# B. Propietats en els sistemes de verificació de la votació electrònica i estudi de proves realitzades

***Jordi Castellà i Roca***

## B.1. Introducció

Des del naixement de la democràcia a l'Atenes del segle 6 aC i les primeres lleis electorals, els sistemes electorals han estat dissenyats i desenvolupats d'acord amb els requisits dels governs democràtics. El procés d'eleccions consisteix a escollir una persona o partit, és a dir, un candidat, per representar a tots els membres d'una comunitat (per exemple, una empresa, un estat o un país). Per al candidat, guanyar les eleccions comporta una gran responsabilitat en termes de representació, però també és molt atractiu per altres motius: per exemple, gestionar recursos, tenir la capacitat de canviar les normes i les lleis existents, etc. Per tant, hi pot haver algunes persones interessades en la manipulació dels resultats de les eleccions i a facilitar la victòria d'un cert candidat.

No obstant això, verificar que els resultats corresponen a les preferències dels votants i al mateix temps garantir que el vot és secret (anonimat del votant) no és una tasca fàcil. En unes altres paraules, els resultats de les eleccions han de ser verificables, i el vot ha de ser secret i no s'ha de poder vincular a un votant. Per exemple, suposem que la ciutadana Alice (assumim que pertany al cens) vota pel candidat Bob. Qualsevol altra persona no ha de ser capaç de deduir la preferència d'Alice a partir del procés de les eleccions i/o els resultats, però, al mateix temps, qualsevol persona ha de poder verificar la correcció del procés de votació. Per tant, la verificabilitat es converteix en un requisit molt important per proporcionar fiabilitat en els resultats de les eleccions, i afecta o involucra candidats i votants.

La verificació que els resultats de les eleccions corresponguin a les preferències dels votants depèn del sistema de votació. Si considerem la ubicació des d'on s'emet el vot, la majoria dels sistemes existents estan basats en col·legis electorals, i els votants van a llocs específics per poder votar. Els sistemes de votació remota, com ara el vot per correu o el vot a través d'internet, són alternatives al vot des d'un lloc fixat.

Des del punt de vista del tipus de butlleta de votació, els sistemes de votació tradicionals utilitzen paperetes en format de paper amb una llista de candidats estandarditzada. Van ser introduïdes per primera vegada a l'estat de Victòria, Austràlia, l'any 1856 (Bellis, 2009). Les butlletes de paper contenen tota la informació necessària per escollir un candidat concret en un format accessible per als humans. Per tant, en el recompte dels vots o escrutini, qualsevol persona pot verificar si la butlleta és correcta, i, en cas afirmatiu, a quin dels candidats correspon aquest vot. No obstant això, el principal inconvenient dels sistemes de votació tradicionals és que les operacions són manuals, i, per tant, poden comportar uns costos econòmics i logístics elevats. Per un altre costat, el procés de recompte pot esdevenir llarg i és susceptible de patir errors humans, especialment quan el sistema de votació és complex.

Les solucions de vot electrònic més modernes incorporen dispositius electrònics per accelerar tot el procés de recompte i evitar els problemes introduïts pels errors humans (Barrat Esteve, 2006). A més a més, també milloren l'accessibilitat dels votants discapacitats i analfabets. Les primeres iniciatives van aparèixer l'any 1964 en alguns estats dels EUA, que utilitzaven targetes perforades i escrutini per ordinador (Bellis, 2009). En termes generals, aquests tipus de solucions poden emprar diferents tecnologies, que van des de targetes perforades fins a escàners òptics (per escanejar les paperetes), mètodes criptogràfics i terminals de votació de gravació electrònica directa (*direct-recording electronic voting machines*, DRE).

Els sistemes de vot electrònic (*e-voting*) efectivament redueixen el cost dels mètodes tradicionals, però també plantegen uns altres tipus de desafiaments en relació amb la verificabilitat en les eleccions. El treball presentat a Kohno i Stubblefield (2004) analitza alguns atacs rellevants que es poden produir en els sistemes de vot electrònic i també qui els podria dur a terme (vegeu la Taula 1). Aquests atacs poden comprometre la verificabilitat del sistema de votació. Per exemple, suposem que en un sistema de votació basat en l'escaneig òptic dels vots Alice escaneja el seu vot. Un treballador del sistema de votació amb suficients permisos elimina la butlleta escanejada sense informar-ne. Si no es proporciona a Alice cap prova sobre l'escaneig del vot, ni ella ni cap altre observador independent no podran estar segurs de si el seu vot electrònic ha estat eliminat o modificat després d'emetre'l.

**Taula 1. Resum d'alguns dels atacs més rellevants dels sistemes de votació**

| Atacs | Atacants | | |
|---|---|---|---|
| | Votant amb unes credencials falses | Treballador del sistema de votació amb accés als mitjans d`emmagatzematge | Desenvolupador del dispositiu de votació |
| Votar diverses vegades | | | |
| Accés a les funcions d'administració | | | |
| Modificar la configuració del sistema | | | |
| Modificar la definició de la butlleta (per exemple, l'afiliació a un partit) | | | |
| Causar un error en el recompte manipulant la configuració | | | |
| Suplantar una màquina de votació legítima o una autoritat de recompte | | | |
| Crear, eliminar i modificar vots | | | |
| Vincular els votants amb els seus vots | | | |
| Manipular les evidències de les auditories | | | |
| Afegir una porta posterior al codi | | | |

A més dels problemes relacionats amb la verificabilitat, també hi ha debilitats que provenen de la tecnologia utilitzada per implementar una infraestructura de vot electrònic i que poden posar en perill l'anonimat dels votants. Cal tenir en compte que el fet que un sistema permeti que un individu determinat pugui vincular un vot amb el votant obre la possibilitat de patir atacs de coacció, és a dir, un votant pot ser obligat a votar per un candidat en particular. En resum, els esquemes de votació electrònica han de considerar aquestes qüestions, proporcionar una verificabilitat adequada, garantir l'anonimat dels votants i reduir els costos en comparació amb les propostes de vot tradicional.

Malgrat aquests reptes i problemes, la tendència és clara i ferma cap a l'ús de mitjans electrònics de votació (E-Voting.CC, Competence Center for Electronic Voting and Participation, 2009), però no només en el recompte electrònic, sinó també en l'emissió del vot electrònic (Barrat Esteve, 2006). Per un costat, això significa que en aquests tipus de sistemes de votació més complexos hi ha més reptes en la verificació, perquè aquesta esdevé computacionalment més complexa. Per l'altre costat, poden ser significativament útils per als ciutadans amb alguna discapacitat o analfabets. Al mateix temps, l'ús de tecnologies de votació electrònica pot reduir els costos econòmics i logístics de les eleccions i les consultes i facilitar que ciutadans que estan allunyats geogràficament dels centres de votació puguin votar.

Per tant, la verificabilitat del sistema de votació esdevé essencial per proporcionar confiança en els sistemes de votació electrònica. Aquesta propietat es classifica en tres grans grups: i) verificació individual; ii) verificació universal, i iii) verificació extrem a extrem (*end-to-end* o *E2E verification*). La verificació individual permet que cada votant pugui comprovar que el seu vot ha estat emès i recomptat correctament. La verificació universal permet que els votants, les autoritats electorals i terceres parts puguin inspeccionar que els resultats de les eleccions corresponen als vots emesos. En els sistemes de votació tradicionals, ambdues verificacions es poden aconseguir mitjançant un conjunt de procediments establerts (operacions manuals dirigides pels funcionaris electorals, o també per entitats independents i/o observadors dels candidats). En el cas dels sistemes de vot electrònic, aquestes verificacions s'aconsegueixen mitjançant una combinació de procediments i, principalment, tecnologies. Finalment, hi ha la verificació extrem a extrem (E2E). Des del punt de vista dels votants, en un sistema de votació E2E el votant pot verificar que el seu vot ha estat emès i recomptat correctament en l'escrutini final de la votació. L'objectiu és augmentar la confiança dels votants en els resultats de les eleccions. Aquesta propietat difícilment es pot aconseguir en els sistemes de vot tradicionals, ja que la votant Alice finalitza la interacció amb el sistema de votació un cop ha introduït la seva butlleta a l'urna. No obstant això, les noves propostes dels sistemes de votació i tecnologies faciliten una verificació E2E.

## *Organització del treball*

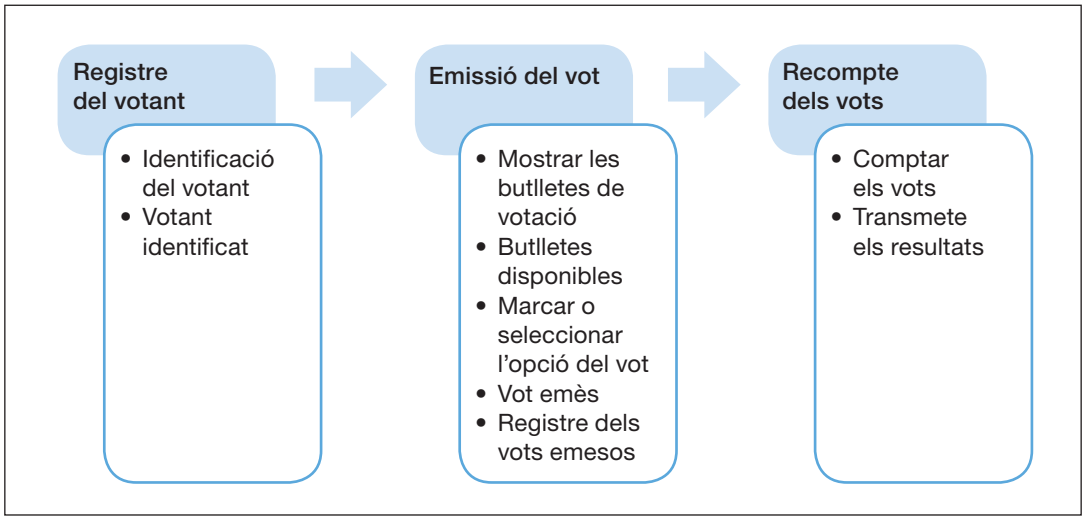
La secció B.2 inclou una descripció dels conceptes que trobarem en un sistema de votació electrònica i com es poden classificar segons el lloc on els usuaris emeten el vot o com és la verificació del sistema de votació. També s'hi descriuen els principals paradigmes de votació electrònica. La secció B.3 conté una descripció de les principals propietats

que hi ha en els sistemes de votació electrònica, com ara la interacció amb l'usuari, la seguretat, com es poden integrar mesures de verificació, i qüestions tècniques bàsiques per a la seguretat i la funcionalitat del sistema. La Secció B.4 introdueix breument dos sistemes de votació remota que s'han utilitzat amb èxit. Finalment, la Secció B.5 presenta les conclusions del treball.

## B.2. Conceptes generals de la votació electrònica

En aquest treball considerem que el procés estàndard de votació està format per les fases següents: (i) registre dels votants i identificació; (ii) emissió del vot mitjançant les butlletes, i (iii) recompte dels vots, en què totes les butlletes es recompten correctament i els resultats imparcials estan a disposició del públic. El procés de votació també inclou tots els procediments i tecnologies per garantir la correcció de la votació. La Figura 1 mostra un diagrama del procediment descrit, juntament amb alguns procediments interns.

**Figura 1. Procés de votació estàndard**




### *Models de votació*

En aquesta secció introduïm dues classificacions dels models de votació: i) segons el lloc des d'on els votants emeten el vot, i ii) segons la Help America Vote Act (HAVA). La HAVA és una llei federal dels Estats Units d'Amèrica (Congrés dels EUA, 2002) que té principalment els tres objectius següents: i) substituir els sistemes de votació basats en targetes perforades i màquines de votació de palanca (*lever voting machine*); ii) crear una comissió d'assistència electoral per ajudar en l'administració de les eleccions federals, i (iii) establir unes normes mínimes per a l'administració dels processos electorals. La classificació HAVA exigeix sistemes de verificació de la votació (*voting verificacion systems*, VVS) per proporcionar proves que permetin als votants i altres observadors verificar que el procés de votació no ha estat manipulat.

a) Classificació segons el lloc d'emissió del vot
Segons el lloc des d'on els votants han d'emetre el vot, podem classificar els sistemes de votació de la forma següent: i) sistemes basats en un centre de votació (*poll-site-based system*), i ii) sistemes de votació remots (*remote voting systems*). En el primer tipus, els votants van a votar a un edifici que anomenem «centre de votació» (*poll site*). Avui en dia és el sistema de votació més utilitzat.
Com a alternativa, els votants poden emetre el vot mitjançant un sistema de votació remota. Aquests sistemes alhora també es poden classificar de la manera següent: i) vot per correu; ii) internet; iii) vot per correu electrònic; iv) vot per SMS, i v) vot remot supervisat.

– El vot per correu va ser introduït l'any 1896 (Stalinaus County, 2010) i és més econòmic (Qvortrup, 2005) que els sistemes tradicionals de votació. No obstant això, la pèrdua de vots o el retard en el lliurament són alguns dels greus problemes que poden sorgir en aquest sistema (Barrat Esteve, 2006; Hasen, 2009). Per superar aquests inconvenients, s'han proposat els esquemes de votació remots.

– El vot per internet permet l'emissió, el lliurament i el recompte electrònics. La primera votació vinculant efectuada per internet a tot el món va ser a Estònia (Estonian National Electoral Committee, 2005).

– El vot per correu electrònic s'ha proposat com un model de votació per als ciutadans que viuen a l'estranger en alguns països i en determinades circumstàncies. Per exemple, aquest sistema es va utilitzar l'any 2004 a les eleccions presidencials i del Congrés dels Estats Units, concretament per als soldats desplegats a l'Iraq. Ha estat criticat pels problemes de seguretat relacionats amb els serveis de correu electrònic que comporta (per exemple, la manipulació del vot durant el transport i la manca de privadesa) (Nakashima, 2006).

– El vot per SMS (és a dir, el servei de missatges curts dels telèfons) va ser utilitzat a Suïssa com a part d'una sèrie de proves pilot en diverses regions del país per introduir el vot electrònic a escala nacional (Gerlach i Gasser, 2009).

– El vot remot supervisat es basa en el desplegament de centres de votació des d'on els votants poden emetre els vots. En cas que el desplegament fos a l'estranger, els vots emesos es podrien recollir electrònicament al país (o a la regió) de recompte. Cal destacar que aquest sistema pot ser molt útil quan els votants són a l'estranger (per exemple, els militars), a banda que ofereix una reducció del temps de recompte.

b) Classificació HAVA
Aquesta classificació ha estat impulsada per la Comissió d'Assistència Electoral (Election Assistance Commission), que és una agència independent del Govern dels Estats Units creada a patir de la Help America Vote Act (HAVA) del 2002. Les guies del sistema de votació voluntària de l'any 2005 –Election Assistance Commission, volum 1, apèndix C), classifica els VVS en quatre tipus:

– Els VVS basats en la separació de processos tenen una arquitectura modular, dividida en dos sistemes independents totalment aïllats, que corresponen als processos de generació i emissió del vot, respectivament.

– Els VVS basats en evidències capturen totes les accions dutes a terme pels votants durant la fase de votació.

– Els VVS d'enregistrament directe generen un registre paral·lel dels vots emesos que permet efectuar una verificació directa dels vots.

– Els VVS basats en mètodes criptogràfics que proporcionen una protecció d'extrem a extrem empren esquemes criptogràfics per obtenir rebuts de votació. Aquests rebuts permeten que els votants puguin verificar que els seus vots no han estat modificats sense revelar-ne les preferències.

## *Paradigmes de la votació electrònica*

Els sistemes de votació electrònica es caracteritzen per incloure algun procediment en el procés de votació dut a terme per mitjans electrònics i/o computacionals. Segons la tecnologia utilitzada, els sistemes de votació electrònica es poden classificar en els següents paradigmes:

– Signatures cegues *(blind signatures).* Les signatures cegues van ser introduïdes per Chaum (1982). Pertanyen a una classe de signatures digitals que permeten signar dades sense revelar-ne el contingut. En el vot electrònic, la papereta s'oculta per garantir la confidencialitat del vot, i a continuació una autoritat signa de forma cega la butlleta oculta. Així es dona validesa al vot. El votant elimina l'ocultació del vot signat i l'envia al sistema de recol·lecció dels vots mitjançant un canal anònim, és a dir, un canal que no permet vincular la informació que s'hi envia amb l'emissor corresponent (Ibrahim *et al*., 2003).

– Compromisos *(commitments).* Els esquemes basats en compromisos de bit van ser definits formalment per Brassard *et al*. (1988). Les opcions de vot (candidats) es representen com a compromisos. El votant n'escull un i es compromet amb el que ha escollit. Aquesta opció no es pot canviar i no ha de ser revelada. El votant pot optar per revelar-ne el valor (de forma anònima) en algun moment posterior. En un sistema de votació electrònica s'acostumen a utilitzar els compromisos proposats per Pedersen (Pedersen, 1992), ja que proporcionen confidencialitat perfecta o privadesa segons la teoria de la informació, que també s'anomena «privadesa eterna» (*everlasting privacy*) (Aumann *et al*., 2002; Moran *et al*., 2006).

– Criptografia homomòrfica *(homomorphic cryptography).* En els esquemes de votació electrònica que utilitzen criptosistemes homomòrfics (Cohen i Fischer, 1985; Paillier, 1999) les paperetes estan xifrades, de manera que quan s'opera amb els vots xifrats el resultat és un criptograma que conté tots els vots acumulats. Aquest mètode és molt eficient en la fase de recompte, ja que només cal desxifrar un criptograma, i, a més, la privadesa del votant es manté. Tanmateix, aquests esquemes comporten més operacions en el moment d'emissió del vot. Hi ha més requisits computacionals a la plataforma client, perquè cal demostrar que el vot està ben format (la butlleta és vàlida) sense mostrar l'opció escollida. També poden limitar el format de butlleta de votació o el nombre de candidats o de votants màxim permès.

– Xarxes de barreja *(mix-nets).* Una *mix-net* (Chaum, 1981) proporciona un canal anònim en un sistema de votació electrònica, perquè desvincula el votant del seu vot. Aquesta xarxa està formada per un conjunt de servidors. Cadascun fa les operacions següents: en primer lloc, permuta l'ordre dels vots d'entrada; a continuació transforma els vots –en general, els torna a xifrar o els desxifra, una operació necessària per evitar que es pugui enllaçar un vot de la sortida amb una de les entrades–, i, finalment, envia els vots al servidor següent. En els servidors de rexifratge la transformació és el xifratge de cada vot, de manera que cada vot es torna a xifrar en cadascun dels servidors. Per contra, en els servidors de desxifratge el votant ha de xifrar el vot tantes vegades com servidors hi hagi a la *mix-net*. Cada servidor elimina un dels xifratges. En tots dos casos, és difícil –no és possible avui en dia amb la capacitat computacional– correlacionar qualsevol sortida amb l'entrada corresponent. Quan els vots han passat per l'últim servidor de la xarxa, s'han dissociat dels seus votants. En aquest cas, cal incorporar proves per verificar que cada servidor ha estat honest, és a dir que no ha eliminat, afegit ni modificat el contingut de cap dels vots d'entrada. La realització d'aquestes proves i la verificació corresponent poden ocasionar un procés de recompte menys eficient que el recompte dels sistemes basats en criptosistemes homomòrfics (Peng *et al*., 2004; Peng, 2009). Per contra, aquests sistemes permeten més flexibilitat en el format del vot, a diferència dels esquemes homomòrfics.

Algunes d'aquestes tecnologies comprenen, com a part del protocol, la realització d'algunes proves per verificar que l'opció escollida pel votant no ha estat modificada, sense revelar la informació en si mateixa. Per tal d'aconseguir aquest objectiu s'utilitzen proves de coneixement nul (*zero-knowledge proofs*, ZKP). Poden diferir en la tecnologia d'acord amb la tècnica criptogràfica que facin servir, tot i que sempre ofereixen les propietats següents (Goldreich *et al*., 1987):

– Completesa *(completeness).* Un provador honest convenç un verificador honest sobre la prova si el resultat d'aquesta és cert.

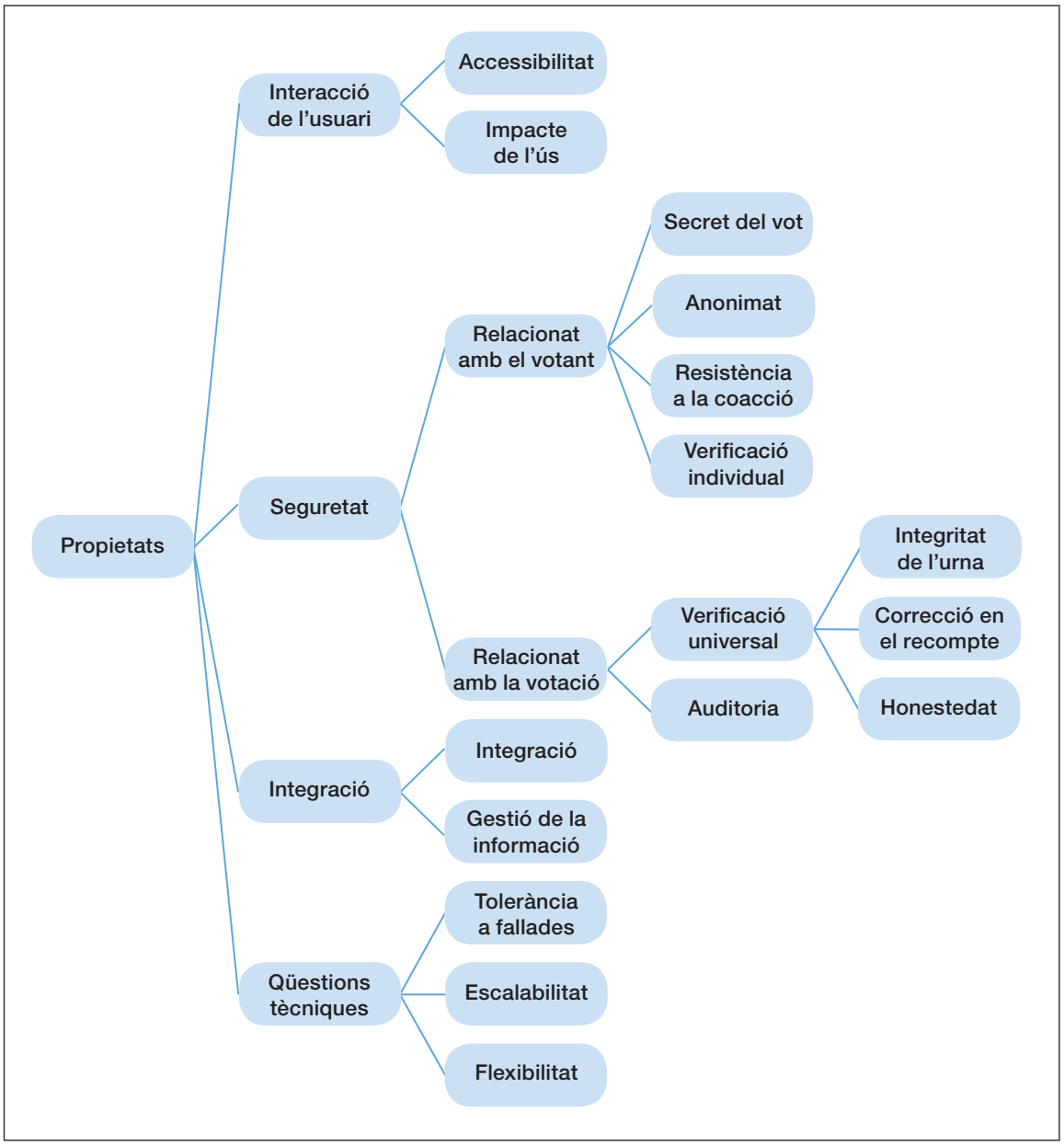
– Solidesa *(soundness).* En cas que el resultat de la prova sigui fals, un verificador deshonest només convencerà un provador honest amb una petita probabilitat.

– No revelació d'informació *(zero-knowledge).* Si el resultat de la prova és cert, un verificador deshonest només obtindrà aquesta informació, i cap dada més sobre el contingut d'aquesta.

## B.3. Propietats en els sistemes de verificació de la votació electrònica

La Figura 2 mostra una classificació de les propietats en els sistemes de votació segons les característiques següents: i) la interacció de l'usuari; ii) la seguretat; iii) la integració (amb un sistema de votació existent), i iv) qüestions tècniques. A continuació es descriuen amb més detall cadascuna de les propietats.

**Figura 2. Propietats dels sistemes de verificació de la votació**




## *Interacció de l'usuari*

La interacció amb l'usuari determina en gran mesura l'opinió dels votants i la usabilitat del sistema de votació. Aquesta interacció ha de tenir en compte les dues propietats següents:

– Accessibilitat. El sistema no ha d'impedir que un usuari amb alguna limitació física pugui votar.

– Repercussió del seu ús. El sistema no ha d'afegir fases més complexes o diferents en el procés de votació. Això podria alterar la interacció amb els votants. Aquests canvis poden ser més significatius en el procés d'emissió del vot i poden provocar una mala experiència o desànim en els votants.

## *Seguretat*

Les propietats de seguretat es poden classificar en dos grans grups: i) relacionades amb el votant, i ii) relacionades amb el procés de votació. En el primer grup hi ha la verificació dels vots per part dels votants, és a dir, la verificació individual. En el segon grup hi ha la verificació pública o verificació universal. També cal considerar si un sistema disposa de la possibilitat de ser auditat. Aquesta propietat és important en els sistemes de votació electrònica (que no utilitzen un rebut en paper) per tal de garantir la correcció en el recompte final i els resultats de les eleccions.

a) Relacionades amb el votant

– Secret del vot. El sistema ha de garantir que una tercera entitat no pugui accedir al contingut de la papereta emesa pel votant.
  • Secret o privadesa eterna *(everlasting secrecy or privacy).* La majoria dels mètodes criptogràfics utilitzats actualment ofereixen una seguretat computacional. És a dir, la seva seguretat es basa un problema matemàtic que no es pot resoldre en un temps raonable amb els recursos computacionals disponibles actualment. A mesura que augmenta la capacitat computacional, cal augmentar la dificultat del problema. Avui en dia podem protegir un secret (xifrar-lo) i ningú excepte qui tingui la informació per accedir-hi (clau de desxifratge) ho podrà fer. No obstant això, al cap d'un cert temps l'augment de capacitat computacional permetrà que s'hi pugui accedir sense aquesta informació (clau). Els secrets protegits d'avui no ho seran demà, a causa de l'avenç de la tecnologia (capacitat computacional). La privadesa eterna és la propietat que garanteix la confidencialitat de la informació independentment de la capacitat computacional existent actualment o en el futur (Aumann *et al*., 2002; Moran *et al*., 2006).

– Anonimat del vot. El sistema de votació ha de garantir que les paperetes de la votació no es puguin vincular amb els seus votants.

– Resistència a la coacció. El coaccionador d'un votant no ha de poder comprovar com ha votat un votant. És a dir, el coaccionador no ha d'estar segur de si el votant ha votat per l'opció que ell desitja. En els sistemes de votació electrònica, la coacció del votant és el perill que, fora del col·legi de votació públic, un votant pugui ser obligat a votar per un candidat en particular. En els sistemes de votació electrònica supervisats, en què l'entorn de votació està controlat per les autoritats electorals, la coacció es limita a la possibilitat de demostrar l'opció escollida pels votants al coaccionador. En els esquemes on es proporcionen rebuts de vot als votants per verificar individualment el vot emès, el coaccionador els pot utilitzar per controlar l'opció escollida pel votant. A més a més, en els sistemes de votació amb un tauler d'anuncis públic (*public bulletin board*) poden tenir lloc certs atacs relacionats amb els «patrons de vot», que també permeten obtenir als coaccionadors una prova de les opcions escollides pels votants.

– Verificació individual. Un votant pot verificar que el seu vot ha estat emès tal com ell volia. Tanmateix, aquesta verificació es pot dividir en els casos següents:

- Emès com vol el votant (*cast as intended*): aquesta propietat garanteix que el votant trobarà les seves opcions a la butlleta de votació i que les pot escollir sense cap mena d'ambigüitat.
- Registrat com s'ha emès (*recorded as cast*): aquesta propietat garanteix que el votant pot verificar que el vot ha estat registrat tal com s'ha emès, o també que el vot ha estat inclòs en el recompte final.
- Recomptat com s'ha registrat (*tallied as recorded*): aquesta propietat fa referència al fet que el vot ha estat comptabilitzat en els resultats finals igual com va ser registrat pel sistema.

– Consideracions. En cas que es garanteixi que el vot ha estat emès com volia el votant (*cast as intended*), s'ha registrat tal com ha estat emès (*recorded as cast*) i s'ha recomptat igual com s'ha registrat (*tallied as recorded*), es diu que compleix la propietat que s'ha comptat com volia el votant (*tallied as intended*). Si es compleixen les propietats *recorded as cast* i *tallied as cast*, compleix la propietat que s'ha recomptat tal com s'ha emès (*tallied as cast*). Si només compleix la propietat *cast as intended*, també compleix la propietat de registrat com es volia (*recorded as intended*).

b) Relacionades amb la votació

– Verificació universal*.* Un sistema de votació electrònica té la propietat de disposar d'una verificació universal si algú –ja sigui un votant o una altra entitat– pot verificar que els vots s'han recomptat tal com van ser emesos (*tallied as cast*). La verificació universal inclou el compliment de les propietats següents:
  - Integritat de l'urna electoral *(ballot box integrity).* Només els vots dels votants que formen part del cens electoral es poden incloure a l'urna electoral. Els vots de l'urna no s'han de poder modificar. A més a més, generalment només s'hi permet incloure un sol vot de cada votant registrat. No obstant això, aquesta última restricció depèn de les propietats del procés de votació. Per lluitar contra la coacció dels votants, alguns sistemes permeten la inclusió de més d'un vot d'un votant a l'urna, però en el recompte només es té en compte un d'aquest vots (l'últim vot emès o el vot que no conté un codi de coacció).
  - Correcció en el recompte *(tally accuracy).* El procés de recompte processa correctament tots els vots emesos.
  - Imparcialitat *(fairness).* El sistema de votació ha de garantir que no es donen a conèixer els resultats parcials abans que acabi el procediment de les eleccions. Tal com s'indica a Rosenberg (2011), la imparcialitat és una preocupació important, ja que pot induir al que es coneix com «efecte tendència popular» (*bandwagon effect*). Si un candidat determinat guanya en alguns districtes pot treure profit d'aquesta victòria, ja sigui per aconseguir el suport de votants que prèviament estaven indecisos o pel fet que alguns votants que volien donar el suport a un altre candidat decideixen abstenir-se i no participar en la votació.

– Auditabilitat *(auditability).* El sistema de votació electrònica (sense evidències en paper) ha de permetre que una tercera part pugui analitzar el que ha passat abans, durant i després d'emetre el vot sense comprometre les propietats de seguretat. D'aquesta manera, s'ha de poder certificar la correcció en el recompte final, i, per tant, en els

resultats de les eleccions. Una aplicació defectuosa o la inclusió de procediments incorrectes poden donar lloc a unes eleccions insegures. El procés d'auditoria detectarà aquests problemes. L'entitat responsable de verificar que el procés de votació electrònica es desenvolupa correctament s'anomena «auditor», i ha de ser un equip de persones multidisciplinari amb coneixements legals, d'enginyeria informàtica, de telecomunicacions i de criptografia. S'espera que aquest equip pugui actuar en nom dels candidats, de l'autoritat de les eleccions o, fins i tot, dels votants.

## *Integració*

Si els VVS formen part del sistema de votació o en són una part independent, cal tenir en compte la viabilitat i l'eficiència de l'adaptació o la interacció del sistema avaluat amb altres sistemes de votació. Concretament, cal tenir en compte la sincronització de les operacions, especialment quan els vots són emesos entre un sistema de votació i el sistema avaluat que actua com un VVS independent [Sherman *et al*. (2006)].

– Integració. El sistema ha de ser fàcil d'implementar o d'adaptar com un sistema de verificació independent que es pugui integrar al sistema que cal avaluar.

– Gestió de les dades. El subsistema d'emissió del vot i el sistema d'avaluació han de proporcionar atomicitat i/o replicació de les dades.

## *Qüestions tècniques*

En aquesta categoria es descriuen les propietats que s'han de tenir en compte en un sistema de votació electrònica des d'un punt de vista tècnic. És a dir, s'hi recullen quins són els desafiaments tecnològics d'un sistema de votació electrònica.

– Tolerància a les fallades *(fault tolerance).* Un votant del cens ha de ser capaç d'emetre el vot en el moment que vulgui dins del temps establert per a la votació electrònica. Això implica que el sistema de votació ha d'estar dissenyat per seguir funcionant malgrat que una part dels seus components no funcionin correctament (Rosenberg, 2011).

– Escalabilitat *(scalability).* El sistema votació ha de ser capaç d'absorbir la demanda dels votants durant tot el procés de votació. En aquest cas, el sistema pot tenir pics de sol·licituds de votació. Aquests pics no han d'alentir en excés el procés de votació ni afectar l'experiència del votant. En aquest apartat també s'inclou la resistència als atacs de denegació de servei *(denial of service*, DoS*)* o *denegació de servei distribuïda (distributed denial of service*, DDoS*)*. Aquests atacs són habituals a internet i fan que els usuaris no puguin accedir a un servei. Si tingués èxit, un atac d'aquest tipus podria impedir la celebració d'una elecció, ja sigui de forma parcial o total. Podem dir que constitueix un gran risc en la votació per internet.

– Flexibilitat. L'esquema criptogràfic emprat pot fixar el format de la butlleta de votació, el nombre de votants màxim o els requisits de la plataforma client.
  - Butlleta de votació. El sistema pot restringir el format de la butlleta. Per exemple, l'esquema criptogràfic pot establir que hi hagi una única opció de vot (respondre «sí» o «no» a una pregunta) o bé permetre diferents opcions i seleccionar-ne només una o més d'una de les possibles. En aquest últim cas, també és possible incorporar un ordre de preferències. Finalment, també hi ha processos electorals que permeten que els usuaris escriguin el nom del seu candidat (*write-in-candidates*). Aquests requisits provenen del sistema electoral i s'han de tenir en compte a l'hora d'escollir un sistema de votació.
  - Nombre de votants. Alguns esquemes de votació poden estar limitats a un nombre de votants màxim. Aquesta limitació pot venir donada pel cost computacional o per restriccions de l'esquema criptogràfic escollit.
  - Nombre de candidats. El nombre de candidats també pot ser una limitació. En alguns casos, el nombre de votants i el de candidats estan vinculats; és a dir, si hi ha més candidats, cal reduir el nombre de votants màxim que pot acceptar el sistema.
  - Plataforma client. Els requisits tècnics o computacionals de la plataforma que empra el client per emetre el vot són importants. Aquestes necessitats poden ser de comunicació o de computació. Ara bé, també hi ha un gran risc en relació amb el fet que la plataforma client no sigui segura (virus, cucs o controlada per un atacant). És a dir, cal avaluar els efectes nocius que hi pot haver si aquesta plataforma conté codi maliciós.

En podeu trobar un estudi més detallat a Jardí-Cedó, R. *et al*. (2012).

## B.4. Experiències de votació electrònica

En aquesta secció es descriuen breument dos sistemes de votació que s'han utilitzat amb èxit en votacions remotes en entorns no supervisats. El primer correspon a l'empresa catalana Verbio, i el segon, a l'empresa Scytl.

### *Vot telefònic a les eleccions al Parlament Europeu*

L'empresa Verbio disposa d'una tecnologia que permet identificar una persona a partir de la seva veu. L'empresa obté una mostra de la veu de la persona i en genera un patró. Quan la persona s'ha d'identificar, pot dir una frase a l'atzar proposada pel sistema. A partir de la resposta, el sistema autentica l'usuari. El sistema també pot obtenir indicis que l'usuari està essent coaccionat. La tecnologia la van provar els habitants de la població del Callús durant les eleccions europees del 25 de maig del 2014. L'anonimat del vot el garanteix la màquina que s'utilitza en la votació, que acumula els vots a mesura que rep les trucades dels votants.

A continuació comentem breument les propietats que hem esmentat en relació amb aquest sistema:

- Interacció de l'usuari:
  - Accessibilitat: la votació per telèfon proporciona una gran accessibilitat. No cal disposar de dispositius especials ni de grans coneixements. Un dels aspectes a tenir el compte són els falsos positius (s'autentica com a vàlid un usuari que no hi ha de poder accedir) i falsos negatius (es nega l'accés a un usuari legítim).
  - Repercussió del seu ús: el procés d'emissió del vot és molt senzill. No obstant això, cal fer el registre de la veu per obtenir-ne el patró abans de les eleccions. Això pot limitar el nombre d'usuaris que utilitzin el sistema.
- Seguretat:
  - En relació amb el votant:
    - ◊ Secret del vot: el secret del vot depèn de la seguretat de tot el canal de comunicació i també del dispositiu de recompte. En cas que el canal de comunicació estigui punxat o que el dispositiu de recompte sigui manipulat, es pot trencar el secret del vot. Cal tenir en compte com pot afectar la veu per IP en aquest sistema.
    - ◊ Anonimat: igual que en la propietat anterior, la vinculació d'un votant amb la seva opció de vot només es pot aconseguir si tot el procés és segur. A més a més, les traces o les evidències del sistema no han de revelar cap mena d'informació. El votant també hauria de tenir la precaució d'emetre el vot en un entorn on ningú pugui sentir la seva conversa.
    - ◊ Resistència a la coacció: el sistema incorpora mesures per detectar quan un votant està essent coaccionat. Tanmateix, no es disposa d'informació sobre els falsos positius ni els falsos negatius.
- Verificació individual: aquest sistema no proporciona aquesta propietat.
  - En relació amb la votació:
    - ◊ Verificació universal:
      - * Integritat de l'urna: el sistema és controlat per un dispositiu. L'urna serà segura si el dispositiu que acumula els vots ho és.
      - * Correcció en el recompte: la seguretat recau en el dispositiu que acumula els vots.
      - * Imparcialitat: el sistema és honest en el recompte segons la facilitat/dificultat per manipular el dispositiu que acumula els vots.
    - ◊ Auditoria: l'auditoria de tot el procés és sensible. Segons la informació que s'acumuli, es pot trencar el secret del vot o donar una informació per verificar parcialment el sistema.
- Integració:
  - Integració: la incorporació d'un sistema de verificació és possible, però pot afectar les propietats de seguretat.
  - Gestió de les dades: la replicació de dades o el fet de desar-les és una operació sensible.

– Qüestions tècniques:
  - Tolerància a fallades: la prova es va fer amb unes dues-centes persones i va funcionar correctament. Com ja s'ha comentat, caldria estudiar amb més detall el nombre de falsos positius i de falsos negatius, i també quines repercussions tindria el mal funcionament del dispositiu que acumula els vots.
  - Escalabilitat: la xarxa de telefonia pot afectar aquest sistema. Igual que trucar per telèfon mòbil en els primers minuts de l'any pot ser molt complicat, la xarxa de telefonia podria ser un coll de botella. Pel que fa a la part del servidor, no es disposa de dades per avaluar-ne l'escalabilitat.
  - Flexibilitat: el sistema proposat ofereix, *a priori*, una gran flexibilitat pel que fa a la butlleta de votació. No hi ha límit en el nombre de candidats ni en les preguntes que es poden fer.

## *Procés de votació electrònica del Consorci de Serveis Universitaris de Catalunya*

Les universitats que formen part del Consorci de Serveis Universitaris de Catalunya (CSUC) empren la solució de votació electrònica que ha desenvolupat l'empresa Scytl. En aquest sistema els usuaris han de disposar d'unes credencials, típicament una parella de claus d'un criptosistema asimètric com RSA. Segons la votació, l'empresa pot proporcionar aquestes credencials o utilitzar aquelles de què ja disposen els usuaris. En cas que s'utilitzin les que proporciona l'empresa, es generen les parelles de claus en un entorn segur. Aquestes claus es protegeixen (es xifren) amb una contrasenya segura, i aquesta contrasenya s'envia de forma segura al votant. El servidor no emmagatzema la contrasenya, sinó només la clau protegida. Quan els usuaris disposen d'unes credencials (parella de claus i certificat), el sistema accepta l'entitat de certificació que ha emès els certificats. La parella de claus pot estar instal·lada a la plataforma client (en un fitxer) o en un dispositiu segur com ara una targeta intel·ligent. Els usuaris accedeixen al portal de votació i s'autentiquen. Aquesta autenticació pot ser diferent segons cada cas. A continuació un *applet* Java permet que l'usuari seleccioni les seves opcions de vot i es protegeixi el vot. Aquesta protecció inclou diverses mesures, que es poden resumir, de forma general, en les següents: i) generació d'un rebut de votació; ii) xifratge de les opcions de vot, i iii) signatura del vot emès. El sistema es pot configurar per tal que un usuari pugui votar més d'un cop; en aquest cas, només es comptabilitza l'últim vot emès. Un cop fet el recompte, es publiquen els rebuts de votació. El rebut permet verificar que el vot ha estat comptabilitzat en els resultats de la votació, però no permet verificar quines opcions ha escollit el votant. Així s'evita que els votants es puguin vendre el vot o puguin ser coaccionats.

El sistema permet gestionar de forma adequada la votació presencial amb la remota. Si un votant ha emès el vot de forma remota, ho pot fer també presencialment; en aquest cas, el vot electrònic no es comptabilitza.

La clau privada necessària per obrir els vots està repartida entre els membres de la mesa electoral mitjançant un esquema llindar, i protegida amb una targeta intel·ligent. Aquestes mesures de seguretat impedeixen que qualsevol part involucrada en la votació pugui accedir a aquesta peça d'informació tan sensible abans o durant el procés de votació.

Una altra característica és l'obtenció de traces o evidències de tot el procés de votació, que s'utilitzen en cas que el procés es vulgui auditar. Tot seguit es comenten breument algunes de les propietats que hem explicat abans.

- Interacció de l'usuari:
  - Accessibilitat: la realització de les operacions criptogràfiques a la plataforma client pot dificultar que els usuaris utilitzin el sistema. Cal disposar de l'entorn d'execució del Java instal·lat. En el cas d'emprar un dispositiu de seguretat, també cal que l'usuari tingui l'equip configurat correctament. No tots els usuaris poden complir aquests requisits, malgrat que els usuaris més joves (presumiblement més hàbils amb les noves tecnologies) sí que hi poden estar més familiaritzats.
  - Repercussió del seu ús: si els usuaris tenen l'entorn configurat, no suposa cap pas més. En el cas de l'enviament de la contrasenya de les claus als usuaris, no suposa que aquests s'hagin de desplaçar.
- Seguretat:
  - En relació amb el votant:
    - ◊ Secret del vot: la utilització de criptosistemes segurs i un esquema llindar per protegir la clau secreta de la mesa electoral garanteixen el secret del vot. No obstant això, no es proporciona *everlasting privacy* si es guarden els vots emesos. Els criptosistemes emprats ofereixen una seguretat computacional.
    - ◊ Anonimat: la desvinculació del vot del votant s'aconsegueix mitjançant una *mix-net* verificable. Es proporcionen evidències (proves de coneixement nul) que tot el procés s'ha dut a terme correctament.
    - ◊ Resistència a la coacció: el sistema permet que un votant emeti més d'un vot per evitar la coacció; és a dir, si un votant és coaccionat, pot tornar a votar. A més a més, el rebut de votació no permet demostrar com ha votat.
    - ◊ Verificació individual: el votant pot verificar, gràcies al rebut, que el vot ha estat processat pel sistema, és a dir, que s'ha tingut en compte en els resultats; tanmateix, no pot verificar si ha estat comptabilitzat tal com ell l'ha emès. Això és així per evitar la venda de vots.
  - En relació amb la votació:
    - ◊ Verificació universal:
      - * Integritat de l'urna: el sistema incorpora la recol·lecció de traces per detectar l'eliminació de vots. La verificació individual també permet detectar aquest cas. La signatura dels vots no permet afegir ni modificar els vots de l'urna. Això és així perquè l'usuari és l'únic que té accés a la clau privada per signar els vots.
      - * Correcció en el recompte: un cop s'ha desvinculat el vot del votant, es procedeix al desxifratge. Aquesta operació és verificable, és a dir, es pot garantir que el desxifratge s'ha fet correctament mitjançant una prova de coneixement nul.

    * Imparcialitat: la utilització d'un esquema llindar –és a dir, el fet que la clau que permet obrir els vots emesos no estigui disponible– no permet conèixer els resultats intermedis.
  ◊ Auditoria: l'auditoria es pot fer a partir de les traces obtingudes durant tot el procés de votació. Per fer l'auditoria calen coneixements avançats de criptografia, de seguretat i del procés legal de la votació.

– Integració:
  • Integració: el sistema estudiat incorpora les mesures de verificació del sistema de votació.
  • Gestió de les dades: el sistema pot replicar les dades sense afectar les propietats del sistema.

– Qüestions tècniques:
  • Tolerància a fallades: el sistema disposa de sistemes redundants, però els problemes en la plataforma client poden afectar l'emissió del vot.
  • Escalabilitat: les proves dutes a terme han demostrat que el sistema ha estat capaç de gestionar correctament les peticions dels usuaris. Ara bé, com qualsevol altre sistema accessible per internet, hi ha el perill que pugui patir un atac de denegació de servei.
  • Flexibilitat: la butlleta de votació ofereix una gran flexibilitat. La seguretat de la plataforma client recau en l'entorn que ofereix Java i en els dispositius segurs que utilitzi l'usuari.

## B.5. Conclusions

En aquest treball s'han descrit breument els conceptes bàsics que podem trobar en un sistema de votació electrònica i com els sistemes es poden classificar segons el lloc on els usuaris emeten el vot o com se'n fa la verificació en el sistema. També s'han presentat els principals paradigmes de votació electrònica.

A continuació s'han explicat les propietats principals que trobarem en els sistemes de votació electrònica: i) la interacció amb l'usuari; ii) la seguretat; iii) la integració de mesures de verificació, i iv) qüestions tècniques bàsiques per a la seguretat i la funcionalitat del sistema.

Finalment, s'han estudiat dos sistemes de votació remota que s'han utilitzat amb èxit. El primer correspon a l'empresa catalana Verbio; la tecnologia es va provar durant les eleccions europees del 25 de maig del 2014 a la població del Callús. El segon correspon a l'empresa Scytl; el seu sistema de votació ha estat provat en diverses universitats del CSUC.