de democracia electrónica com vista a uma futura generalização;
- Aferir/testar a adesão a esta nova forma de exercer o direito de voto;
- Estudar a capacidade e a usabilidade deste tipo de sistema.

Pela sua importância, vale a pena transcrever a deliberação “A privacidade dos eleitores no voto electrónico,” aprovada na sessão de 14 /11/2005 da Comissão Nacional de Protecção de Dados (CNPd), relativa às autorizações concedidas para a realização dos testes de votação electrónica presencial de 2004 e presencial e não presencial de 2005.

Depois de referir a legitimidade da autorização concedida ao abrigo do disposto no art.º 30º da Lei 67/98 de 26/10 (LPD-Lei da Protecção de Dados Pessoais), pela CNPD à UMIC para proceder ao tratamento de dados pessoais dos eleitores para efeitos de experiências não vinculativas de votação electrónica presencial e não presencial – nome e número de eleitor, no primeiro caso, e nome, morada e número de eleitor dos cidadãos eleitores residentes no estrangeiro para efeitos da experiência de voto electrónico não presencial, no segundo, a CNPD refere que:

a) para a Experiência de voto electrónico presencial nas eleições europeias de 13 de Junho, exigiu que:

“[...] os dados pessoais fossem conservados pelo prazo máximo de 60 minutos após o encerramento das urnas de voto

[...] a comunicação dos dados pessoais da BDRE – Base de Dados de Recenseamento Eleitoral – pelas Comissões de Recenseamento à UMIC por meio digital (disquete ou cd-rom) fosse encriptada [cifrada] por palavra-passe, para segurança da comunicação dos dados

que essa comunicação acontecesse imediatamente antes da abertura das urnas, procedendo-se à imediata transferência dos dados do suporte digital para o disco dos computadores do processo da votação electrónica

que imediatamente após a introdução dos dados no sistema o suporte digital (disquete ou cd-rom) fosse destruído

fosse feita a monitorização de cópia dos ficheiros com cópia do log para disquete, assinada digitalmente, seguida de formatação dos computadores instalados nas Comissões Recensadoras das freguesias seleccionadas, com observância dos procedimentos que impedissem recuperação dos dados formatados

fossem encriptados [cifrados] os ficheiros temporários entretanto criados e utilizados, desde a instalação dos computadores até à eliminação dos dados e finalização do tratamento

fossem observadas, no quadro do sistema operativo dos computadores utilizados, as mais elementares regras de segurança informática, ou seja, password [palavra chave] de acesso, password de protecção da tela e protecção de BIOS; não ficasse registada a hora do exercício do voto electrónico, bem como a escolha tomada pelo eleitor, a par do registo da hora de apresentação do eleitor junto da mesa de voto, para descarga no caderno eleitoral, pois esses registos permitiam, na óptica da CNPD, com elevado grau de probabilidade e de certeza, conhecer o sentido de voto dos eleitores, o que violava o disposto no art.º.2º, nas alíneas a) e c) do art.º.5º e n.º.1 e 2 do art.º.7º (uma vez que não existia lei nem consentimento dos titulares)

A CNPD fez impender sobre a UMIC o ónus de demonstrar cabalmente que seriam tomadas todas as cautelas e medidas técnicas suficientes para impedir que tal acontecesse. A Autorização concedida pela CNPD ficou dependente da condição dessa demonstração”.

b) para a experiência de voto electrónico presencial nas eleições legislativas de 2005, o pedido de autorização não trouxe qualquer aspecto que o distinguisse do pedido feito para a experiência de 2004, pelo que também a autorização da CNPD a esse pedido não conteve qualquer diferença face àquela que se descreveu na alínea anterior.

c) para a experiência de voto electrónico não presencial nas eleições legislativas de 2005, o pedido de autorização de comunicação de dados pessoais da BDRE à UMIC revestiu algumas especificidades, desde logo porque essa comunicação incluiu o dado pessoal morada dos eleitores residentes e eleitores fora do território nacional. Para a CNPD, distinguiram-se três momentos. Primeiro, a comunicação de dados pelo STAPE; segundo, o processo de atribuição de nomes e chaves de utilizador, bem como o envio de mensagens de correio; por fim, o exercício do voto.

Quanto ao primeiro aspecto (comunicação de dados pelo STAPE), foi necessário aferir, face à Lei do Recenseamento Eleitoral (LRE) conjugada com a Lei de Protecção de Dados (LPD), se se encontravam reunidos os requisitos que estas prevêm para que a comunicação se possa efectuar. A resposta foi positiva, com igual fundamentação àquela que presidiu nas experiências anteriormente descritas.

Quanto ao segundo aspecto (atribuição de nomes e chaves de utilizador), importou verificar se estavam cumpridos os requisitos previstos na LPD. Efectivamente, a UMIC pretendeu enviar correspondência a todos os eleitores portugueses residentes no estrangeiro, no sentido de providenciar informação para os sensibilizar a participar nesta experiência, enviando-lhes o(s) código(s), nome e chave de utilizador, de modo a habilitar as pessoas a participar na experiência de voto electrónico.

Para efeitos de envio das mensagens de correio aos eleitores, a UMIC subcontratou a CESA – Campos Envelopagem, S.A. Para tratamento de dados subcontratou a NovaBase, S.A. Ambos os sub-contratados são empresas privadas.

Na primeira carta que a UMIC enviou ao titular dos dados, a CNPD fez impender sobre a UMIC o dever de fornecer todas as informações indicadas no art.º 10.º, n.º 1 da LPD. Assim, por uma questão de transparência, haveria de ficar claro para o titular dos dados que o responsável do tratamento era a UMIC, qual a finalidade daquele tratamento e que os dados foram obtidos junto do STAPE.

A CNPD impôs ainda que fosse facultado ao titular dos dados informação sobre a possibilidade de o eleitor “se opor, em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados” (Cfr.art.º 12.º al. a) da LPD).

Importou ainda analisar a questão relativa às medidas de segurança e de confidencialidade do tratamento. A CNPD considerou que a UMIC não deixava de ser a responsável pelo tratamento, uma vez que as empresas intervenientes (CESA e Novabase) actuaram sempre na qualidade de sub-contratantes, ou seja, mediante instruções do responsável pelo tratamento (no n.º 1 do art.º 14.º e art.º 16.º da LPD). No entanto, o contrato devia conter especificamente quais as medidas técnicas e organizativas que o responsável considerava adequadas para proteger os dados, sendo o nível de segurança estipulado pelo responsável, tendo em conta os riscos que o tratamento apresentava e a natureza dos dados.

Quanto ao terceiro aspecto (exercício do voto electrónico não presencial), a CNPD condicionou a autorização à garantia dos aspectos relativos à confidencialidade e secretismo do voto e expressou fortes preocupações quanto à fiabilidade do voto final registado face à opção efectivamente tomada pelo eleitor.

Na aferição da CNPD, não se tinham eliminado, evitado ou diminuído os riscos de viciação do processo eleitoral a partir do computador do eleitor. A título de exemplo, a CNPD indicou os procedimentos conhecidos por “*The man in the middle*”, “*DNS Spoofing*” ou *Phishingscam*, a par da introdução de vírus nos computadores dos eleitores ou naqueles que estes utilizariam para o exercício de voto (onde podem encontrar-se instalados ou serem introduzidos *Screenloggers* e, ou, *Keyloggers*), como ocorrências passíveis de acontecer e que desvirtuavam o sistema de voto electrónico não presencial, na medida em que o resultado final do voto exercido não coincidiria com a opção tomada pelo eleitor, ou então permitiam o conhecimento da opção tomada pelo mesmo eleitor.

Assim, a CNPD autorizou a comunicação de dados por parte do STAPE relativamente aos cidadãos eleitores residentes no estrangeiro para que a UMIC pudesse iniciar o processo de atribuição de nomes e chaves de utilizador, bem como o seu envio aos eleitores. Não obstante, o tratamento de dados por parte da UMIC ficou condicionado ao cumprimento do direito de informação, à existência de um contrato ou acto jurídico com as entidades sub-contratantes e sob condição das garantias de confidencialidade, secretismo e fiabilidade do voto, de acordo com o supra exposto.

Análise dos relatórios de auditoria das experiências

O voto electrónico carece de um enquadramento multidisciplinar. Os quadros jurídicos, como, de resto os políticos, os económicos e os sociológicos, não são apenas formais; são também materiais e os respectivos conteúdos devem ser avaliados segundo os seus próprios critérios.

Ora, a abordagem experimental do voto electrónico foi eminentemente técnica, tendo sido avaliada predominantemente nessa perspectiva. Nos relatórios de auditoria não se encontraram quaisquer considerações jurídicas acerca da conformidade ou desconformidade das referidas experiências com os princípios eleitorais em vigor no nosso país.

Em todo o caso, foram detectados do ponto de vista técnico várias situações que subsumidas às previsões normativas que estruturam o nosso sistema eleitoral são absolutamente incompatíveis com ele.

A única aferição de ordem jurídica, e também técnica, que consultámos foi a efectuada pela CNPD e que consta da deliberação “A privacidade dos eleitores no voto electrónico”, aprovada na sessão de 14/11/2005 da CNPD.

A CNPD acompanhou os processos das experiências das votações electrónicas não vinculativas, presenciais e não presenciais, e destacou diversas críticas. Alguns dos problemas são técnico-organizacionais, como: a inexistência de palavras-chave nalgumas máquinas; o carregamento de cadernos eleitorais nas urnas electrónicas muito antes do permitido; a não cifragem nem destruição dos ficheiros no fim do acto eleitoral; a utilização de motores de bases de dados sem segurança acrescida, o que permitiria, caso essas bases de dados colocassem estampilhas temporais nas operações de registo de eventos, relacionar eleitores com votos expressos, colocando em crise o secretismo da votação; o sistema de protecção contra falhas era insuficiente e defeituoso, não estando as máquinas preparadas nem configuradas para trabalharem em redundância.

Mas o mais importante é a reflexão efectuada pela CNPD, na secção II da deliberação. Para a CNPD, a análise da votação electrónica reclama a avaliação do tratamento dos dados pessoais dos eleitores nesse âmbito e para essa mesma finalidade – do exercício do voto através de meios electrónicos – à luz do regime jurídico da protecção de dados pessoais.

Assim e em primeiro lugar, a CNPD invoca a exigência do processamento transparente dos dados pessoais (artº.2 da LPD). O princípio da transparência efectiva-se através dos direitos à informação (artº.10) e acesso (artº.11) garantidos ao titular dos dados pessoais, pelo que o tratamento de dados pessoais no âmbito de e para a finalidade do exercício do voto através dos meios electrónicos deve contar com o pleno conhecimento por parte dos cidadãos eleitores, titulares desses dados, sobre todos os termos, modos e condições que

esse tratamento conhece, pelo menos aqueles que são elencados no formulário da notificação junto da CNPD.

Em segundo lugar e de acordo com a alínea a) do n.º.1 do art.º.5 da LPD, os dados pessoais objecto de processamento devem ser tratados de forma lícita e com respeito pelo princípio da boa fé.

Assim e desde logo requer-se o cumprimento do art.º.5. da LPD. Assim os dados pessoais dos eleitores têm de ser: (i) recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades; (ii) adequados, pertinentes e não excessivos relativamente à finalidade para que são recolhidos e posteriormente tratados; (iii) exactos e actualizados; e (iv) conservados apenas durante o período necessário à prossecução da finalidade.

O princípio da licitude e o princípio da lealdade envolvem, não apenas as garantias funcionais que abarcam todo o processo, uma garantia funcional suplementar de ordem técnica, juridicamente tutelada, que “consiste na obrigação de especial diligência por parte das entidades que procedem ao registo no sentido de assegurar a segurança dos ficheiros contra a sua destruição ou perda acidental ou contra o acesso, modificação ou difusão não autorizados” (art. 7º).

Destes princípios - licitude, lealdade e transparência - resulta a obrigação da entidade responsável pelo tratamento dos dados pessoais de tomar as medidas técnicas e organizativas adequadas “para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito” (n.º.1 do art.º.14).

A CNPD sublinha que se tivermos em conta que (i) os dados pessoais a proteger, no caso do exercício electrónico do direito de voto por parte dos cidadãos titulares e eleitores, são o nome, a morada, o número de eleitor (constantes da BDRE) e a opção de voto efectivamente tomada numa eleição política, que (ii) existe um risco particularmente significativo de ataques externos aos dados pessoais dos eleitores no exercício electrónico do direito de voto político, atenta a vulnerabilidade dos computadores, sobretudo se estiverem ligados a uma rede aberta e, ainda, que (iii) a eleição política é, porventura, o cerne dos regimes e das sociedades democráticas, as regras e os resultados, no que toca à segurança da integridade, fiabilidade e confidencialidade dos dados pessoais é a mais exigente que se pode impor a qualquer entidade responsável pelo tratamento.

Citando Catarina Sarmiento e Castro, o CNPD precisa que “a garantia de segurança traduz-se na salvaguarda da informação, mas também na manutenção da sua integridade, através da adopção de medidas que impeçam a alteração dos dados, que permitam detectar disfuncionalidades e corrigi-las”, e “impõe que os responsáveis pelos tratamentos

impossibilitem a difusão ou o acesso não autorizados de dados pessoais, assim se garantindo a sua confidencialidade”.

Outro aspecto focado pela CNPD tem a ver com a legitimidade de quem procede ao tratamento de dados pessoais dos eleitores. É opinião da CNPD, que o tratamento de dados pessoais dos eleitores para fins de eleição política através de exercício do voto por meios electrónicos tem de encontrar a sua legitimidade sedimentada em lei da Assembleia da República, atendendo, não ao n.º.2 do art.º.7º da LPD e ao n.º.3 do art.º.35º da Constituição da República Portuguesa (CRP), mas agora, porque se trata de matéria eleitoral, à devida submissão à alínea a) do art.º.64º da CRP.

A CNPD ressalva contudo as experiências não vinculativas que podem encontrar a sua condição de legitimidade, no que toca ao tratamento dos dados pessoais dos eleitores, na alínea d) do art.º.6 da LPD – execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados.

Síntese dos resultados das experiências portuguesas

Tendo em conta as experiências realizadas podem-se retirar as seguintes ilações:

- Não há indicações que conduzam à conclusão de que a utilização dos sistemas de votação electrónica comprometa, só por si e de algum modo, os princípios e regras de direito eleitoral – a oficiosidade, obrigatoriedade, permanência e unicidade do recenseamento eleitoral, o sufrágio directo, secreto e universal, a liberdade e unicidade do voto;
- O respeito pelos princípios e regras de direito eleitoral reflecte-se, no que concerne à protecção de dados pessoais, não apenas na qualidade dos dados pessoais dos eleitores, mas também na transparência, licitude, boa fé e legitimidade do tratamento de dados pessoais dos eleitores;
- A votação electrónica pode ser compatível com os princípios eleitorais básicos, desde que as normas jurídicas, técnicas e operacionais sejam de molde a garanti-los.

EXPERIÊNCIA PORTUGUESA DE 2004: PERSPECTIVA TÉCNICA

Pedro Antunes, Luís Carriço e António Ferreira

Este capítulo reporta e analisa as acções de auditoria realizadas por uma equipa da Faculdade de Ciências da Universidade de Lisboa (FCUL) durante a experiência de voto electrónico realizada em 13 de Junho de 2004¹⁰⁸. O objectivo principal da equipa foi detectar falhas nos sistemas de votação electrónica utilizados, tendo em vista a sua posterior correcção.

Em geral, a experiência de voto electrónico foi bem sucedida, não só pelo entusiasmo revelado por eleitores, representantes autárquicos e outros agentes, incluindo os responsáveis pela experiência, como também pelo manancial de informação que permitiu recolher.

A equipa da FCUL visitou algumas freguesias onde se encontravam instalados vários tipos de sistemas (foram utilizados três sistemas diferentes):

- Santa Maria de Belém (Lisboa)
- São Sebastião (Setúbal)
- Sé (Portalegre)
- São Bernardo (Aveiro)
- Salvador (Beja)

Relativamente aos comentários apresentados abaixo devem ser consideradas duas ressalvas importantes. A primeira é que, pela sua própria natureza, a actividade de auditoria tende a realçar mais os factos negativos que os positivos, pelo que o tom negativo da avaliação das experiências deve ser entendido nesse contexto particular. Em segundo lugar, deve ser referido que, por razões de planeamento e organização de projecto de toda a experiência, não foram atribuídos todos os meios (recursos e tempo) necessários e suficientes para: (1) a análise, desenvolvimento e teste rigoroso dos protótipos utilizados; (2) preparação de um conjunto de regras e procedimentos sobre a utilização dos protótipos; e (3) formação cuidada dos operadores, incluindo os eleitores.

¹⁰⁸ Antunes, P., N. Neves, L. Carriço, P. Veríssimo, R. Pinto and F. Simões (2004). Projecto de Avaliação de Sistemas de Votação Electrónica: Resultados da Auditoria. Faculdade de Ciências da Universidade de Lisboa.

Sobre o contexto em que foi realizada a experiência

A experiência envolveu a realização de um segundo voto experimental, em recinto controlado, após a votação oficial. Em todas as freguesias visitadas verificou-se que o local de voto electrónico se encontrava bem visível e próximo do local de voto “legal”, sendo todos os eleitores estimulados a participar na votação electrónica. Verificou-se também que os eleitores estavam bem informados da ocorrência da experiência e demonstraram em geral grande entusiasmo em participar.

A tipologia do local de voto electrónico variou consoante o número de eleitores, sendo caracterizada por 1-2 mesas eleitorais, onde se fazia a verificação do direito de voto do eleitor (e nalguns casos, consoante o sistema utilizado, se colocavam os votos na urna), e 2-10 máquinas electrónicas de registo directo.

Verificou-se que nalguns locais de voto as quantidades de mesas eleitorais e de máquinas de registo directo não estavam dimensionadas de forma a evitar filas de espera, sendo necessário no futuro proceder a um melhor dimensionamento dos sistemas.

Notou-se uma clara distinção entre a sala de voto “legal” e a sala de “voto electrónico”, sendo a primeira claramente mais formal que a segunda. Para esta situação contribuíram dois aspectos fundamentais:

- Na sala de voto electrónico estavam diversos elementos oficiais com a função de ajudar os eleitores no processo de votação, o que não acontece no processo normal;
- A constituição das mesas eleitorais do voto electrónico não seguia exactamente a lei eleitoral.

Este último aspecto foi bastante evidente nas freguesias onde as mesas não tinham elementos designados pelos partidos políticos. Em algumas freguesias estavam presentes na mesa eleitoral elementos designados pelos partidos e que normalmente participam no processo eleitoral. Neste último caso foi possível recolher (informalmente) informação mais rica sobre o processo de voto electrónico.

A informalidade assumida pela experiência de voto electrónico criou algumas dificuldades à avaliação do processo, já que dificultou a obtenção de comentários pertinentes dos agentes normalmente envolvidos num processo eleitoral e criou um cenário demasiado artificial, com consequentes desvios na análise dos resultados.

Sobre o papel dos avaliadores

A equipa da FCUL assumiu fundamentalmente o papel de observadora do processo. Observaram-se as acções dos eleitores, tentando não colocar em causa o Anonimato: na maior parte das situações não foi possível observar directamente as interacções dos eleitores com os dispositivos de votação (nas outras tal ocorreu por solicitação dos eleitores, para fornecer ajuda). Foi possível observar sem restrições as acções dos elementos nas mesas eleitorais.

As observações foram complementadas com conversas informais com os diversos agentes envolvidos no processo eleitoral, desde presidentes de juntas de freguesia aos elementos das mesas eleitorais e outros elementos oficiais que prestavam ajuda aos eleitores.

Falhas detectadas relacionadas com os equipamentos

Numa freguesia ocorreram problemas com a inicialização do software de gestão dos eleitores, aparentemente devidas a incompatibilidades com o tipo de ficheiro de dados fornecido pela Junta de Freguesia. Esses problemas resultaram num atraso de 45 minutos na abertura do voto electrónico.

Noutra freguesia ocorreram também problemas na inicialização do software de gestão dos eleitores, agravados pela demora do software em gerar os cartões de identificação dos membros da mesa eleitoral. Estes problemas originaram um atraso de cerca de uma hora na abertura do voto electrónico.

Ocorreu uma avaria de um cartão de memória utilizado por uma máquina de registo directo, deixando essa máquina inoperacional. O elemento de apoio da empresa responsável pelo sistema, presente no local de voto, não conseguiu resolver o problema, tendo este sido posteriormente resolvido após a chegada de outro elemento chamado para o efeito. Os votos armazenados na máquina que falhou não foram perdidos. Notou-se no entanto a inexistência de procedimentos em caso de ocorrência de falhas nos equipamentos.

Ocorreu ainda uma outra falha numa máquina de registo directo, mas que ficou resolvida após reinicialização da máquina. Os votos armazenados também não foram perdidos.

Observou-se ainda que, após o fecho das eleições, uma das máquinas de registo directo apresentou dificuldades em estabelecer ligação telefónica para proceder ao envio de resultados. Este problema foi resolvido após algumas tentativas da operadora que estava no local, sendo devido a problemas nos contactos da ficha telefónica.

Observou-se ainda que o uso em grande escala da ligação telefónica deve ser estudado com detalhe, parecendo à partida ser um processo demorado. A título de exemplo, a transmissão dos resultados de uma freguesia constituída por apenas 10 urnas demorou cerca de meia hora.

Observou-se um caso em que o cartão magnético utilizado para transferir o voto entre a máquina de registo directo e a urna apresentou um problema técnico, não descarregando o voto do eleitor. Neste caso, o cartão previsivelmente defeituoso foi colocado à parte por um elemento da mesa e ao eleitor foi atribuído um novo cartão. Observou-se que não existia nenhum procedimento especial para lidar com cartões defeituosos nem nenhum procedimento para registar essas ocorrências.

Observou-se também uma ocorrência de falha de energia, quando o cabo de alimentação de uma das máquinas de registo directo se soltou e a urna não emitiu qualquer aviso sonoro, ao contrário do que referia a documentação do sistema. Observou-se que a máquina continuou a funcionar devido à existência de uma UPS embutida.

Ainda relativamente a falhas de energia, numa freguesia observou-se a ocorrência de uma falha de cerca de 10 minutos. Durante esse período os equipamentos instalados continuaram a funcionar, devido à existência de UPS. No entanto observou-se que o dispositivo que realizava o registo de eleitores não tinha uma fonte de energia alternativa. No caso em concreto foi possível recorrer aos cadernos eleitorais tradicionais em papel para colmatar o problema. Desconhece-se no entanto de que forma se procedeu no fim da eleição à reconciliação entre dos registos de eleitores.

Em resumo, foram verificadas múltiplas ocorrências de problemas com os equipamentos, nenhuma delas crítica, mas observou-se também que não existiam procedimentos estabelecidos para registar e lidar com essas ocorrências.

Tudo indica que a probabilidade de falha localizada do sistema de voto electrónico é significativa. Não tendo dados científicos substantivos para atribuir um valor a essa probabilidade, deve no entanto referir-se que num universo de 5 freguesias ocorreram:

- 2 falhas de inicialização com atraso superior a 45 minutos;
- 3 falhas de equipamento que foram resolvidas num tempo razoável;
- 3 incidentes, também eles resolvidos num tempo razoável;
- 2 Faltas de procedimentos.

Falhas detectadas nos procedimentos de operação do sistema

Como já foi referido anteriormente, o ambiente geral em que decorreu a experiência não permitiu estabelecer padrões rígidos de controlo do sistema de votação electrónica. Por essa razão, todo o processo de selagem dos equipamentos antes das eleições e verificação imediatamente antes de dar início ao processo eleitoral não foi ensaiado.

A finalização formal do processo eleitoral não foi igualmente testada. Em particular, considerando que a contagem de votos pode ser verificada cruzando informação das máquinas de registo directo e do software de registo de eleitores, não foi acautelado o rigor necessário a esse cruzamento.

Foi possível verificar a ocorrência de um incidente em que foi dado o direito de voto sem que esse direito tenha sido efectivamente exercido e sem que o direito de voto tenha sido posteriormente cancelado.

Num outro caso verificou-se ainda que o software que fazia o registo de eleitores não foi fechado às 20:00, pelo que era possível aos passantes usar o software, por exemplo para indicar que novos eleitores tinham votado.

Numa outra situação ocorreu um incidente mais complexo, mas que por isso mesmo deve ser descrito em maior detalhe. O caso ocorreu quando uma eleitora, depois de votar, saiu do local levando o cartão magnético que descarregava o seu voto na urna e que deveria ser entregue na mesa. Após alguns instantes sem que a eleitora voltasse, foi decidido pelo membro da mesa que o seu direito de voto devia ser cancelado. O software de registo de eleitores geria uma lista com os eleitores a quem tinha sido atribuído o direito de voto, materializado pela posse do cartão magnético. Junto a cada entrada dessa lista o software mostrava botões para aceitar ou cancelar o direito de voto. A situação que ocorreu foi que o membro da mesa se enganou, acabando por cancelar o direito de voto de outro eleitor. Esta operação não é reversível. Em seguida a eleitora voltou ao local, sendo o membro da mesa obrigado a pedir-lhe que votasse de novo, tendo para o efeito, no software, seleccionado não o nome da eleitora mas sim o nome de outro eleitor que sem o saber viu o seu direito de voto cancelado. Notou-se que não existiam procedimentos de registo de ocorrência de incidentes pelos elementos da mesa, de forma a acautelar possíveis problemas levantados por auditorias posteriores.

Parece-nos ainda que os dispositivos electrónicos de registo dos eleitores devem ser estudados com mais atenção, já que introduzem pontos de falha no sistema de votação electrónica que não existem quando se recorre aos antigos cadernos eleitorais em papel. Em

particular, deve notar-se que a verificação cruzada do registo de eleitores, efectuada por diversas pessoas, se torna menos eficaz: a manipulação do software fica normalmente centralizada numa única pessoa, e a mera inspecção visual pode falhar por razões cognitivas associadas à repetição e cansaço.

Nalguns casos o ciclo do processo eleitoral não foi devidamente controlado. Em particular, relativamente ao processo de votação que recorria a cartões magnéticos não reutilizáveis para descarregar os votos nas urnas, verificou-se que toda a gestão dos cartões foi pouco controlada, devendo estes idealmente encontrar-se numa caixa especial que permitisse a entrega de um único cartão de cada vez, não estando nenhum outro cartão acessível. Verificou-se ainda que os cartões não eram guardados de forma segura.

Observou-se ainda que os cartões magnéticos entregues a cada votante para realização da votação apresentavam uma numeração, o que possibilitaria a quebra do Anonimato, se fossem relacionados com informação de registo temporal da máquina de registo directo. Observou-se ainda que os cartões entregues aos eleitores não eram entregues de forma totalmente aleatória, mas sim de forma sequencial, o que também facilitaria a quebra de Anonimato, ou pelo menos a sua suspeição.

Falhas detectadas no processo de votação

Verificou-se que num dos locais de voto se formavam longas filas de espera para votar. Apesar de a relação mesas eleitorais/máquinas de registo directo ser desfavorável (existia apenas uma mesa e duas máquinas de registo directo), o problema deveu-se fundamentalmente a um processo pouco optimizado de votação. As medições efectuadas indicaram:

- Duração média de uma utilização da máquina de registo directo: 4 minutos;
- Duração mínima observada de uma utilização da máquina de registo directo: 2 minutos;
- Tempo necessário para a leitura do cartão magnético na urna: 15 segundos.

Foi registado que os membros da mesa eleitoral se queixavam em particular da demora na leitura dos cartões magnéticos. Na realidade, a arquitectura do sistema de votação electrónica, tal como estava concebida, originava três filas de espera distintas: (1) diante da mesa de voto, para votar; (2) diante das máquinas de registo directo; e (3) de novo diante da mesa de voto, para proceder à leitura do cartão magnético na urna.

Em contraponto, num outro local foram medidos:

- Duração média de uma utilização da máquina de registo directo: 2 minutos;
- Duração mínima observada de uma utilização da máquina de registo directo: 1 minuto;

Neste segundo caso o sistema não exigia leitura do cartão magnético, o que tornou o processo de votação mais expedito.

Usabilidade dos dispositivos

A usabilidade dos dispositivos de interface de todas as máquinas de registo directo revelou-se particularmente crítica na experiência que foi realizada, tendo sido observados diversos problemas.

Num determinado caso, a interface de votação iniciava-se com a apresentação de duas bandeiras, para escolha de idioma, sem qualquer texto adicional ou indicação visual de que os eleitores deviam seleccionar uma das bandeiras. Observou-se que os eleitores, não percebendo o que fazer, ficavam à espera de ajuda.

A interface de votação de um outro sistema tinha um botão para “terminar” a votação que levava os eleitores a pensar que já podiam retirar o cartão da máquina de registo directo, pois o processo estava terminado. A interface no entanto não funcionava desse modo, apresentando aos utilizadores, demasiado tempo após seleccionarem tal botão, uma janela a dizer que já podiam retirar o cartão. Esta funcionalidade inadequada resultou numa taxa muito elevada de cartões que acabavam por ser retirados da máquina antes de o voto ser neles registado, situação posteriormente detectada pela urna, obrigando os eleitores a votar segunda vez.

Ainda relativamente à utilização de cartões magnéticos, observou-se que a urna demorava demasiado tempo a ler os cartões (cerca de 15 segundos), gerando um evidente desconforto quer nos eleitores quer nos membros da mesa eleitoral. Pensamos que a situação está associada a funções criptográficas realizadas no cartão, o que levanta a questão sempre interessante de conseguir conciliar adequadamente a usabilidade com a segurança.

O “cartucho” utilizado por um outro sistema, em substituição dos cartões magnéticos, não dava indicações aos utilizadores de como deveria ser colocado na ranhura da máquina de registo directo, tendo sido observado que os utilizadores sistematicamente realizavam diversas tentativas, com consequentes demoras no processo de votação. Este problema observou-se praticamente com todos os utilizadores.

Observou-se que um botão de bloqueamento do “cartucho” – um botão físico colocado no topo da máquina de registo directo, ao centro – estava fora da área de foco dos utilizadores, que era normalmente em baixo, deixando assim os eleitores perdidos e a necessitarem de ajuda. Apesar do botão físico colocado no topo da máquina ter uma luz que ficava intermitente, avisando os eleitores que tinham ainda de premir o botão, esse aviso foi sistematicamente ignorado.

Observou-se também que, numa determinada interface, os botões de selecção de idioma (Português/Inglês) se encontravam demasiado juntos e num alinhamento vertical, o que originou que diversos eleitores acabassem por seleccionar o idioma errado (o alinhamento horizontal reduz a taxa de erros, por causa do posicionamento dos dedos na mão na altura de seleccionar uma opção). A agravar esta situação, observou-se que a selecção de idioma não era reversível.

Ainda relativamente a problemas de interface, observou-se que os eleitores tinham muitas dificuldades em perceber alguns mecanismos de interacção mais complexos, por exemplo um que consistia em primeiro seleccionar o voto e depois premir um botão amarelo com a palavra “seguinte”. Este tipo de mecanismo de interacção é evidente para quem utiliza correntemente os computadores, mas não se aplica ao universo eleitoral.

Observou-se que uma ranhura frontal existente num tipo de máquina de registo directo, destinada a produzir um relatório em papel, foi muitas vezes confundida pelos eleitores com a ranhura onde deveriam introduzir o cartão magnético de registo do voto.

As maiores dificuldades relacionadas com usabilidade foram sem dúvida o auxílio prestado aos menos letrados. As pessoas menos letradas apresentaram imensas dificuldades em lidar com o processo de votação, sendo sempre necessária ajuda para que o eleitor iniciasse e completasse o processo de votação.

Numa freguesia ainda se experimentou que os eleitores menos letrados usassem a urna destinada aos invisuais, mas tal solução não resultou: para além do processo se tornar demasiado lento, nunca deixou de ser necessária ajuda, pelo que tal solução rapidamente deixou de ser aplicada.

Em geral, a linguagem utilizada nas interfaces estava correcta mas tendia a ser pouco compreensível para pessoas menos letradas. Foram utilizadas palavras demasiado extensas, como “terminar”. Teria sido preferível a utilização sistemática de palavras mais curtas, como “fim”. Os sistemas deveriam também ter recorrido ao uso sistemático de cores, como o “verde” para aceitar ou “vermelho” para cancelar ou alguns símbolos comuns, como o “X” para cancelar.

Relativamente à interface para invisuais, notou-se que a sua utilização era extremamente demorada (cerca de 15 minutos por eleitor). Registou-se inclusivamente um caso em que o tempo limite temporal para votar imposto pela máquina foi excedido. Notou-se em particular que a vocalização dos textos era realizada de forma demasiado lenta e monótona.

Informação disponibilizada aos eleitores

Este tema está obviamente relacionado com o anterior, no sentido em que a falta de informação clara e precisa sobre o processo de votação e uso dos dispositivos de votação agrava os problemas de usabilidade.

A informação distribuída aos eleitores foi insuficiente, tendo sido notado que praticamente 100% dos eleitores necessitaram de ajuda. Foi particularmente evidente que mesmo os eleitores mais letrados recorreram sistematicamente a ajuda de elementos oficiais.

Numa freguesia foram distribuídos aos eleitores uns folhetos que apresentavam as instruções, em poucos passos mas com grande exactidão, utilizando fotografias que reproduziam exactamente o local e o modo como iriam votar. Foi observado que alguns eleitores votavam seguindo as instruções desse folheto, convenientemente colocado na mão esquerda, enquanto votavam com a mão direita. Ao contrário, numa outra freguesia, os folhetos não davam o mesmo tipo de ajuda: sem imagens e com um número demasiado elevado de passos (10). Observou-se que não eram utilizados.

Noutra freguesia, ao invés de folhetos era apresentado um filme que ilustrava o processo de votação. O equipamento de projecção ficava precisamente nas costas da fila que os eleitores formavam para votar, pelo que acabava por não ter papel relevante.

Observou-se ainda que o uso de palavras técnicas, como “smartcard”, deve ser evitado neste tipo de folhetos.

Ficou absolutamente evidente na experiência que os folhetos disponibilizados aos eleitores são um componente fundamental do sistema de votação electrónica, não podendo de todo ser negligenciados.

Foi sugerido por elementos das juntas de freguesia que alguns exemplares dos sistemas de votação deveriam ser facultados antes do processo eleitoral, de forma a que os elementos das mesas, e até eventualmente os eleitores, se pudessem familiarizar com a tecnologia antes do acto eleitoral.

O CASO DAS ELEIÇÕES NA FLÓRIDA

Pedro Antunes

O sistema eleitoral dos EUA é muito peculiar, já que não possui regulamentação para as eleições a nível federal, mas sim estadual. Daí existir uma grande diversidade de sistemas e processos de votação.

Actualmente, existe um esforço gradual de convergência num tipo de tecnologia, os dispositivos electrónicos de registo directo. No entanto, quando ocorreu o caso das eleições na Flórida no ano 2000, um dos sistemas de votação mais populares era baseado em cartões perfurados.

O Vote-O-Matic é um equipamento de cartões perfurados (*punch-card*) que foi utilizado em 15 municípios da Florida durante as eleições para a Presidência dos EUA realizadas em Novembro de 2000. O Vote-O-Matic é tecnologicamente muito pouco sofisticado, sendo constituído por uma caixa portátil onde pode ser colocado um livro contendo a lista de eleições e de candidatos. Este livro é necessário porque nos EUA ocorrem geralmente muitas eleições em simultâneo para diversos cargos e diversos níveis de governação, e ainda para decidir questões estaduais e locais.

O Vote-O-Matic apresenta uma ranhura onde se insere o cartão perfurado que regista as opções do eleitor, ficando o cartão por detrás do livro. Após a inserção do cartão perfurado, o eleitor pode folhear as diversas páginas do livro. Ao centro do livro, no eixo vertical aparece uma série de furos. Cada furo representa uma opção de voto na eleição correspondente às páginas abertas do referido livro. Quando o eleitor decide por uma opção, coloca um lápis perfurante no furo correspondente. O resultado é que esse lápis acaba por perfurar o cartão colocado por detrás do livro.

Quando o eleitor termina de votar, o cartão perfurado é introduzido num leitor, que conta os votos a partir de um sistema electrónico de luzes e sensores (os orifícios deixam passar a luz por um lugar determinado, o sensor é activado e assim fica contado o voto).

Este sistema tornou-se mundialmente famoso em Novembro de 2000 porque a diferença de votos entre os candidatos George W. Bush e Al Gore acabou por apresentar uma margem inimaginável de 537 votos, ficando a eleição presidencial dependente dos resultados do condado de Palm Beach na Flórida.

Ora o problema é que os resultados do condado de Palm Beach foram muito controversos e geraram contestação e pedidos de recontagem. A base principal para a contestação resulta de um problema fundamental do sistema de cartões perfurados:

- O leitor óptico rejeita os votos que não têm o orifício do cartão completamente desobstruído;
- No entanto, nas situações em que o eleitor marca o cartão com o lápis de forma suficiente para o cartão ficar marcado, mas sem o orifício desobstruído, a intenção do eleitor está “potencialmente” expressa mas não é considerada pelo sistema de votação.

Este problema teve de ser explicado com inesperada minúcia às autoridades que geriam as eleições na Flórida pelo próprio criador do Vote-O-Matic¹⁰⁹.

Dos diversos pedidos de recontagem de votos ficou a imagem disseminada a nível mundial de elementos oficiais analisando os cartões e discutindo se a intenção do eleitor estava ou não expressa.

Como se sabe, o impasse gerado só foi resolvido após declaração de vitória de George W. Bush e aceitação de derrota por parte de Al Gore, depois de o Supremo Tribunal dos EUA ter decidido suspender a recontagem de votos por considerar que feria a equidade do processo.

Um estudo comparativo de diversos sistemas de votação realizado pelo consórcio universitário Caltech/MIT¹¹⁰ ¹¹¹ veio quantificar a percentagem de erro na contagem dos votos pelos sistemas de cartões perfurados. Os resultados obtidos encontram-se na tabela seguinte.

¹⁰⁹ <http://transcripts.cnn.com/TRANSCRIPTS/001124/se.01.html>. Consultado em 12 de Dezembro de 2007.

¹¹⁰ The Caltech/MIT Voting Technology Project (2001). Residual Votes Attributed to Technology. Caltech/MIT.

¹¹¹ S. Ansolabehere and C. Stewart III. Residual Votes Attributable to Technology. *Journal of Politics*, Vol. 67, No. 2: 365-389.

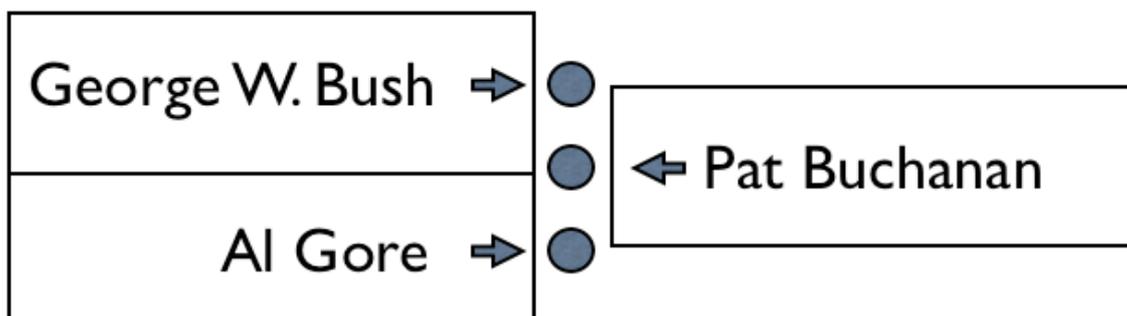
Tipo de sistema	Porcentagem de erro	Desvio padrão
Votação em papel	1.9	2.1
Alavancas	1.7	1.7
Cartões perfurados		
Vote-O-Matic	2.6	1.9
DataVote	2.4	2.7
Leitura óptica	1.6	2.8
Registo directo	2.2	1.8
Global	2.1	2.2

Como se pode observar, a percentagem de erro do Vote-O-Matic é maior que a de qualquer outro sistema. Note-se ainda que esta percentagem de erro permitiria mudar o resultado eleitoral para qualquer um dos dois candidatos, já que oficialmente a margem de vitória foi de apenas 537 votos¹¹².

No entanto, um problema adicional, eventualmente mais interessante, foi ainda levantado relativamente ao sistema Vote-O-Matic:

- O livro contendo a lista de eleições e de candidatos estava construído de uma forma que não tornava obvio para os votantes em qual candidato estavam realmente a votar.

A forma como o livro foi construído está esquematizada na figura abaixo. Observe-se que os candidatos são alternativamente arrumados à esquerda e à direita (na figura apenas se



apresentam três candidatos apesar de o livro apresentar mais).

O problema desta arrumação é que, para quem olha para o lado esquerdo do livro, o candidato Al Gore é o segundo da lista; no entanto, considerando também os candidatos do

¹¹² Walter R. Mebane Jr. (2004). The Wrong Man is President! Overvotes in the 2000 Presidential Election in Florida, *Perspectives on Politics*, 2(3).

lado direito do livro, para seleccionar Al Gore é necessário perfurar a terceira marca do cartão e não a segunda. Note-se ainda que o problema será agravado para os eleitores que escrevem com a mão direita, pois na altura de seleccionar um candidato a mão direita tende a obstruir o lado direito do livro, reforçando implicitamente que para votar em Al Gore será necessário perfurar a segunda marca e não a terceira.

Estudos demográficos realizados após as eleições demonstraram que Pat Buchanan recebeu cerca de 20% dos votos em Palm Beach enquanto que na totalidade do estado da Flórida recebeu apenas 7%¹¹³. Cerca de 2.000 votos destinados a Al Gore foram aparentemente atribuídos a outro candidato. Relembramos que a diferença oficial entre George W. Bush e Al Gore foi de 537 votos.

Em conclusão, este terá sido um caso concreto em que os problemas de concepção da interface terão influenciado decisivamente os resultados eleitorais.

¹¹³ H. Brady, M. Herron, W. Mebane, J. Sekhon, K. Shotts, J. Wand (2001). Law and Data: The Butterfly Ballot Episode. Political Science and Politics, pp. 59-69.

AUDITORIA

Pedro Antunes

Um requisito chave que um sistema de votação electrónica deve cumprir é a confiança: os eleitores e a sociedade em geral devem poder confiar que o processo electrónico não elimina nenhuns dos princípios fundamentais associados a uma votação democrática num país livre. A este requisito fundamental devem depois ser acrescentados muitos outros, que representem significativas vantagens para os utilizadores do sistema, sem os quais não se justifica adoptar este novo processo de votação.

A confiança no sistema tem de ser obtida de diversas formas e a diversos níveis, nomeadamente legal, técnico e societário. A auditoria ganha especial relevo como método destinado a avaliar o rigor dos sistemas de votação electrónica para cumprir com os requisitos técnico-legais exigidos, contribuindo também para a formação de confiança na sociedade sobre o sistema, o processo e o seu impacto positivo.

A confiança transmitida pela auditoria será tanto maior quanto o próprio processo de auditoria for transparente, detalhado e preciso. Neste capítulo pretende-se apresentar um plano de auditoria que cumpre os requisitos mínimos de qualidade de um processo de auditoria de sistemas de votação electrónica. O plano proposto está dividido em três partes:

- Definição do objecto da auditoria;
- Definição da metodologia de avaliação;
- Definição dos objectivos a atingir.

Objecto da auditoria

O objecto da auditoria identifica as partes do sistema de votação electrónica que devem ser objecto de avaliação. Devem ser consideradas:

Infraestrutura de suporte

Componente técnica do sistema, englobando os seus diversos dispositivos de hardware, componentes de software, interfaces físicas e lógicas e componentes de comunicações.

Interfaces com os utilizadores

Englobando os diversos dispositivos físicos e lógicos de interligação entre o sistema e os utilizadores (eleitores, gestores do sistema, manutenção, supervisores, auditores, etc.).

Sistema socio-técnico

O sistema de votação electrónica perspectivado como uma caixa negra, apresentando-se com um conjunto de atributos, funcionalidades e restrições. Engloba as componentes processuais de votação, operação, manutenção, etc.

Esta divisão em três perspectivas deve ser sistematicamente utilizada durante todo o processo de auditoria.

Definição da metodologia de avaliação

Independentemente da metodologia concreta que for adoptada para auditar um sistema de votação electrónica, ela deve ser compatível com as melhores práticas utilizadas na engenharia de software, designadamente nos processos para assegurar a qualidade recomendados pelas normas ISO e IEEE. Nessa perspectiva, o processo de auditoria deve compreender pelo menos as seguintes tarefas:

1. Avaliação global do cumprimento das propriedades fundamentais dos sistemas de votação electrónica (e.g. anonimato, privacidade, direito de voto, etc.), numa perspectiva socio-técnica;
2. Avaliação do processo eleitoral, analisando o cumprimento das propriedades fundamentais dos sistemas de votação electrónica relevantes em cada uma das fases do processo eleitoral (votação, contagem, etc.);
3. Avaliação dos diversos componentes do sistema, designadamente aqueles definidos na arquitectura de referência, analisando o cumprimento das propriedades fundamentais dos sistemas de votação electrónica relevantes em cada um desses

componentes (gestão de votos, gestão de contagem, etc.); e no seu conjunto, analisando as dependências e trocas de informação entre componentes;

4. Avaliação da infraestrutura de suporte do sistema, verificando o cumprimento das propriedades fundamentais dos sistemas de votação electrónica pelos diversos dispositivos e subsistemas que compõem a infraestrutura de suporte do sistema (computadores, redes, servidores, etc.);
5. Avaliação das interfaces com os utilizadores, verificando o cumprimento das propriedades fundamentais dos sistemas de votação electrónica pelas interfaces para cada um dos distintos utilizadores do sistema (eleitores, operadores, etc.);
6. Avaliação da qualidade dos restantes elementos associados aos sistemas de votação electrónica (documentos de projecto, manuais, etc.).

Seguindo ainda as melhores práticas no desenvolvimento de software, para cada uma das tarefas acima mencionadas devem ser desenvolvidos planos detalhados de verificação e validação que conduzirão a processos de inspecção. Os processos de inspecção são normalmente realizados em equipa e adoptam a seguinte estrutura:

1. Planeamento da inspecção;
2. Preparação da inspecção;
3. Inspecção, apoiada pelos técnicos responsáveis pelo equipamento a auditar;
4. Análise causal e preenchimento de uma grelha de conformidades e não conformidades, eventualmente contando com o apoio dos técnicos responsáveis pelo equipamento a auditar;
5. Definição de próximos passos, com sugestões e recomendações para a resolução de não conformidades.

Definição dos objectivos a atingir

As auditorias aos sistemas tendem a fornecer dois tipos muito distintos de resultados: quantitativos e qualitativos.

Resultados quantitativos

A auditoria deve fornecer resultados quantitativos que permitam realizar comparações entre diferentes sistemas e tecnologias, por exemplo por contagem de conformidades e

não conformidades. Nesse contexto, para cada uma das tarefas a realizar pelo processo de auditoria devem ser utilizadas grelhas de avaliação.

Por exemplo, apresenta-se abaixo uma grelha de avaliação relativa à avaliação global das propriedades fundamentais dos sistemas de votação electrónica.

Grelha de avaliação global			
	Sistema 1	Sistema 2	Sistema n
Autenticidade			
Singularidade			
Direito de Voto			
Anonimato			
Integridade dos Votos			
Não-coercibilidade			
Privacidade			
Auditabilidade			
Certificabilidade			
Confiabilidade			
Detectabilidade			
Disponibilidade			
Integridade do Sistema			
Invulnerabilidade			
Precisão			
Rastreabilidade			
Recuperabilidade			
Verificabilidade			
Autenticação do Operador			
Documentação			
Cifra dos Dados			
Fisicamente Seguro			
Integridade do Pessoal			
Política de Salvaguarda e Recuperação			
Tolerância a Ataques			
Tolerância a Falhas			
Totais			

Esta grelha de avaliação resulta do cruzamento entre o objecto da auditoria, discriminado nos componentes relevantes para a tarefa de auditoria em causa, e os critérios de avaliação associados a essa tarefa. Cada célula da grelha avalia o grau de correlação entre um componente do sistema de votação electrónica e um critério de avaliação. Uma abor-

dagem corrente em avaliações deste tipo (QFD – *Quality Function Deployment*¹¹⁴) utiliza os valores 0, 1, 3 e 9 (nenhuma, fraca, média e forte, respectivamente) para medir estas correlações.

A utilização de valores numéricos permitirá, a partir desta grelha, ordenar diferentes sistemas de votação electrónica, nos casos em que vários forem auditados. Deve no entanto ser ressaltado que nem todos os critérios de avaliação possuem o mesmo grau de importância, pelo que os resultados a fornecer pela auditoria não podem ser meramente resumidos a pontuações globais.

Resultados qualitativos

Uma auditoria deve também fornecer resultados qualitativos sobre o processo e os sistemas de votação electrónica, com o fim de produzir informação relevante para posteriores melhoramentos da tecnologia e dos processos, desenvolvimento de padrões nacionais sobre votação electrónica, certificação nacional de sistemas e dispositivos, assim como contribuições para o desenvolvimento de normas, regras, procedimentos e mesmo legislação.

Esta informação qualitativa poderá ser organizada na forma da tabela ilustrada abaixo, com indicação precisa de pontos fortes e pontos fracos, oportunidades e ameaças.

	Sistema 1	Sistema 2	Sistema n
Sistema socio-técnico			
Processo eleitoral			
Componentes			
Arquitectura			
Interfaces			
Outros elementos			

¹¹⁴ Akao, Y (1990) *Quality Function Deployment: Integrating Customer Requirements into Product Design*. Cambridge, Massachusetts, Productivity Press.

AUDITORIA PROACTIVA

Filipe Simões e Pedro Antunes

Genericamente, a auditoria de um sistema destina-se a minimizar os riscos desse sistema pela via preventiva, assegurando que os mecanismos de controlo de qualidade levam a um maior cuidado na análise, desenho, especificação e desenvolvimento do sistema. Nesta perspectiva preventiva, a auditoria de sistemas de votação electrónica tem como objectivo:

- Reduzir a probabilidade de ocorrência de situações que coloquem em risco o funcionamento normal do processo eleitoral. Já vimos no capítulo relativo à análise de risco que falhas de sistema e falhas humanas podem comprometer o sistema de votação electrónica;
- Verificar a existência de defesas, barreiras e salvaguardas contra incidentes e acidentes;
- Verificar a resiliência do sistema, mantendo a sua operacionalidade face a incidentes e acidentes.

No capítulo onde se discutiu a questão da auditoria, apresentaram-se diversos princípios e metodologias que permitem atingir estes objectivos. Neste capítulo iremos abordar outro tipo de auditoria: a auditoria proactiva, destinada a minimizar os riscos dos sistemas de votação electrónica em tempo real, permitindo testar e verificar o funcionamento do sistema durante o processo eleitoral; e permitindo também intervir em tempo real através da aplicação de defesas e salvaguardas contra incidentes e acidentes de sistema. A auditoria proactiva é portanto complementar da auditoria preventiva.

Como também já vimos no capítulo relativo à arquitectura dos sistemas de votação electrónica, nenhuma das arquitecturas propostas faz referência explícita a um componente de auditoria, apesar de existirem em alguns casos componentes de apoio à verificação do voto, o que corresponde a uma forma muito mitigada de auditoria proactiva.

Os componentes de apoio à verificação do voto - verificação essa realizada pelo votante - podem ser considerados como capazes de auditar partes do sistema de votação electrónica, permitindo aos próprios votantes fazer uma verificação em tempo real do funcionamento do sistema.

Numa perspectiva mais abrangente, a auditoria proactiva deve ser realizada através de uma combinação de actividades de verificação e validação dos eleitores, das entidades oficiais e eventualmente de entidades não oficiais (e.g., associações profissionais, universidades) devidamente credenciadas de forma a dar garantias de isenção, idoneidade e correcção do processo de votação electrónica.

Por outro lado, os componentes de apoio à verificação do sistema, quando existentes, concentram-se numa determinada fase, normalmente no final do processo de votação. Mas não é apenas no final da votação que a auditoria proactiva deve incidir, mas sim ao longo de todo o processo eleitoral. Se um problema apenas for detectado no final da votação, poderá ser demasiado tarde para recorrer a procedimentos de salvaguarda.

A possibilidade de auditar proactivamente o sistema em qualquer uma das suas fases irá tornar o sistema mais credível perante as entidades oficiais e o público em geral. Só a auditoria a cada componente do sistema e a confirmação em tempo real de que ele cumpre as funções para as quais foi construído poderá dar a garantia de que as propriedades do sistema (inerentes à democracia, de sistema e requisitos) se verificam.

A auditoria proactiva é um processo que corre em paralelo com o processo de votação, permitindo monitorar em permanência cada componente do sistema de forma a garantir que ele cumpre as propriedades que lhe são inerentes.

Realça-se a perspectiva de prevenção das situações de risco associadas aos sistemas de votação electrónica, verificando dinamicamente as ocorrências de incidentes e acidentes. Assim, durante a monitorização do percurso do voto ao longo do processo de votação devem ter-se em conta os seguintes objectivos:

- Verificar a integridade do percurso percorrido pelo voto; isto é, confirmar que o boletim passou por todas as fases do processo e componentes do sistema;
- Identificar casos de falha de componentes ou sistema, erro humano e sabotagem;
- Procurar eventuais padrões de falha de componentes ou sistema, erro humano e sabotagem;
- Garantir a qualidade do próprio processo de auditoria proactiva.

A auditoria proactiva deverá ser efectuada pelas seguintes entidades:

- Auditores oficiais e não oficiais devidamente credenciados e com conhecimento do funcionamento dos sistemas de votação electrónica;
- Votantes, que vão obtendo retorno do sistema sobre as operações efectuadas;
- O próprio sistema, utilizando capacidades endógenas de cruzamento e verificação de dados.

Tendo por base a arquitectura de referência anteriormente proposta, importa poder auditar os componentes em cada uma das fases do processo, ao longo de todo o processo e ainda relativamente a cada um dos seguintes componentes:

Fases do processo	Componentes
Pré-registo	Geração de listas de votantes
	Preparação de boletins de voto
Registo	Servidor de registo de eleitores
	Servidor de credenciais
Validação	Servidor de validação de eleitores (credenciais e direito de voto)
Votação	Disponibilização de boletins
	Contagem parcial
	Cifra de boletins
Anonimização	Anonimização
Contagem / apresentação de resultados	Contagem final
	Divulgação de resultados

Se tomarmos como exemplo a fase de votação, por se tratar de uma fase crucial para o sistema, a auditoria proactiva permite monitorar o disponibilizador de boletins, o contador parcial e o componente de cifra de boletim.

Podemos ainda exemplificar alguns casos que demonstram a importância de monitorar os sistemas de votação electrónica com este nível de granularidade:

- Se um determinado componente não receber um voto que um outro acabou de tratar (preparar, contar, cifrar, etc.), o voto poderá ter-se extraviado. Se a informação de que o voto não chegou ao componente esperado for instantaneamente enviada para os auditores do sistema, a continuação e propagação deste problema poderá, eventualmente, ser mitigada. Sob este ponto de vista de auditoria proactiva, fornecer informação de modo mais dinâmico para quem acompanha o processo eleitoral, fará com que uma falha de componentes ou de sistema, erro humano ou sabotagem possam ser imedia-

tamente detectadas. Por exemplo, através da visualização de um aviso relativo à integridade do voto;

- A circulação de mensagens não previstas ou não autorizadas poderá indiciar a ocorrência de algum tipo de sabotagem relacionada com Intercepção, Vírus ou Cavalo de Tróia. Se o sistema de auditoria proactiva tiver a capacidade de contabilizar e comparar o número de mensagens que deveriam circular no sistema de votação electrónica, poderá permitir ao auditor uma vigilância mais apertada do funcionamento do sistema;
- A partir da capacidade de monitorar as entradas/saídas de utilizadores, o sistema poderá reagir a tentativas de acesso ao hardware e software por utilizadores não autorizados;
- A detecção atempada do extravio de um voto poderá permitir tomar medidas que permitam votar de novo, ou pelos menos que evitem que mais votos se percam;
- A capacidade de recolher e guardar os registos sobre as acções realizadas por cada componente do sistema irá dar uma maior garantia de Rastreabilidade do sistema, evitando por exemplo que os atacantes tentem eliminar evidências sobre as suas tentativas de ataque. A auditoria permanente a estes registos permite a substituição de um componente por uma sua réplica sempre que um registo se torne suspeito, isto em tempo útil.

Propomos a auditoria em tempo real dos seguintes dados registados em cada componente:

- Data/hora da passagem de um voto pelo componente;
- Contagem dos votos que passaram pelo componente;
- Mensagens de erro produzidas pelo componente;
- Acesso à base de dados do componente, se existir;
- Entradas/saídas de utilizadores, se o componente envolver interacção com utilizadores;
- Alteração de privilégios dos utilizadores do componente;
- Data/hora de inicialização e fecho do componente;
- Data/hora de substituição do componente.

É a visualização em tempo real destes dados que irá permitir ao auditor manter um controlo o mais apertado possível do comportamento do sistema e por conseguinte uma rápida e acertada tomada de decisão.

SIMULADOR DE AUDITORIA

Duarte Vieira e Pedro Antunes

Este capítulo documenta a realização de um protótipo destinado a realizar auditoria proactiva em sistemas de votação electrónica. Pretendeu-se com este protótipo ilustrar a importância da realização de auditoria proactiva na identificação de problemas, redução de riscos e mitigação de consequências decorrentes da operação de sistemas de votação electrónica.

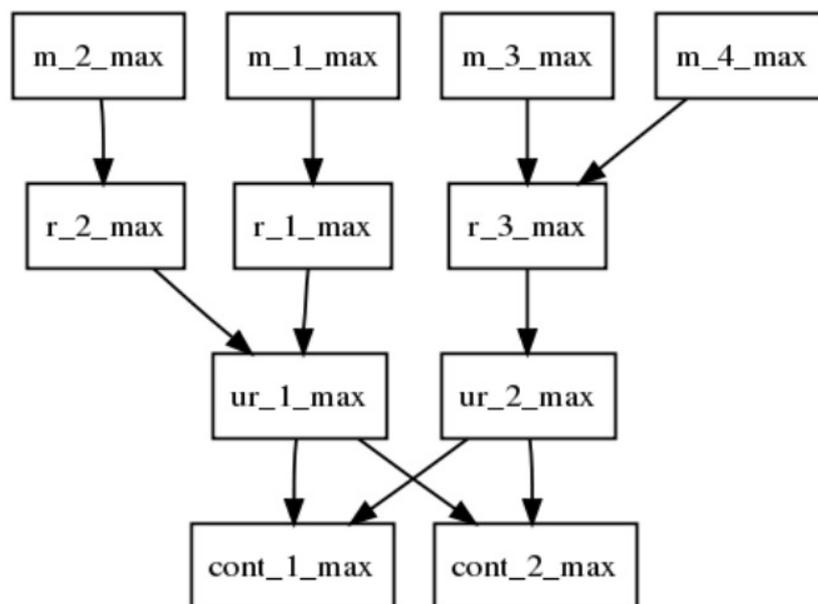
O protótipo desenvolvido destina-se a modelar três tipos de processos de votação electrónica¹¹⁵:

- Maximalista - Utilizando mesas de voto electrónico, máquinas electrónicas de registo directo e urnas electrónicas;
- Intermédio - Utilizando mesas de voto electrónico e máquinas electrónicas de registo directo;
- Minimalista - Utilizando apenas máquinas electrónicas de registo directo.

Para qualquer um destes processos o protótipo considera ainda a existência de recintos de votação e contadores. Os recintos de votação destinam-se a agregar um número variado de mesas, máquinas de registo e urnas numa única unidade lógica. É por exemplo normal que um recinto possua uma única mesa, uma única urna, mas um número variado de máquinas de registo, por forma a aumentar a velocidade e fluidez do processo de votação. Os contadores destinam-se naturalmente a proceder à apuração global dos resultados eleitorais. Tendo em vista modelar formas diferentes de contabilizar os votos, por exemplo com contadores distribuídos por assembleias eleitorais, assim como permitir redundância, o protótipo considera a possibilidade de existirem diversos contadores.

Deste modo o protótipo permite analisar o percurso de um voto desde o momento em que um eleitor se dirige à mesa de voto (no caso maximalista) até que esse voto chega aos contadores. A figura abaixo ilustra o modelo de um sistema de votação constituído por dois recintos, sendo que um desses recintos é constituído por duas mesas (m), duas máquinas de registo (r) e uma urna (u), e o outro recinto é constituído por duas mesas (m), uma máquina de registo (r) e uma urna (u). O modelo considera ainda a existência de dois contadores a operar de forma redundante.

¹¹⁵ Ver capítulo dedicado à questão da caixa negra.



Característica técnicas do protótipo

O protótipo foi desenvolvido utilizando a plataforma TurboGears. Esta plataforma permite o desenvolvimento de aplicações do tipo cliente-servidor baseadas em servidores WWW e clientes *browser*. A plataforma foi desenvolvida em Python e assenta no estilo arquitectural *Model-View-Control*. No lado do cliente (*browser*) é ainda utilizado código JavaScript. Para concretizar os modelos foi utilizada uma base de dados SQLITE. Para permitir a visualização dos modelos foi ainda utilizado o GraphViz, software de visualização de grafos, e o yapgb (*Yet Another Python GraphViz Binding*), para a geração dos grafos de ligações entre os componentes do sistema. Finalmente, de modo a facilitar a interacção entre cliente e servidor, que durante a especificação dos modelos quer durante a simulação, foi utilizada tecnologia AJAX.

Funcionalidades do protótipo

O protótipo implementa essencialmente quatro funcionalidades:

- Definição do modelo do sistema de votação - Permite especificar dinamicamente que tipos de componentes constituem o sistema de votação, que número de componentes é utilizado, assim como são interligados esses componentes;

- Definição de contadores - Estes contadores constituem o elemento fundamental sobre o qual a auditoria proactiva se concretiza. Um contador revela informação actual sobre o estado de um determinado componente do sistema de votação electrónica, por exemplo qual o número de votos que já foram entregues numa urna. A auditoria proactiva permite em cada instante analisar o estado de um contador, avaliar a evolução do contador e confrontar o estado desse contador com os estados de outros contadores pertencentes a outros componentes do sistema, permitindo dessa forma cruzar dados;
- Definição de regras - Uma regra permite estabelecer uma relação entre contadores de um ou de vários componentes. Por exemplo, uma regra que se aplica à mesa de voto é que o contador “número de votos autorizados” somado ao contador “número de votos não autorizados” tem que ser igual ao contador “número de registo de votantes”. No seu conjunto, estas regras permitem estabelecer três propriedades fundamentais do voto electrónico: Singularidade, Integridade do Voto e Integridade do Sistema;
- Operação sobre os contadores e visualização de resultados - Basicamente, esta funcionalidade destina-se a estudar dinamicamente o funcionamento de um sistema de votação electrónica, por via da verificação das regras previamente estabelecidas. É não só possível ao operador do simulador proceder à verificação e entrega de votos como também simular a ocorrência de falhas, como a perda de um voto ou a duplicação de um voto num componente.

Definição de modelos

O protótipo permite armazenar diferentes modelos na base de dados. Cada modelo corresponde a um processo de votação caracterizado por:

- Nome da votação;
- Tipo de modelo (maximalista, intermédio ou minimalista);
- Quantidade e nomes dos recintos de votação;
- Quantidades e nomes das mesas, máquinas de registo e urnas (maximalista); Quantidades e nomes das mesas e quiosques de votação (intermédia); Quantidades e nomes dos quiosques de votação (minimalista);
- Quantidades e nomes dos contadores definidos para cada componente.

A figura abaixo ilustra a especificação pelo operador dos componentes do modelo.

votacaoMaximalista	aa,freguesiaB,freguesiaC	Maximilista	▼
freguesiaA	mesas	registos	urnas
freguesiaB	mesas	registos	urnas
freguesiaC	mesas	registos	urnas
contadores		Criar	

Recinto freguesiaA

mesaA1	▼ ->	registoA	▼	continuar	▼
mesaA2	▼ ->	registoA	▼	continuar	▼
registoA	▼ ->	urnaA	▼	continuar	▼
urnaA	▼ ->	contador1	▼	continuar	▼
urnaA	▼ ->	contador2	▼		▼

Recinto freguesiaB

mesaB	▼ ->	registoB	▼	continuar	▼
registoB	▼ ->	urnaB	▼	continuar	▼
urnaB	▼ ->	contador1	▼	continuar	▼
urnaB	▼ ->	contador2	▼		▼

Recinto freguesiaC

mesaC	▼ ->	registoC	▼	continuar	▼
registoC	▼ ->	urnaC	▼	continuar	▼
urnaC	▼ ->	contador1	▼	continuar	▼
urnaC	▼ ->	contador2	▼		▼

Enviar

A figura abaixo ilustra a especificação de ligações entre componentes do modelo.

Definição de contadores

Os contadores são criados conjuntamente com os restantes componentes do modelo. A figura abaixo ilustra a forma como os contadores podem ser visualizados e manipulados pelo operador do simulador. Neste caso concreto observa-se que o recinto 1 tem 2 mesas e que cada mesa tem 2 contadores: “votantes autorizados” e “votantes negados”. Os sinais + e - que aparecem junto de cada contador permitem ao operador manipular o estado do contador, simulando por exemplo a perda ou o aparecimento inusitado de um voto registado.

- ◆ **Recinto rec_1_max**
 - Mesas do recinto rec_1_max**
 - ◊ m_1_max
 - votantes autorizados: - 2 +
 - votantes negados: 0 +
 - ◊ m_2_max
 - votantes autorizados: 0 +
 - votantes negados: 0 +
 - Registos do recinto rec_1_max**
 - ◊ r_1_max
 - votos registados: 0 +
 - ◊ r_2_max
 - votos registados: - 2 +
 - Urnas do recinto rec_1_max**
 - ◊ ur_1_max
 - votos depositados: - 2 +

Definição de regras

A definição de regras é crucial para permitir simular e analisar o funcionamento do sistema de votação electrónica. Uma vez que a existência de múltiplos componentes pode levar a erros na criação de regras, o protótipo utiliza dois filtros que reduzem as opções em cada selecção: filtro de ligação e filtro de recinto. Ao utilizar o filtro de ligação, a escolha dos operandos da regra é limitada aos operandos de componentes que estão ligados entre si; por exemplo, uma máquina de votação que está ligada a uma urna. Ao utilizar o filtro por recinto, a escolha dos operandos é limitada aos componentes que estão no mesmo recinto. em todo o caso é sempre possível utilizar regras globais, por exemplo uma regra que especifique que o número de votos entregues em todas as urnas de todos os recintos tem de ser igual ao total de votos contados.

As regras assumem a seguinte forma:

terminar := {}

operador := + | - | > | < | == | != | AND | OR | terminar

componente := Mesa | Registo | Urna | QuiosqueInt | QuiosqueMin | Contador

regra := componente(cont) operador componente(cont) operador | regra.

As regras são introduzidas no simulador da forma ilustrada na figura abaixo. Observe-se que é possível associar a cada regra um pequeno texto explicativo.

Adicionar uma regra

Por ligação ▾

Mesa: m_2_max ▾	votantes autorizados ▾	igual ▾
Registo: r_2_max ▾	votos registados ▾	igual ▾
Urna: ur_1_max ▾	votos depositados ▾	Terminar Regra ▾

Descrição

Verifica a integridade entre uma mesa, registo e urna que estão ligados entre si. ver grafo.

Criar

As regras são permanentemente avaliadas pelo simulador, que informa o operador através da interface indicada abaixo. Observe-se à esquerda a indicação do estado da regra (verde

Regras

Estado	Descricao	Regra
Estado	Verifica problemas entre as mesas e os registos do recinto rec_1_max.	votantes autorizados de Mesa m_2_max mais votantes autorizados de Mesa m_1_max e igual a votos registados de Registo r_2_max mais votos registados de Registo r_1_max
Estado	Verifica problemas entre os registos e a urna do recinto rec_1_max.	votos registados de Registo r_1_max mais votos registados de Registo r_2_max e igual a votos depositados de Urna ur_1_max

- válida; vermelho - inválida), mais à direita o texto explicativo da regra e, do lado direito, uma descrição formal da regra num formato que se aproxima da linguagem natural.

Discussão

Um dos aspectos interessantes do protótipo que foi desenvolvido é permitir a especificação e análise de regras a aplicar aos diversos componentes de um sistema de votação electrónica, independentemente da maior ou menor complexidade desse sistema. Naturalmente, observa-se que quanto mais complexo for o sistema do ponto de vista arquitectural (maximalista), mais regras podem ser especificadas e consequentemente detalhes mais finos da operacionalidade do sistema podem ser avaliados. As experiências que foram realizadas com o simulador permitiram ganhar sensibilidade a este problema, já devidamente discutido no capítulo dedicado à questão da caixa negra.

Outro aspecto importante a considerar é que o simulador permite facilmente identificar a ocorrência de problemas no sistema de votação. Certos tipos de problemas, como sejam as falhas de componentes, erro humano ou sabotagem podem ser facilmente detectados pela análise dos contadores. A auditoria proactiva permite ainda facilmente identificar em que componente ocorreu o problema e eventualmente isolar esse componente do sistema ou mesmo substituí-lo por um novo componente.

IDENTIDADE DIGITAL E VOTO ELECTRÓNICO

Pedro Antunes

O voto electrónico relaciona-se com a problemática da identidade digital¹¹⁶ em duas vertentes distintas: registo eleitoral e segurança do voto. Iremos analisar cada um destes problemas separadamente.

Parece ser consensual, nos diversos estudos até hoje realizados, que o registo eleitoral é crítico num sistema de votação electrónica, num grau superior ao existente numa votação tradicional. Diversas razões concorrem para esta situação. Por um lado, algumas vantagens do voto electrónico, como por exemplo a possibilidade de votar em qualquer lugar, só são possíveis se o registo eleitoral também for electrónico, possibilitando a distribuição e actualização dinâmica dos registos dos eleitores que numa eleição já exerceram o seu direito de voto, de modo a assegurar o princípio de que apenas podem votar os eleitores que têm esse direito, e de que o podem exercer uma única vez numa eleição.

Por outro lado, se admitirmos que o registo eleitoral pode ser defraudado, por exemplo permitindo que um eleitor seja registado diversas vezes, devemos também admitir que num sistema de votação electrónica será mais fácil que esse eleitor realmente exerça essa fraude. Por exemplo, no caso da votação pela Internet, não existem restrições físicas ao voto em locais geograficamente distantes, nem existe verificação pessoal da identidade do eleitor. Outro exemplo considera a possibilidade de utilizar o registo de um eleitor que já morreu mas que não foi removido do registo eleitoral, que é mais uma vez bastante facilitado no caso de votação remota.

Esta questão, de roubo, usurpação ou forja de uma identidade com o objectivo de quebrar o direito e a unicidade do voto é bastante agravada com a possibilidade de voto pela Internet, já que este modo de votação remove barreiras geográficas e temporais, e elimina o controlo cara-a-cara do processo eleitoral tradicional.

Um exemplo simples mas demonstrativo de que as barreiras são menores é que num voto pela Internet um eleitor do sexo masculino pode usurpar a identidade de uma eleitora do sexo feminino, algo que não nos parece tão fácil de realizar no sistema de votação tradicional. Outro exemplo que demonstra a complexidade do voto pela Internet é a possibilidade de um mesmo votante, por via da compra de votos, poder realizar sucessivas votações, algo que no processo tradicional também não se nos afigura fácil, pelo menos em grande escala.

¹¹⁶ APDSI (2007). *A Identidade Digital*, Actividade nº 1045, Lisboa, Fevereiro.

Dos exemplos aqui apresentados podemos concluir que existem duas forças de sinal contrário relacionadas com a identidade digital e o registo eleitoral: uma força relacionada com o aumento da flexibilidade (espacial, temporal) dos eleitores, levando à adopção do registo eleitoral electrónico, distribuído e dinâmico; e outra, decorrente da adopção de meios electrónicos, que reduzem o controlo e as barreiras à fraude eleitoral. Note-se que diversos estudos indicam que o recurso a mecanismos biométricos permite conciliar este jogo de forças. No entanto, a maioria dos estudos consultados indica que a utilização de mecanismos biométricos ainda não está suficientemente desenvolvida, continuando em investigação, e levanta diversas questões éticas e legais, designadamente quanto ao registo e utilização de dados biométricos numa escala nacional e mesmo internacional.

Assumindo assim que, do ponto de vista tecnológico, ainda não é possível contrariar o jogo de forças acima mencionado, pensamos ser fundamental estudar e desenvolver duas outras abordagens, que consideramos complementares.

A primeira abordagem considera fundamental desenvolver mecanismos e processo sociais que permitam o controlo, realizado por pessoas, do registo eleitoral, no que se refere à inscrição, actualização e remoção de eleitores desses registos, assim como o controlo humano da utilização desses registos durante as eleições, designadamente no processo de verificação do direito de voto e listagem dos eleitores que já exerceram esse direito.

A segunda abordagem considera fundamental aumentar a percepção, capacidade de avaliação, e eventualmente o limiar de aceitação da sociedade, sobre os riscos envolvidos na adopção do registo eleitoral electrónico. Ou seja, cabe à sociedade, de forma esclarecida e transparente, identificar e adoptar o grau de risco que considerar mais aceitável e conveniente, não devendo o ónus dessa decisão ser remetido para os fornecedores de sistemas eleitorais, nem para os peritos informáticos que eventualmente sejam envolvidos na utilização, inspecção e certificação desses sistemas.

Iremos agora analisar a relação entre identidade digital e segurança do voto. Esta discussão assume que os princípios da unicidade e direito de voto, relacionados com o registo eleitoral já analisado acima, se encontram assegurados. Sendo assim, as questões a discutir relacionam-se com a possibilidade de quebra do anonimato, da privacidade, e da modificação ou eliminação dos votos individualmente expressos pelos eleitores.

Julgamos que outros problemas relacionados com a votação electrónica, como por exemplo as falhas de contagem, robustez do sistema ou os problemas de usabilidade, não se relacionam directamente com a identidade digital e portanto não serão analisados.

Para facilitar a discussão, iremos separar as questões em dois temas distintos: anonimato e privacidade, num âmbito mais social; e modificação e eliminação de votos, que apresentam um contexto mais tecnológico.

O anonimato é um dos requisitos fundamentais de um sistema eleitoral livre e democrático e destina-se a garantir que não é possível associar a identidade de um eleitor ao

voto por ele produzido. A relação entre esta propriedade e a identidade digital é negativa, no sentido em que num sistema de votação o que se pretende assegurar é a não-identidade digital.

Sendo verdade que num sistema de votação tradicional - em urna - podem existir casos extremos de quebra de anonimato (por exemplo, quando apenas um eleitor exerce o seu direito de voto), a sociedade em geral considera que a urna permite assegurar o anonimato do eleitor de forma transparente, i.e. todos os eleitores podem verificar essa propriedade. No entanto, no caso da votação electrónica a questão é bastante mais complexa e menos transparente.

Em primeiro lugar porque existem diversas arquitecturas de sistemas de votação electrónica que não utilizam uma urna, não sendo portanto transparente a dissociação entre eleitor e voto, por estar escondida por detrás de uma barreira tecnológica. Em segundo lugar, porque os sistemas electrónicos de votação permitem registar informação muito detalhada sobre os utilizadores e as acções que realizam no sistema.

A este respeito, há que referir que diversos estudos indicam que é possível o cruzamento de dados entre diversos dispositivos electrónicos por forma a associar os votos aos eleitores, quebrando dessa forma o anonimato. Este problema é técnico mas levanta problemas sociais, cabendo a quem desenvolve estes sistemas o ónus de demonstrar - para além da dúvida razoável - que não é possível associar votos a eleitores.

Finalmente, porque muitos mecanismos destinados a assegurar o anonimato, designadamente mecanismos criptográficos, oferecem riscos estimados estatisticamente e, portanto, não absolutos; agravados pelo conhecimento da sociedade de muitas situações em que estes mecanismos foram quebrados. Reforçando este comentário, num sistema de votação electrónica, e ao contrário de outros sistemas, é possível aplicar todo o esforço na quebra de um único voto (por exemplo o voto do Presidente da República), sendo essa quebra suficiente para desacreditar todo o sistema perante a sociedade.

A questão da privacidade está intimamente associada ao voto pela Internet. De acordo com os diversos estudos sobre voto pela Internet que foram por nós analisados, quer o ambiente empresarial quer o ambiente familiar não oferecem condições para assegurar a privacidade dos eleitores.

No caso do ambiente empresarial, porque os computadores utilizados para votar se encontram normalmente associados a um único funcionário e são geridos de acordo com as regras da organização, que pode, mesmo de forma não intencional, adoptar princípios e utilizar mecanismos de segurança e controlo que quebrem a privacidade do acto eleitoral. O ambiente familiar apresenta também diversas restrições à privacidade, possibilitando o chamado “voto familiar”: restrições físicas, porque o computador se encontra num espaço partilhado; restrições de acesso, porque o computador pode ser controlado por um ele-

mento familiar; e restrições de poder, quando alguns elementos exercem poder sobre os restantes membros da família.

É curioso no entanto observar a existência de alguns mecanismos que permitem atenuar estes problemas, por forma a torná-los aceites pela sociedade, designadamente a possibilidade de votar sucessivamente, incluindo o voto presencial tradicional, e a declaração sob compromisso de honra de que o voto foi exercido em total liberdade e privacidade. No é no entanto claro que estes mecanismos resolvam completamente o problema. Podemos admitir, por exemplo, que o voto sucessivo possa ser restringido por pressão familiar ou por algum agente colocado à porta de casa do votante.

Em resumo, a questão da privacidade no voto pela Internet depende apenas da percepção social dos riscos associados, da definição dos limites mínimos de privacidade, e da legislação necessária para assegurar o cumprimento legal desses limites.

Iremos finalmente discutir o tema da modificação e eliminação de votos, que apresentam um contexto mais tecnológico. Admite-se que a votação electrónica em recinto fechado (mesas eleitorais) possa ser assegurada por uma infra-estrutura tecnológica dedicada a suportar esse processo, com restrições de acesso pelo exterior, reduzindo assim significativamente os riscos de ataque aos votos dos eleitores. Sendo assim, a situação mais interessante de analisar será a que permite a votação em qualquer lugar, designadamente através da Internet.

A modificação ou eliminação de votos configura um roubo de identidade, no sentido em que retira expressamente ao eleitor o direito de manifestar a sua opinião. No contexto da votação pela Internet, a modificação ou eliminação de votos é possível através de diversos mecanismos tecnológicos, que atacam o computador utilizado pelo eleitor para produzir o seu voto e a rede utilizada para transmitir esse voto.

Quer os computadores quer as redes públicas actuais são muito vulneráveis a este tipo de ataques, o que é facilmente comprovado pela quantidade de novos vírus, Cavalos de Tróia e Ataques de Pesca (*phishing*) divulgados pelas empresas que identificam e combatem estes tipos de ataque. Apesar da existência destas organizações, observamos que o seu modelo de funcionamento baseia-se no combate a posteriori, após a identificação de novos tipos de ataque, o que é desadequado num contexto de votação electrónica já que, sendo uma votação normalmente circunscrita no tempo, a identificação e o combate podem não ser efectuados em tempo útil.

Uma alternativa que tem sido ponderada para aumentar a resistência a estes ataques consiste em combinar os componentes inseguros (computadores e redes) com componentes seguros (e.g. dispositivos de leitura de cartões, já discutidos num capítulo anterior). Parecendo promissora, esta solução levanta no entanto problemas económicos e logísticos que podem reduzir a universalidade da votação pela Internet.

Finalmente, outra questão a considerar é que existe normalmente uma relação inversa entre segurança e usabilidade, dado que a definição de mecanismos e procedimentos de prevenção de ataques (e.g., requerendo actualizações constantes dos sistemas operativos) mais seguros normalmente reduz a facilidade de utilização dos sistemas, o que num contexto de votação electrónica tem especial impacto dada a grande diversidade de capacidades dos utilizadores.

SUSPEIÇÕES E TEORIAS DA CONSPIRAÇÃO

Pedro Antunes

Os sistemas de votação electrónica parecem atrair um número inusitado de comentários negativos, suspeições, paranóias e teorias da conspiração. Vale a pena analisar esta questão porque ela tem contribuído fortemente para dificultar o desenvolvimento e adopção desta tecnologia.

Serve igualmente esta análise para evidenciar os riscos sociais e financeiros associados ao desenvolvimento destes sistemas. As empresas que desenvolvem esta tecnologia tendem naturalmente a preocupar-se com problemas mais imediatos e tangíveis - planos, arquitecturas, sistema operativo, algoritmos de cifra, funcionalidades, interface com os utilizadores, erros de software, etc. - descurando as questões mais intangíveis - suporte do estado, grau de confiança dos eleitores, credibilidade da empresa, mitigação dos riscos, abertura aos auditores, abertura à sociedade.

Deve dizer-se que grande parte dos argumentos que questionam os sistemas de votação electrónica se baseiam na observação de que actualmente não existem meios eficazes para combater os riscos de sabotagem. Um estudo recente realizado nos EUA¹¹⁷ concluiu que todos os sistemas de votação electrónica que foram analisados (1) tinham falta de controlos de integridade; (2) apresentavam vulnerabilidades que poderiam facilmente ser exploradas por código malicioso; e (3) falharam na adopção de políticas e processos efectivos para lidar com esses problemas.

Um exemplo concreto desta situação foi publicado no boletim electrónico The Register¹¹⁸, reportando que uma vulnerabilidade crítica no sistema de votação da Diebold permitia instalar software malicioso nas máquinas de registo directo do voto. Um outro exemplo aconteceu na Holanda, tendo sido demonstrado que os votos introduzidos nas máquinas de registo directo do voto podiam ser interceptados a cerca de 20-30 metros de distância (via rádio)¹¹⁹.

A publicidade dada nos meios de comunicação a vulnerabilidades nos sistemas de votação electrónica têm tido um impacto significativo. Dados referidos no *New York Times*

¹¹⁷ Jennifer L. Brunner (2007). Ohio Secretary of State, Project E V E R E S T: Evaluation and Validation of Election Related Equipment, Standards and Testing, December.

¹¹⁸ http://www.theregister.com/2006/05/14/diebold_e-voting_flaw/. Acedido em 2/4/2008.

¹¹⁹ http://www.theregister.co.uk/2006/10/31/dutch_votingmachines_inadequate/. Acedido em 2/4/2008.

referem que o negócio das máquinas de votação electrónica da Diebold passaram de um volume de 195 milhões USD em 2006 para 61 milhões USD em 2007¹²⁰.

Dado o panorama geral, são de certa forma credíveis algumas teorias conspirativas em que ataques organizados e em grande escala permitiriam modificar o software dos sistemas de votação electrónica por forma a silenciosamente modificarem o sentido do voto dos eleitores ou publicamente destruírem a credibilidade de um país. Diversas organizações activistas, como a fundação Holandesa “*We do not trust voting computers*,”¹²¹ ou a americana “*Voters Unite*”¹²² veiculam estas suspeições e teorias conspirativas.

Pelo menos até hoje, não há notícias deste tipo de ataques durante os processos eleitorais. Existe no entanto um registo vasto de outros tipos de problemas, normalmente associados a falhas de sistema e erro humano, que reduz o grau de confiança nesta tecnologia. A organização “*Voters Unite*” possui um registo de 1022 problemas ocorridos em 314 condados de 36 estados dos EUA, apenas relativamente às eleições ocorridas em 2006¹²³.

Não sendo possível, de forma credível, eliminar totalmente as vulnerabilidades dos sistemas de votação electrónica, tem emergido em diversos países um movimento a favor do comprovativo em papel, como forma de verificação e resolução de problemas. Um desses movimentos é o “Voto Seguro,”¹²⁴ organização informal brasileira que tem acompanhado de perto os problemas do sistema de voto electrónico instituído nesse país.

Uma das teorias conspirativas seria que um número reduzidos de pessoas - responsáveis máximos pelo desenvolvimento do sistema de votação - hipoteticamente se poderia coligar por forma a definir o resultado eleitoral. Uma possibilidade que foi considerada era a de que o então candidato Lula da Silva poderia não ser eleito por manipulação em grande escala dos votos¹²⁵. Ora sem comprovativos em papel seria praticamente impossível detectar tal conspiração.

Apesar de tal não ter acontecido, o problema de um sistema de votação ficar refém de um número reduzido de pessoas tem também alguma credibilidade e deve ser seriamente ponderado.

¹²⁰ M. Merced (2008) Diebold Receives a Takeover Offer. The New York Times. <http://www.nytimes.com/2008/03/03/>. Acedido em 12 de Maio de 2008.

¹²¹ <http://www.wijvertrouwenstemcomputersniet.nl/>.

¹²² <http://www.votersunite.org/>.

¹²³ Voters Unite (2007). E-Voting Failures in the 2006 Mid-Term Elections: A sampling of problems across the nation.

¹²⁴ <http://www.votoseguro.org/>.

¹²⁵ Mário jakobskind e Osvaldo Maneschy (2002). Burla Electrónica. Fundação Alberto Pasqualini.

O movimento “Voto Seguro” relata muitas situações em que o sistema brasileiro falhou, em menor escala, e onde o comprovativo em papel poderia, pelo menos, permitir identificar os problemas ocorridos.

A lei N.º. 10.408, de 10 de Janeiro de 2002 veio consagrar o comprovativo em papel no Brasil, respondendo assim a muita polémica que tinha sido levantada. A lei N.º. 10.740/03 de 1 de Outubro de 2003 veio no entanto alterar essa situação, tendo eliminado o comprovativo em papel¹²⁶. Uma explicação possível para esta alteração poderá ser não se saber exactamente o que fazer quando a contagem dos votos electrónicos não for igual à dos comprovativos em papel. Deverá prevalecer a contagem em papel? Mas esta não está também sujeita a erros e fraude? (aliás reconhecidamente elevada no sistema de voto tradicional no Brasil¹²⁷). Deverá prevalecer a contagem electrónica? Mas nesse caso não será muito útil ter uma contagem em papel.

A situação paradoxal a considerar é que a adopção do comprovativo em papel pode servir para credibilizar o voto electrónico - se não ocorrerem problemas - mas também poderá servir para definitivamente levar ao seu abandono - se ocorrerem problemas e não existirem soluções para os resolver e explicações credíveis sobre os fenómenos ocorridos.

¹²⁶ <http://www.votoseguro.org/>.

¹²⁷ Amílcar Brunazo Filho. A breve história do voto eletrônico do Brasil.

MAIS PROPRIEDADES

Pedro Antunes

O número de propriedades já identificadas neste documento e relacionadas com sistemas de votação electrónica é muito grande. Mesmo assim, podem sempre ser definidas novas propriedades, geralmente derivadas de visões mais complexas ou mais dirigidas para determinados problemas. Neste capítulo apresentamos algumas dessas propriedades.

Democracia

Esta propriedade surge em diversa literatura relativa aos sistemas de votação electrónica, normalmente servindo o objectivo de integrar as seguintes propriedades numa única: Autenticidade, Singularidade, Anonimato e Integridade dos Votos. Numa perspectiva mais abrangente, pode-se considerar que a propriedade integra todas as propriedades e requisitos inerentes à democracia (ver capítulo introdutório sobre propriedades).

Conveniência

Um sistema de votação electrónica só será útil se permitir aos eleitores exercerem o seu direito de voto de forma rápida, com o mínimo de tecnologia, e sem operações demasiado complexas, como por exemplo utilizar palavras-chave com regras muito exigentes sobre o número, o tipo e a variedade de caracteres que as constituem.

Usabilidade

Trata-se de uma especialização da Conveniência especificamente desenvolvida para o domínio do software. De acordo com a Directiva Comunitária 90/270/ECC¹²⁸, por usabilidade entende-se a concepção, desenvolvimento, selecção ou modificação de software assegurando:

- Que é adequado para a tarefa;
- Que é fácil de usar e, quando apropriado, adaptado (ou adaptável) ao conhecimento e experiência dos utilizadores (que no caso em questão abrange qualquer pessoa maior de idade);

¹²⁸ European Community Health and Safety directive 90/270/ECC, Minimum Health and Safety Requirements for Work with Display Screen Equipment.

- Oferece retorno adequado sobre o seu desempenho aos utilizadores;
- Mostra informação num formato e segundo um ritmo ajustado aos utilizadores;
- Está conforme os princípios da ergonomia.

Acessibilidade

Esta propriedade destina-se a assegurar que o sistema e a informação gerida pelo sistema são acessíveis a utilizadores com necessidades especiais. O Governo Português, através da Resolução do Conselho de Ministros 155/2007 de 2 de Outubro de 2007, determinou um conjunto mínimo de características que devem ser aplicadas aos sistemas de informação da administração pública, tendo por base as recomendações do consórcio W₃C¹²⁹. Os equipamentos de votação enquadram-se naturalmente neste contexto.

Flexibilidade

Um sistema de votação electrónica deve permitir uma diversidade de processos de votação (e.g., eleição legislativa e referendo), de questões colocadas aos eleitores, formatos de apresentação e métodos de recolha das escolhas dos votantes¹³⁰.

Mobilidade

O sistema de votação electrónica deve evitar ou eliminar restrições relativas ao local onde o eleitor pode votar. Mais recentemente, esta propriedade tem sido alargada por forma a considerar o uso de dispositivos móveis no processo de votação.

Transparência

Os sistemas de votação electrónica devem permitir que os eleitores compreendam quer o processo eleitoral quer o funcionamento interno do próprio sistema de votação. Esta propriedade está intimamente ligada aos conceitos de caixa negra, caixa de vidro e confiança desenvolvidos anteriormente em capítulo próprio.

Viabilidade

¹²⁹ <http://www.w3.org/>.

¹³⁰ Cranor, L. (1996) "Electronic Voting." ACM Crossroads, 2(4).

Os sistemas de votação electrónica devem ser economicamente viáveis, considerando uma relação custo/benefício face ao processo tradicional de votação em papel¹³¹.

¹³¹ Gerk, Ed, (2001) “Voting Systems: From Art to Science”, Voting Technology Conference, Caltech/MIT.

AINDA MAIS PROPRIEDADES: A VISÃO DO CONSELHO DA EUROPA

João Ferreira Dias e Domingos Magalhães

É pacífica a opinião de que os sistemas de votação electrónica devem cumprir um conjunto de princípios, propriedades e requisitos que dizem respeito ao processo eleitoral no geral e ao acto de votar em especial.

São princípios e regras de direito eleitoral a oficiosidade, obrigatoriedade, permanência e unicidade do recenseamento eleitoral, o sufrágio directo, secreto e universal, a liberdade e a unicidade do voto.

No que respeita ao processo eleitoral é imperativo garantir: a transparência, a neutralidade da condução, a simplicidade e a fiscalização do processo.

No quadro seguinte resume-se a recomendação do Conselho da Europa¹³² (COE), que constitui o documento de referência sobre os requisitos de sistemas de votação electrónica.

Princípios legais

I - Universalidade do sufrágio		
1	A interface de votação deve ser compreensível e facilmente utilizável.	The voter interface of an e-voting system shall be understandable and easily usable.
2	A eventual necessidade de registo do votante não deve impedir ou dificultar a participação na votação.	Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.
3	O sistema deve ser concebido para maximizar as oportunidades das pessoas com deficiência.	E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.
4	Os canais de votação remota devem ser complementares, salvo se forem universalmente acessíveis.	Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

¹³² Rec(2004)II de 30/9.

II - Igualdade no sufrágio		
5	Para cada sufrágio, um votante só pode depositar na urna um único voto.	In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.
6	O sistema deve impedir a deposição na urna de mais do que um voto por votante e por sufrágio, independentemente do número de canais de votação.	The e-voting system shall prevent any voter from casting a vote by more than one voting channel.
7	Todo o voto depositado na urna deve ser contado e deve-o ser uma única vez.	Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.
8	Quando diferentes canais são utilizados, deve ser garantido um método seguro e confiável de agregação e contagem de todos os votos.	Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

III - Liberdade no sufrágio		
9	A organização do sufrágio deve garantir a livre formação e expressão da opinião do votante e, onde requerido, o exercício pessoal do direito de voto.	The organisation of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.
10	O mecanismo de orientação do votante no processo de votação deve prevenir a votação precipitada ou irreflectida.	The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.
11	Os votantes devem poder alterar a sua escolha ou interromper o processo a todo o momento antes da deposição do voto na urna.	Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.
12	Durante a votação o sistema não deve permitir a influência ou manipulação sobre o votante.	The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.
13	O sistema deve permitir ao votante o exercício da não preferência sobre as opções propostas, por exemplo através do voto em branco.	The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.
14	O sistema deve indicar claramente ao votante quando é que o voto foi considerado como depositado e quando é o processo terminou.	The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.
15	O sistema deve impedir a alteração do voto uma vez depositado na urna.	The e-voting system shall prevent the changing of a vote once that vote has been cast.

IV – Secretismo no sufrágio		
16	A organização do sufrágio deve excluir em qualquer etapa do processo, designadamente na autenticação do votante, tudo o que faça perigar o secretismo do voto.	E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.
17	O sistema deve garantir que os votos depositados, na urna ou na fase de contagem, permaneçam anónimos e que seja impossível restabelecer o elo entre o voto e o votante.	The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
18	O sistema deve ser concebido para impedir a associação dos resultados dos votos esperados com os votantes individualmente considerados.	The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.
19	O sistema deve assegurar que a informação necessária durante o processo seja utilizada para quebrar o secretismo do voto.	Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

Salvaguardas procedimentais

I – Transparência		
20	Os estados devem tomar medidas que assegurem que os eleitores compreendam e tenham confiança nos sistemas de votação electrónica em uso.	Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.
21	A informação sobre o funcionamento do sistema deve ser pública.	Information on the functioning of an e-voting system shall be made publicly available.
22	Os eleitores devem ter a oportunidade de praticar qualquer novo método de votação, antes e separadamente do exercício de votação real.	Voters shall be provided with an opportunity to practise any new method of e-voting before, and separately from, the moment of casting an electronic vote.
23	Os observadores, no quadro legal, devem poder observar e comentar o sistema de votação electrónica, incluindo o estabelecimento dos resultados.	Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.

II - Verificação e responsabilização		
---	--	--

24	Os componentes do sistema devem poder ser abertos, pelo menos para as autoridades eleitorais, para serem verificados e certificados.	The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
25	Desde antes da introdução do sistema e depois numa base periódica, uma entidade independente, indicada pelas autoridades eleitorais, deve verificar que o sistema funciona correctamente e que as medidas de segurança foram tomadas.	Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.
26	Deve existir a possibilidade de recontagem. As funcionalidades que possam influenciar a correcção dos resultados devem ser verificáveis.	There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.
27	O sistema não deve impedir na prática a repetição parcial ou total duma eleição.	The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

	III - Operacionalidade e segurança	
28	As autoridades do estado devem assegurar a fiabilidade e segurança dos sistemas de votação electrónica.	The member state's authorities shall ensure the reliability and security of the e-voting system.
29	Todas as medidas possíveis devem ser tomadas para evitar a possibilidade de fraude ou intervenção não autorizada que afecte o sistema durante o processo de votação.	All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.
30	O sistema deve assegurar a disponibilidade dos serviços durante o processo de votação, face a interrupções, avarias, etc.	The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.
31	Antes de qualquer sufrágio, a autoridade eleitoral deve assegurar que o sistema de votação electrónica é genuíno e funciona bem.	Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.
32	Só as pessoas indicadas pela autoridade eleitoral terão acesso, segundo regras claras, à infraestrutura central, aos servidores e aos dados da eleição. As actividades técnicas críticas devem ser realizadas por equipas de pelo menos 2 pessoas, cuja composição deverá ser mudada regularmente. Na medida do possível, tais actividades devem ser realizadas fora dos períodos eleitorais.	Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.

33	Quando uma urna é aberta, qualquer intervenção autorizada deve ser efectuada por equipas de pelo menos 2 pessoas, ser objecto dum relatório, ser acompanhada pelos representantes da autoridade eleitoral e de qualquer observador eleitoral.	While an electronic ballot box is open, any authorised intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers.
34	O sistema deverá garantir a disponibilidade e a integridade dos votos. Também deve garantir a confidencialidade dos votos e mantê-los selados até ao processo de contagem. Se armazenados ou comunicados fora de ambientes controlados, os votos devem ser cifrados.	The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.
35	Os votos e a informação do eleitor permanecerão selados enquanto puderem ser associados. A informação de autenticação deverá estar separada da decisão do eleitor até uma etapa predefinida do processo.	Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

Padrões operacionais

I - Notificação		
36	As provisões legais que governam uma eleição deverão requerer calendários claros para todas as fases do processo.	Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.
37	Um voto electrónico não pode ser descarregado antes da notificação da eleição. Quanto ao voto remoto, o período será definido e tornado conhecido bem antes do início do processo de votação.	The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.
38	Antes do início da votação, os eleitores serão informados de forma clara e simples, da forma como o processo está organizado e da sequência das etapas para participar e votar.	The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organised, and any steps a voter may have to take in order to participate and vote.

I - Notificação		
39	Haverá um registo dos eleitores, actualizado regularmente. No mínimo, o eleitor deve poder consultar a informação sobre si e solicitar correções.	There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections.

40	Deve ser considerada a possibilidade de criação de um ficheiro electrónico de eleitores com um mecanismo de registo em linha e, se aplicável, de votação electrónica. Se a participação no voto electrónico exigir uma candidatura pelo eleitor e/ou etapas adicionais, deve ser considerado um procedimento electrónico.	The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.
41	Nos casos em que existe uma sobreposição dos períodos de registo e de votação, devem ser tomadas as providões necessárias para a adequada autenticação.	In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.

III - Candidaturas		
42	Deve ser considerada a possibilidade de registo em linha dos candidatos.	The possibility of introducing online candidate nomination may be considered.
43	A lista de candidatos gerada e divulgada electronicamente deve ser também publicitada por outros meios.	A list of candidates that is generated and made available electronically shall also be publicly available by other means

III - Candidaturas		
44	Nos casos em que a votação remota tem lugar em simultâneo com a votação nas assembleias de voto, o sistema deve evitar que um votante vote mais do que uma vez por sufrágio.	It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once
45	A votação remota pode começar ou acabar mais cedo que a votação em assembleia de voto, mas não deve continuar após o seu fecho.	Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.
46	Para cada canal de votação electrónica, deve existir apoio e orientação aos eleitores. No caso da votação remota, esse apoio deve existir também através de canais alternativos.	For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

47	Deve haver igualdade na forma de apresentação das opções de voto no dispositivo utilizado para a recolha do voto.	There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.
48	A urna electrónica não deve dar informações sobre as opções em votação, salvo a estritamente necessária para a recolha do voto. O sistema não deve permitir mensagens que possam influenciar o eleitor.	The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.
49	Se existir informação sobre as opções em votação, esta informação deve ser apresentada com igualdade.	If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.
50	Antes de recolher o voto electrónico, o sistema deve alertar que se trata duma eleição real. No caso de testes, os participantes devem ser informados que não estão a participar numa votação real e, caso esses testes se realizem no período eleitoral, devem ser convidados a votar nos canais de votação apropriados.	Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.

IV - Votação		
51	O sistema de votação não deve dar uma prova da votação que indique o conteúdo do voto.	A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.
52	Num ambiente controlado, a informação do voto deve desaparecer do terminal utilizado logo que recolhido. Quando é emitido um voto em papel, o eleitor não deve poder mostrá-lo a outrem nem transportá-lo para fora da assembleia de voto.	In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.
53	O sistema não deve permitir o cálculo dos votos para cada opção, antes do fecho da urna. Os votos para cada opção em votação só devem ser difundidos no fim do período de votação.	The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.
54	O sistema deve impedir o processamento parcial que permita revelar as escolhas individuais dos votantes.	The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.

55	A descodificação eventualmente requerida para a contagem dos votos deve ser efectuada logo que exequível após o fecho do período de votação.	Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.
56	A autoridade eleitoral e qualquer observador devem poder participar na contagem dos votos.	When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.
57	O processo de contagem deve ser documentado com informação sobre as horas de início e de fim e as pessoas envolvidas.	A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.
58	No caso de irregularidades que possam afectar a integridade dos votos, esses votos devem ser registados como tal.	In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.

	VI - Auditoria	
59	O sistema deve ser auditável	The e-voting system shall be auditable.
60	As ilações dos processos de auditoria devem ser consideradas em futuros actos eleitorais.	The conclusions drawn from the audit process shall be applied in future elections and referendums.

Requisitos técnicos

	A - Acessibilidade	
61	Deve assegurar-se que os serviços relevantes disponíveis possam ser utilizados por todos os eleitores e, se necessário, providenciar diferentes meios de votação.	Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.
62	Os utilizadores devem ser envolvidos na concepção do sistema, particularmente na identificação de restrições e no teste da facilidade de utilização em cada etapa importante do processo de desenvolvimento.	Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.
63	Os utilizadores que o requeiram devem ter acesso, sempre que possível, a facilidades adicionais como interfaces especiais e assistência pessoal. Essas facilidades devem estar de acordo com as orientações da <i>Web Accessibility Initiative</i> (WAI).	Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).
64	No desenvolvimento de novos produtos deve ter-se em conta as exigências de compatibilidade com os já existentes, designadamente os que utilizam tecnologias para ajudar pessoas com deficiências.	Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.

65	A apresentação das opções de votação deve ser optimizada para o utilizador.	The presentation of the voting options shall be optimised for the voter.
----	---	--

B – Interoperabilidade		
66	Padrões aberto devem ser utilizados para assegurar a interoperabilidade de componentes e serviços técnicos possam ser assegurados por diversas fontes.	Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.
67	Actualmente, existe o padrão <i>EML-Election Markup Language</i> (disponível no sítio Web do Conselho da Europa), que deve ser utilizado sempre que possível. Contudo, a decisão da sua utilização cabe ao estado.	At present, the Election Markup Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this recommendation, and supporting documentation are available on the Council of Europe website.
68	Nas situações com requisitos específicos dos dados, um procedimento local deve ser utilizado. Isto permite ampliar ou reduzir a informação a fornecer, mantendo a compatibilidade com a versão genérica do EML. O procedimento recomendado é o uso de linguagens estruturadas e linguagens padrão.	In cases which imply specific election or referendum data requirements, a localisation procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.

C – Operação do sistema (para os sistemas central e do cliente em ambientes controlados)		
69	A autoridade eleitoral deve publicar a lista oficial do software utilizado. O estado pode excluir da lista software de protecção de dados por razões de segurança. Ao menos deve ser indicado o software usado, as versões, a data de instalação e uma breve descrição. Devem ser definidos procedimentos para a instalação regular de correcções e versões actualizadas do software de protecção. Deve ser possível a todo o momento verificar o estado de protecção do equipamento de votação.	The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.
70	Os responsáveis pela operação do equipamento devem estabelecer procedimentos de contingência. Qualquer sistema de cópias de segurança deve obedecer aos mesmos padrões e requisitos que o original.	Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.

71	Os recursos de cópias de segurança devem ser suficientes e em estado de prontidão para assegurar que o processo corra bem. As equipas associadas devem intervir oportunamente no quadro de procedimentos definidos pela autoridade eleitoral.	Sufficient backup arrangements shall be in place and be permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.
72	Os responsáveis pelos equipamentos devem ter definido procedimentos especiais que assegurem a satisfação dos requisitos durante o período de votação.	Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.
73	Antes de cada sufrágio, o equipamento deve ser testado e aprovado de acordo com protocolos definidos pela autoridade eleitoral, designadamente especificações técnicas. Os relatórios devem ser fornecidas à autoridade eleitoral.	Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.
74	Todas as operações técnicas devem obedecer a um protocolo formal. Todas as alterações substanciais nos equipamentos críticos devem ser notificadas.	All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.

	C – Operação do sistema (para os sistemas central e do cliente em ambientes controlados)	
75	O local onde se encontra o equipamento-chave deve ser considerado seguro e deve ser protegido, durante o período eleitoral, contra qualquer tipo de interferência e intrusão de pessoas não autorizadas. Nesse período deve existir um plano de contingência de catástrofes. Os dados de votação devem ser armazenados em local seguro.	Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.
76	Em caso de incidentes que ameacem a integridade do sistema, os responsáveis pela operação dos equipamentos devem informar imediatamente a autoridade eleitoral para a tomada de medidas. O nível de incidente a partir do qual deve ser informada a autoridade eleitoral deve ser definido antecipadamente.	Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.

	D – Segurança - I - Requisitos gerais (fases de pré-votação, votação e pós-votação)	
--	--	--

77	Devem ser tomadas medidas organizacionais para assegurar que os dados não são perdidos em caso de avaria ou falha.	Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.
78	O sistema deve garantir a privacidade dos votantes e dos registos armazenados ou comunicados.	The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.
79	O sistema deve ser sujeito a testes regulares para se assegurar que os componentes operam conforme as especificações técnicas.	The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.
80	O sistema deve restringir o acesso aos seus serviços apenas aos utilizadores autorizados e após autenticação da sua identidade.	The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.
81	O sistema deve proteger a informação de autenticação, para evitar o conhecimento, a modificação, a interceptação ou a utilização indevida, de parte ou da totalidade, dos dados. Em ambientes não controlados aconselha-se que a autenticação se baseie em mecanismos cifrados.	The e-voting system shall protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.
82	O sistema deve assegurar a identificação única dos eleitores e candidatos para prevenir a troca de identidades.	Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured
83	O sistema deve gerar dados de funcionamento detalhados e confiáveis para monitorização. O momento em que um processo gerou esse dados deve ser indicado. A autenticidade, disponibilidade e integridade dos dados devem ser mantidas.	E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.
84	O sistema deve sincronizar o relógio com fontes credíveis, para permitir a marcação do tempo nos registos de observação, auditoria e operação eleitoral.	The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.
85	A autoridade eleitoral tem a responsabilidade total pela garantia de conformidade com estas exigências da segurança, que serão avaliadas por entidades independentes.	Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies.

D – Segurança - II - Requisitos (fases de pré-votação)

86	A autenticidade, disponibilidade e integridade dos registos dos eleitores e as listas dos candidatos devem ser mantidas. A fonte dos dados deve ser autenticadas. As regras para a protecção dos dados devem ser respeitadas.	The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.
87	Deve ser assegurado o cumprimento dos prazos legais para as designações e a aceitação dos candidatos pela autoridade eleitoral.	The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.
88	Deve ser assegurado o cumprimento dos prazos legais no registo dos leitores nos respectivos cadernos.	The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

D – Segurança - III - Requisitos (fases de votação e pós-votação)		
89	Deve ser assegurada a autenticação e a integridade da comunicação dos cadernos eleitorais.	The integrity of data communicated from the pre-voting stage (e.g. voters' registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.
90	Deve ser assegurada a autenticidade da urna apresentada ao eleitor. No caso de votação electrónica remota o eleitor deve ser informado sobre os meios a utilizar para se assegurar que foi estabelecida uma ligação segura ao servidor oficial e que a urna apresentada é autêntica.	It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.
91	Deve ser assegurado que o voto foi recolhido dentro do prazo pré-definido.	The fact that a vote has been cast within the prescribed time limits shall be ascertainable.
92	Devem ser providenciados os meios necessários para garantir que o sistema de votação utilizado pelos eleitores está protegido contra influências que possam modificar o voto.	Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.
93	Informação residual sobre o voto, incluindo a imagem no ecrã, deve ser destruída após a recolha do voto. No caso de votação electrónica remota, o eleitor deve ser informado, sempre que possível, sobre como destruir o rasto do processo no dispositivo utilizado.	Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.
94	O sistema deve assegurar-se primeiro que quem quer votar tem capacidade eleitoral. Na votação remota o sistema deve autenticar o eleitor e assegurar que só deposita os votos nos sufrágios que lhe respeitam.	The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.
95	O sistema deve assegurar que a escolha do eleitor está representada no voto e que este é depositado na urna.	The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.

96	Encerrado o período de votação não será permitido a nenhum eleitor o acesso ao sistema de votação. Contudo, a urna continuará a aceitar votos electrónicos por um período de tempo suficiente para receber as comunicações em curso ou atrasadas.	After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.
----	---	---

D – Segurança - IV - Requisitos (fases pós-votação)		
97	Deve ser assegurada a autenticação da fonte e a integridade dos dados comunicados durante a fase de votação.	The integrity of data communicated during the voting stage (e.g. votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.
98	O processo de contagem dos votos deve ser correcto e reproduzível.	The counting process shall accurately count the votes. The counting of votes shall be reproducible.
99	O sistema deve manter a integridade e a disponibilidade dos votos na urna, bem como o resultado da contagem, pelo tempo requerido.	The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

E - Auditoria - I - Geral		
100	O sistema de auditoria deve ser concebido e implementado como parte integrante do sistema de votação e as suas funcionalidades devem estar presentes nos diferentes níveis – lógico, técnico e aplicativo.	The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.
101	A auditoria completa do sistema deve incluir facilidades de registo, monitorização e verificação. Os requisitos das secções II a V, abaixo, devem ser cumpridos.	End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

E – Auditoria - II - Registo		
102	O sistema de auditoria deve ser aberto, compreensível e focado nas ameaças e riscos potenciais.	The audit system shall be open and comprehensive, and actively report on potential issues and threats.
103	A auditoria deve registar tempos, eventos e acções, incluindo: a) todas as informações relativas à votação - n.º de eleitores activos, n.º de votos recolhidos, n.º de votos inválidos, contagens, recountagem, etc. b) quaisquer ataques ao sistema incluindo a infra-estrutura de comunicações.	The audit system shall record times, events and actions, including: a. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;; b. any attacks on the operation of the e-voting system and its communications infrastructure.

E - Auditoria - III - Monitorização		
104	O sistema de auditoria deve providenciar a capacidade de supervisionar a eleição e verificar se os resultados e procedimentos obedecem às regras legais.	The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.
105	Deve impedir-se a suspensão da auditoria por instruções de pessoas não autorizadas.	Disclosure of the audit information to unauthorised persons shall be prevented.
106	A auditoria não deve nunca quebrar o anonimato do votante.	The audit system shall maintain voter anonymity at all times.

E - Auditoria - IV - Verificação		
107	O sistema de auditoria deve ter a capacidade de verificar a correcta operação do sistema de votação e a fiabilidade dos resultados, detectar fraudes e provar que todos os votos depositados são autênticos e que todos foram contados.	The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.
108	O sistema de auditoria deve ter a capacidade de verificar que uma eleição cumpriu os regras legais e, portanto, que os resultados expressam os votos.	The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

E - Auditoria - V - Outros		
109	O sistema de auditoria deve ser ele próprio protegido contra ataques que possam corromper, alterar ou eliminar os seus registos.	The audit system shall be protected against attacks that may corrupt, alter or lose records in the audit system.
110	O estado devem assegurar a confidencialidade de qualquer informação obtida por qualquer pessoa no exercício de funções de auditoria.	Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

F - Certificação		
III	O estado deve introduzir processos de certificação que assegurem que qualquer componente de informação e comunicação testado está em conformidade com os requisitos aqui referidos.	Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.
II2	Para desenvolver a cooperação internacional e evitar trabalho duplicado, os estados devem considerar a associação das suas agências a acordos internacionais de reconhecimento mútuo, como sejam a European Cooperation for Accreditation (EA), o International Laboratory Accreditation Cooperation (ILAC), o International Accreditation Forum (IAF) e outras entidades afins.	In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Cooperation for Accreditation (EA), the International Laboratory Accreditation Cooperation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.

Refira-se também a existência e os importantes trabalhos (i) da comissão OASIS que desenvolve a EML-Election Markup Language¹³³ e da (ii) IEEE Standards Association Voting Systems Standards (SCC38) Project on Voting Equipment (P1583) que desenvolveu uma descrição funcional detalhada para urnas electrónicas¹³⁴.

¹³³ www.oasis-open.org.

¹³⁴ IEEE-STD P1583 - Draft Standard for Evaluation of Voting Equipment.

PARECERES OFICIAIS

Pedro Antunes

Reino Unido¹³⁵ ¹³⁶

- Não deve haver implementação nacional sem estarem garantidas a segurança, integridade e penetração tecnológica;
- A implementação deve ser incremental, por forma a reduzir o risco tecnológico;
- A implementação deverá ser baseada em múltiplas tecnologias e canais de votação;
- É fundamental implementar um sistema seguro de registo dos eleitores;
- É fundamental adoptar o princípio da descentralização como mecanismo de segurança;
- A análise de risco deve não só incluir a faceta tecnológica mas igualmente a satisfação e confiança dos eleitores;
- A confiança pode ser aumentada através da utilização de código livre;
- A utilização de terminais como caixas multibanco e de lotarias, habitualmente consideradas seguras, não é considerada viável por não serem suficientemente privadas, colidirem com a operação comercial e não estarem disponível em muitas zonas rurais;
- A utilização de computadores pessoais é comprometida pela existência generalizada de vírus, agravada pelo facto de os mecanismos de protecção apenas responderem a vírus conhecidos;
- A utilização da Internet está comprometida pela inexistência de defesas contra ataques em grande escala do tipo Negação de Serviço;
- A utilização de redes de comunicação de dados, Internet ou empresariais, aumenta o risco de quebra do anonimato do voto, por associação entre o votante e o computador onde é realizada a votação;
- Não há suficiente confiança dos eleitores na segurança do voto electrónico;

¹³⁵ UK Government (2002) In the service of democracy – A consultation paper on a policy for electronic democracy, United Kingdom, Official Report, 15 July 2002.

¹³⁶ Pratchett, L. (2002) The Implementation of Electronic Voting in the UK, De Montfort University of Essex, May.

- O estudo das implicações legais do voto electrónico levanta dúvidas sobre se o estado deve assegurar a privacidade do voto ou apenas providenciar os meios que garantam essa privacidade;
- Os estudo das limitações tecnológicas do voto electrónico identificou vulnerabilidades em: ataques do tipo Negação de Serviço; Vírus; Intercepção; Mascaramento; ataques à confiança no processo eleitoral; falhas na alimentação dos dispositivos; limitação à capacidade dos sistemas em situações de grande procura;
- A habitação do eleitor não é considerada um local suficientemente privado, devido a restrições espaciais (localização dos computadores em espaços comuns), sociais (coerção) e tecnológicas (assimetrias no acesso à tecnologia);
- Os benefícios totais de um sistema de votação electrónica só podem ser conseguidos num ambiente multi-canal;
- Um passo interino para a implementação de votação remota é a possibilidade de votar em qualquer local de voto;
- A estratégia de implementação do voto electrónico deve envolver uma significativa componente de educação pública;
- Qualquer sistema de suporte a votação electrónica deve ter código aberto e verificável.

EUA¹³⁷ ¹³⁸ ¹³⁹ ¹⁴⁰

- Os fabricantes de sistemas de votação electrónica têm falhado na adopção, implementação e acompanhamento dos padrões e melhores práticas da indústria no desenvolvimento dos seus sistemas;

¹³⁷ United States Government Accountability Office(2005). ELECTIONS, Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed, Report to Congressional Requesters, September.

¹³⁸ Roy G. Saltman (1988) Accuracy, Integrity, and Security in Computerized Vote-Tallying, Institute for Computer Sciences and Technology, National Bureau of Standards, August.

¹³⁹ Chet Culver (2001). Iowa's Election 2000: Facts, Findings, and Our Future, Iowa Secretary of State, March.

¹⁴⁰ Jennifer L. Brunner (2007). Ohio Secretary of State, Project E V E R E S T: Evaluation and Validation of Election Related Equipment, Standards and Testing, December.

- Os sistemas de votação electrónica não cumprem os padrões de segurança da indústria e estão susceptíveis a quebras de segurança que podem colocar em causa a integridade do processo de votação;
- Os princípios de segurança e fiabilidade do voto electrónico devem ser assegurados em todo o seu ciclo de vida: desenvolvimento, aquisição e operação;
- Diversos grupos de interesse, em particular entidades oficiais, peritos em segurança e grupo de pressão social têm identificado falhas na segurança e fiabilidade dos sistemas de votação electrónica, devidas principalmente a deficientes mecanismos de controlo, falhas de concepção, deficiente controlo de versões, falhas nos testes e configuração dos sistemas e má gestão da segurança;
- Um requisito importante de um sistema de votação electrónica é a verificação do registo do votante. Sendo possível utilizar um mecanismo de autenticação semelhante aos utilizados na banca, a utilização desse serviço por muitas pessoas mas poucas vezes por ano é problemática;
- Para além dos requisitos tecnológicos, um sistema de votação electrónica deve assegurar a igualdade de acesso à tecnologia de votação, verificação do registo do voto, possibilidade de votar secretamente e sem intimidação, igualdade no tratamento das partes em confronto e capacidade de demonstrar, através de auditorias e testes, que o funcionamento do sistema é correcto;
- A concepção do sistema de votação electrónica deve garantir que a impossibilidade de contabilizar um voto, por falha do sistema, não possa ser tomada por um voto em branco deliberado;
- Como opção de concepção, o sistema não deve fazer registos do processo de introdução de dados dos votantes;
- Os sistemas actuais de registo dos votantes sofrem de diversas falhas: na identificação e acompanhamento da mobilidade dos eleitores; na actualização dos registos; na identificação dos eleitores que não podem votar; na remoção de eleitores;
- Não existem mecanismos de cruzamento de dados entre registos de eleitores e resultados eleitorais.

Comissão Europeia¹⁴¹

- Na generalidade dos países europeus é considerado que existe compatibilidade entre o voto remoto e o princípio da privacidade, ou pelo menos condições que assegurem a livre expressão de opinião;
- Em alguns países o voto remoto é apenas permitido em recinto controlado;
- Considerando os tratados internacionais que governam o voto eleitoral, deve ser considerado um padrão mínimo de protecção do segredo do voto remoto, recorrendo às medidas adoptadas para o voto por correspondência, considerando em particular que o eleitor preencha individualmente o seu voto e declare solenemente que o voto foi realizado nessas condições;
- A infra-estrutura de suporte ao voto electrónico deve acompanhar as restrições imposta ao voto por correspondência, designadamente que o serviço postal é seguro e fiável. Estas restrições englobam a privacidade, prevenção da manipulação de dados, protecção do anonimato, autenticidade e integridade do voto;
- Considera-se uma precaução mínima a capacidade de o eleitor verificar o voto imediatamente após a submissão do seu voto, designadamente através de comprovativo em papel.

Portugal¹⁴²

- Requerido controlo e protecção dos cadernos eleitorais, assim como posterior destruição após o acto eleitoral;
- Requeridas normas básicas dos sistemas de informação para além da palavra-chave, designadamente actualização do sistema operativo;
- Estes requisitos oferecem uma garantia funcional suplementar, que obriga a especial diligência pela entidade gestora dos dados;
- O tratamento de dados pessoais para efeitos de votação electrónica necessita de legitimidade em lei emanada pela Assembleia da República, designadamente quanto aos requisitos do exercício do voto, local de voto e presença de eleitores no local de voto;

¹⁴¹ European Commission for Democracy Through Law (2004). Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe, Strasbourg, 18 March.

¹⁴² Comissão Nacional de Protecção de Dados (2005). A Privacidade dos Eleitores no Voto Electrónico, Deliberação aprovada pela Comissão Nacional de Protecção de Dados – CNPD, na sessão de 14 de Novembro de 2005.

- O software deve constituir código aberto e ser publicado oficialmente;
- O recenseamento eleitoral deve ser realizado electronicamente.

SOBRE OS AUTORES

Lista de autores por ordem alfabética:

André Zúquete	Professor Auxiliar do Departamento de Electrónica e Telecomunicações da Universidade de Aveiro
António Ferreira	Assistente do Departamento de Informática da Faculdade de Ciências da Universidade de Lisboa
Carlos J. Costa	Professor Auxiliar do Departamento de Ciências e Tecnologias da Informação do Instituto Superior de Ciências do Trabalho e da Empresa
Domingos Magalhães	Director de serviços de apoio ao recenseamento e processo eleitoral da Direcção-Geral de Administração Interna (MAI). Representante na comissão técnica que elaborou a Recomendação sobre voto electrónico do Conselho da Europa aos Estados membros - normas jurídicas, operacionais e técnicas - Rec(2004)11, 30-Set-2004
Duarte Vieira	Aluno de Mestrado em Informática da Faculdade de Ciências da Universidade de Lisboa
Filipe Simões	Mestre em Informática pela Universidade de Lisboa, tendo elaborado tese sobre auditoria de sistemas de votação electrónica
João Ferreira Dias	Professor agregado do Instituto Superior de Ciências do Trabalho e da Empresa, professor convidado da Fundação Getúlio Vargas (Brasil), ex-dirigente e quadro da Direcção Geral dos Serviços de Informática do Ministério da Justiça
Luís Carriço	Professor Auxiliar do Departamento de Informática da Faculdade de Ciências da Universidade de Lisboa

Paulo Ferreira	Professor Associado do Departamento de Engenharia Informática do Instituto Superior Técnico de Lisboa. Coordenador do projecto <i>Electronic Democracy</i> , financiado pela FCT
Pedro Antunes	Professor Associado do Departamento de Informática da Faculdade de Ciências da Universidade de Lisboa. Coordenador do projecto <i>E-Voting - A new Architectural Framework for Handling Risk in E-Voting Systems</i> , financiado pela FCT
Rui Joaquim	Assistente do Departamento de Engenharia de Electrónica e Telecomunicações e de Computadores do Instituto Superior de Engenharia de Lisboa. Actual aluno de Doutoramento, onde aborda a problemática do voto em plataformas não seguras/controladas