

**E.P.A.P. Ente Previdenza ed Assistenza Pluricategoriale**

Via Vicenza 7 - 00185 Roma –

**Fax 06 6964555 - 06 6964556**

**p.c.**

**Ministero del Lavoro, della Salute e delle Politiche Sociali**

**Direzione Generale per le politiche previdenziali**

**Divisione III - Vigilanza giuridico-amministrativa sugli Enti previdenziali**

Via Flavia 6 - 00187 Roma

Fax 0646832847

**Ministero dell'Economia e delle Finanze**

**Ispettorato Generale di Finanza - I.G.F. - Ufficio VIII**

Via XX Settembre n. 97 - 00187 Roma

Fax: 0647613735

**Consiglio Nazionale Geologi**

Via Vittoria Colonna ,40

00193 Roma

Fax 06/68807742

**Raccomandata a/r anticipata a mezzo fax**

**OGGETTO: ELEZIONI DELL'ENTE PREVIDENZA ED ASSISTENZA PLURICATEGORIALE (EPAP)**

Il sottoscritto dott. Francesco Russo, nella qualità di candidato alla carica di membro del Consiglio di Amministrazione dell'EPAP e di Presidente dell'Ordine dei Geologi della Campania, in allegato alla presente trasmette copia della relazione accademica, da cui si evincono le anomalie che caratterizzano l'espressione del voto per via telematica nell'ambito delle elezioni in oggetto.

Al riguardo lo scrivente sottolinea che tale modalità di voto - diversamente da quella per corrispondenza - non è assistita da pubblica fede relativamente alla identificazione dell'elettore.

Inoltre, fa presente che la procedura di voto elettronico adottata dall'EPAP potrebbe dar luogo, oltre alla alterazione delle elezioni in corso, alla commissione di reati informatici, con evidenti responsabilità amministrative anche in capo all'Ente previdenziale stesso.

Il sistema di voto telematico prescelto dall'EPAP preoccupa ancor di più in considerazione del fatto che - a circa 24 ore dall'inizio delle operazioni di voto - non vi è stata ancora una completa trasmissione di tutti gli elementi occorrenti per una corretta espressione del voto telematico da parte della totalità degli iscritti.

Pertanto, lo scrivente chiede che l'EPAP si attivi nell'immediato per adottare tutte le misure ritenute più opportune e che gli organi di vigilanza e controllo, destinatari della presente per conoscenza, intervengano per prevenire ogni ipotesi di illecito prospettabile.

dott. Francesco Russo

# Parere sulla procedura di voto elettronico adottata dall'EPAP

Fisciano (SA), 9 Marzo 2010

Proff. Carlo Blundo, Giuseppe Cattaneo, Alfredo De Santis

## La sicurezza dei sistemi di votazione elettronica su Internet

La votazione per via telematica (detta anche voto elettronico su Internet ) è l'atto di esprimere un voto utilizzando un sistema che impiega Internet quale mezzo per comunicare l'espressione di voto dell'elettore. Il voto elettronico su Internet consiste in un sistema di votazione in cui la scheda elettorale è in formato digitale di modo che essa possa essere trasmessa attraverso Internet ad un seggio elettorale virtuale dove viene scrutinata al termine della tornata elettorale. Si possono identificare tre tipi di sistemi di votazione su Internet. Essi sono classificati in una sequenza crescente di complessità a partire da un sistema relativamente semplice che offre pochi nuovi servizi all'elettorato ma che ha *implica* poche preoccupazioni relativamente alla sicurezza del sistema, fino ad arrivare ad un sistema molto sofisticato che fornisce all'elettorato delle comodità senza precedenti, ma con problemi di sicurezza maggiori da superare. I tre tipi di sistemi sono:

1. Votazione su Internet presso il seggio elettorale assegnato all'elettore.
2. Votazione su Internet presso un qualsiasi seggio elettorale.
3. Votazione Elettronica Remota da casa, ufficio o da un qualsiasi dispositivo connesso ad Internet.

I sistemi di votazione elettronica su Internet possono essere divisi in due classi: voto elettronico in seggio elettorale (votazione presidiata) e voto elettronico remoto (votazione non presidiata).

Con il termine *Voto Elettronico in Seggio Elettorale* facciamo riferimento ad una procedura elettorale in cui i cittadini si recano in ogni caso presso un Seggio Elettorale per esprimere la propria preferenza. Presso il seggio elettorale vi saranno dei *terminali per la votazione* (ad esempio, personal computer equipaggiati con lettore di smart card) gestiti dai membri del seggio elettorale. I terminali utilizzati per la votazione devono soddisfare precisi requisiti architettonici definiti nella specifica del protocollo di votazione. Tutti i terminali di tutti i seggi elettorali soddisfano identiche caratteristiche. I membri del seggio elettorale garantiscono anche l'identificazione degli elettori. In questo caso, gli elettori devono comunque recarsi presso un seggio elettorale. Un esempio di votazione su Internet presso il seggio elettorale assegnato all'elettore è il sistema di votazione realizzato dal CINECA ([http://www.cineca.it/area/e-vote\\_miur.htm](http://www.cineca.it/area/e-vote_miur.htm)). Tale sistema è utilizzato in ambito accademico per l'elezione delle Commissioni di Valutazione Comparativa necessarie al reclutamento del personale docente e ricercatore delle università italiane.

Con il termine *Voto Elettronico Remoto* facciamo riferimento ad una procedura elettorale in cui gli elettori possono esprimere la propria preferenza elettorale attraverso Internet. Ad esempio, gli elettori, dal comfort della propria abitazione o da qualsiasi punto ove ci sia una connessione Internet, potrebbero votare usando un qualsiasi personal computer accedendo con un browser ad un sito web; oppure gli elettori potrebbero esprimere le proprie preferenze attraverso il proprio cellulare in qualunque parte del globo essi si trovino. La votazione non è sotto il controllo dei membri del seggio elettorale. Il dispositivo connesso ad Internet utilizzato per la votazione è sotto il completo controllo dell'elettore, può essere configurato a suo piacimento, deve soddisfare soltanto requisiti architettonici minimali (ad esempio, deve avere la possibilità, tramite web browser, di accedere ad un sito web). Un esempio di Voto Elettronico Remoto è **ID\_eVoting** (<http://www.idtech.it/?q=evoting>). Tale sistema di votazione telematica, sviluppato dalla ID Technology, è stato adottato dall'EPAP.

Le proprietà di base, che un qualsiasi sistema elettorale deve soddisfare, sono le seguenti:

- **Democrazia:** solo i cittadini che hanno gli opportuni requisiti (elettori) possono votare e lo possono fare una sola volta.
- **Accuratezza:** il voto di un elettore non può essere alterato, duplicato o rimosso senza che il fatto passi inosservato. Voti non validi (schede bianche o nulle) non saranno presi in considerazione nel conteggio finale.
- **Anonimia:** non c'è modo di mettere in relazione un elettore ed una preferenza espressa su di una scheda elettorale nell'urna.

## Problematiche del voto elettronico

È noto che sistemi per il voto elettronico in seggio elettorale hanno evidenziato problemi di sicurezza. Ad esempio, nel 2007, lo stato della California ha condotto uno studio approfondito sui dispositivi utilizzati per la votazione elettronica in seggio elettorale. Esperti di sicurezza informatica hanno esaminato i dispositivi di voto prodotti da tre aziende eseguendo sia un'analisi di un attacco di tipo red-team sia un dettagliato esame del codice sorgente usato da tali dispositivi. Sono state individuate una serie di problematiche di sicurezza. Come risultato di tale studio, tutti i dispositivi esaminati non sono stati più certificati. Di conseguenza non sono stati più utilizzati nelle elezioni in California. I maggiori problemi di sicurezza derivavano dalla scarsa attenzione posta nella progettazione dei dispositivi stessi e dal fatto che i dispositivi non fossero stati sottoposti ad un'analisi esterna da parte di persone esperte in sicurezza informatica.

Ci sono stati molti casi documentati di errori e problemi di natura tecnica nelle votazioni elettroniche in seggio elettorale. A questi si aggiungono frodi intenzionali. Ad esempio, c'è stata una frode elettorale nel Kentucky (USA) dove cinque pubblici ufficiali della contea di Clay sono stati arrestati all'inizio del 2009 per aver manipolato i dispositivi di voto elettronico in modo da modificare i risultati di elezioni federali, locali e statali negli anni 2002, 2004 e 2006. Gli arrestati sono stati imputati di associazione a delinquere per frode elettorale e per violazione dei diritti degli elettori, estorsione, frode postale, ostacolo alla giustizia,

Nel 1871 William Marcy Tweed affermava: *"As long as I get to count the votes, what are you going to do about it?"* testimoniando l'esigenza di regole precise per il conteggio e verifica della correttezza delle operazioni. Con l'utilizzo di dispositivi elettronici per la votazione, il problema posto nel 1871 è più che mai attuale.

Qualsiasi sistema di votazione elettronica da remoto oltre ai problemi evidenziati per votazioni in seggio elettorale, genera delle serie di problematiche ulteriori relative alla sicurezza del voto a causa dell'ambiente (Internet) in cui tale votazione avviene. La votazione telematica da remoto soffre di due problemi fondamentali: la mancanza di autenticazione faccia-a-faccia che, ad esempio, potrebbe favorire la compra-vendita di voti, e l'utilizzo di computer personali che una gestione non rigorosa della loro configurazione aumenta il rischio di attacco di codice maligno (*malware*).

Oltre a problematiche di sicurezza, ci sono molti aspetti sociologici del voto elettronico remoto che generano preoccupazioni e che devono essere seriamente presi in considerazione nella progettazione e sviluppo di un qualsiasi sistema di voto elettronico remoto. Le preoccupazioni principali sono:

- **Coercibilità:** il pericolo che all'esterno di un seggio elettorale un elettore possa essere costretto a votare per un particolare candidato.
- **Vendita del voto:** l'opportunità per gli elettori di vendere facilmente il proprio voto.
- **Voto per delega:** il pericolo che non essendoci un seggio elettorale un intero gruppo di elettori potrebbe delegare un singolo rappresentante a votare in loro vece.

Soprattutto negli Stati Uniti, ci sono stati molti progetti di votazione elettronica da remoto che sono stati abbandonati per insufficienti garanzie di sicurezza. Ad esempio, il Pentagono ha considerato di adottare un proprio sistema di votazione (**SERVE**) prima di abbandonarlo nel 2004 a causa di problemi di sicurezza. Con la tecnologia attuale, non è proponibile un sistema di voto elettronico da remoto che garantisca le proprietà basilari di Accuratezza e Anonimia. Infatti, nel settembre del 2008 negli Stati Uniti trenta tra esperti di informatica e professori delle principali università hanno firmato un documento in cui affermavano che fino a quando *"serie e potenzialmente insuperabili difficoltà tecniche"* non sono superate, permettere l'uso di

Internet in votazioni elettroniche da remoto "è uno straordinario ed inutile rischio per la Democrazia".

Dalle precedenti considerazioni si evince che qualsiasi sistema di votazione elettronica deve prevenire qualunque tipo di frode intenzionale sia da parte di chi gestisce il sistema sia da parte degli utilizzatori.

## Perplessità sulla procedura adottata dall'EPAP

A tutte le preoccupazioni e perplessità di utilizzo di un sistema di voto elettronico da remoto, l'adozione del sistema **ID\_eVoting** aggiunge una serie di dubbi che non sono fugati dalla limitata documentazione disponibile sul sistema di voto stesso.

Dall'analisi delle procedure di voto tramite il sistema ID\_eVoting si evince che ogni elettore è identificato esclusivamente tramite username e password. Il voto espresso dall'elettore non è né cifrato né firmato digitalmente dall'elettore stesso (soltanto la comunicazione tra seggio elettorale virtuale ed elettore è cifrata tramite SSL). Una conseguenza immediata di tale strategia di identificazione dell'elettore è il mancato rispetto del Comma 1 dell'Articolo 8 - "Modalità per la espressione del Voto" del **Nuovo Regolamento Elettorale dell'EPAP** che stabilisce che "Le elezioni si svolgono a suffragio diretto nell'ambito di ciascun Collegio elettorale, mediante votazione a scrutinio segreto e senza ammissione di delega." Un elettore che utilizzi ID\_eVoting può facilmente delegare qualsiasi persona (anche chi non ha diritto al voto) a votare al suo posto. È sufficiente fornire al delegato solo le credenziali di accesso a ID\_eVoting (username e password). Comunque, è necessario osservare che il problema della delega non è un problema solo del sistema ID\_eVoting. Qualsiasi sistema di voto elettronico remoto che prevede l'autenticazione dell'elettore esclusivamente tramite username e password senza utilizzare dispositivi di autenticazione biometrica e che non cifra né firma il voto espresso con chiavi in possesso solo dell'elettore è suscettibile del problema di *delega*. Ovviamente la facilità con cui si può delegare al voto potrebbe favorire la compravendita dei voti.

Un altro problema della procedura di voto per via telematica individuata dall'EPAP deriva dalla modalità di generazione delle credenziali di accesso (username, password) fornite all'elettore. La procedura di voto prevede che le credenziali siano generate automaticamente ed inviate tramite raccomandata presso il domicilio dell'elettore. Il dispositivo che ha generato le credenziali potrebbe conservare le credenziali di accesso ed quindi potenzialmente di esprimere un voto al posto di qualsiasi elettore. Questo è un problema noto e comune a tutti i sistemi di voto elettronico remoto che generano (e conservano) le credenziali per ogni elettore e in cui l'elettore non cifra/firma il voto espresso.

In un qualsiasi sistema di voto elettronico remoto si deve avere una completa fiducia nel sistema utilizzato in quanto il problema principale è che in genere, il software utilizzato da sistemi di voto elettronico remoto è completamente chiuso e proprietario (il codice non è di pubblico dominio e non se ne può quindi verificare autonomamente la correttezza). Il software che implementa il sistema ID\_eVoting potrebbe *“essere robusto ed onesto”* ma chi garantisce che i server su cui girano gli applicativi di gestione della procedura di voto per via telematica non siano stati attaccati da un codice maligno (virus e/o malware) che modifica il comportamento degli applicativi stessi in modo da alterare i risultati della votazione? Inoltre, un software maligno (malware) potrebbe essere diffuso con lo scopo di installarsi sul PC dell'elettore e attendere la procedura di voto e interferire con il suo comportamento. In questo caso, anche disponendo dell'ultimo aggiornamento di un buon antivirus non verrebbe assicurata l'immunità da questo attacco per la postazione PC del singolo dell'elettore (è risaputo che l'aggiornamento di un antivirus viene rilasciato dopo che la ampia diffusione del virus è stata rilevata). Il verificarsi di una simile evenienza non potrebbe essere in nessun modo rilevata da nessun sistema di votazione.

Premesso che non abbiamo avuto a disposizione la descrizione dettagliata del protocollo di votazione elettronica da remoto utilizzato nel sistema ID\_eVoting, non è chiaro come sia preservata l'anonimia degli elettori e come venga garantito che il voto espresso dall'elettore non venga cambiato prima di essere depositato nell'urna virtuale. Il sistema prevede (si veda la circolare Prot. 2942/10 dell'EPAP) un database *“strutturato in modo da non registrare l'associazione tra votante e voto espresso, al fine di non consentire la ricostruzione di questa relazione”*. Il server che gestisce la votazione, o chi ha accesso al server stesso, prima di depositare il voto nell'urna (registrare il voto nel database) potrebbe cambiarlo in quanto il voto depositato non è né cifrato né firmato digitalmente dall'elettore (l'elettore non ha modo di cifrare/firmare il suo voto in quanto non è in possesso di nessuna chiave di cifratura/firma). Inoltre, prima che il voto sia depositato nell'urna il server che gestisce la votazione è a conoscenza della relazione elettore-voto. Il sistema adottato dovrebbe fornire le stesse garanzie di anonimia degli altri due metodi di votazione adottati dall'EPAP: presso il seggio elettorale di Roma o per corrispondenza. In entrambe le modalità è evidente che non c'è modo di collegare un elettore ad un voto né tantomeno di cambiare il voto dell'elettore; mentre con il voto elettronico da remoto, prima di registrare il voto, il server (o chi ha accesso al server) conosce l'associazione voto-elettore e quindi, oltre a poter modificare a suo piacimento il voto espresso, potrebbe anche conservare questa associazione. Anche in questo caso si deve avere una completa fiducia nel sistema che implementa la votazione elettronica.

Non è chiaro come con la procedura di voto per via telematica utilizzata (ID\_eVoting) si possa garantire il *non ripudio* della votazione. Non è chiaro come sia possibile provare, anche eventualmente ad una terza parte, che un elettore abbia effettivamente votato. Un elettore che ha votato da remoto potrebbe asserire che non lo ha fatto oppure l'elettore veramente non

ha votato, ma qualcuno è venuto a conoscenza delle sue credenziali ed ha votato in sua vece. Non avendo a disposizione la descrizione del sistema ID\_eVoting è difficile valutare se il sistema garantisca o meno la proprietà di non ripudio. In generale, riteniamo che non si possa garantire il non ripudio in quanto l'autenticazione dell'elettore avviene solo tramite le credenziali generate dal sistema stesso e il voto dell'elettore non è né cifrato né firmato dall'elettore. Si tenga presente che tale proprietà di non ripudio è implicitamente garantita nelle altre due modalità di votazione previste dal regolamento elettorale dell'EPAP. Nella votazione per corrispondenza l'elettore deve firmare una busta e la firma deve essere autenticata (la busta è controllata da un notaio nel seggio elettorale); mentre, nella votazione presso il Seggio Elettorale istituito nell'unica sede dell'Ente l'elettore deve firmare un registro durante la procedura di voto.

In conclusione un qualsiasi sistema di votazione elettronica remota può essere utilizzato soltanto in situazioni in cui c'è uno scarso interesse ad esercitare coercizione degli elettori e/o delega arbitraria.

## Riferimenti

- [1] "Computer Technologists' statement on internet voting." 11 settembre 2008.  
<http://www.verifiedvoting.org/article.php?id=5867>
- [2] Pentagon e-voting plan 'flawed', 22 gennaio 2004  
<http://news.bbc.co.uk/2/hi/technology/3419775.stm>
- [3] David L. Dill, Bruce Schneier, and Barbara Simons. Voting and Technology: "Who Gets to Count Your Vote?", Communications of the ACM, Vol. 46, No. 8, Agosto 2003.

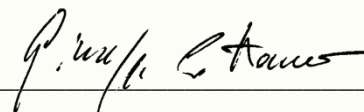
In fede,

Fisciano (SA), 9 marzo 2010

Carlo Blundo, Professore Ordinario di Informatica



Giuseppe Cattaneo, Professore Associato di Informatica



Alfredo De Santis, Professore Ordinario di Informatica

