Relazione sulle modalità di voto telematico per la FNOMCeO

Addendum

Digitally signed
by REALE ROBERTO
C=IT

Premessa

Il presente addendum alla Relazione sottoposta a codesta Federazione il giorno 15 ottobre u.s. (di seguito Relazione) è motivato dall'acquisizione, successiva rispetto a tale data, di ulteriori notizie tecniche dagli Ordini di seguito indicati:

Ordine	**Protocollo arrivo**
Campobasso	12352/2020 del 23-10-2020
Latina	12524/2020 del 27-10-2020
Nuoro	12145/2020 del 21-10-2020
Piacenza	N/D

Valutazione

Si premette che la presente valutazione non osta all'adozione di procedure di voto telematico tout court, che è invece fortemente consigliata in quanto favorisce una maggiore partecipazione al voto (a maggior ragione in condizioni in cui il voto in presenza non è praticabile) e può garantire comunque le medesime salvaguardie e garanzie del voto in presenza a condizione che vengano posti in essere tutti gli accorgimenti tecnici che la letteratura scientifica in materia di e-voting ha da tempo riconosciuto. Il legislatore ha certamente inteso favorire la transizione a modalità di voto elettronico nel riconoscimento della necessità di una transizione digitale della pubblica amministrazione, senza tuttavia ammettere deroghe alle prerogative procedimentali già in essere per il solo fatto che il diritto al voto venga espletato attraverso strumenti digitali anziché in forma tradizionale.

Si auspica pertanto che codesta Federazione voglia procedere alla costituzione di un tavolo tecnico interistituzionale per la definizione di linee guida tecniche in assenza delle quali le soluzioni finora presentate non possono considerarsi conformi alle esigenze di assoluta segretezza del voto e di trasparenza delle procedure. Tali linee guida potranno naturalmente raccordarsi con la normativa primaria e secondaria in materia di servizi fiduciari, identità digitale, interoperabilità, conservazione documentale, e in generale con la strategia digitale nazionale (ivi compreso il Piano Triennale corrente) e comunitaria. In particolare, benché certamente sia opportuno che dette linee guida mantengano un approccio c.d. "agnostico" rispetto alla scelta dello "stack" tecnologico da adottare, non si può escludere che vengano prese in considerazione soluzioni basate su tecnologie a registri distribuiti.

Ciò premesso, le soluzioni tecniche proposte si ritengono ad oggi non del tutto adeguate allo scopo, e ciò in considerazione del fatto che non vengono affrontate né risolte le criticità già individuate nella Relazione.

In particolare:

1) disaccoppiamento dei voti dai votanti e segretezza e anonimità del voto

Con particolare riferimento alla crittografia dei voti espressi dagli elettori, la soluzione presentata (ELIGO) dispone di funzionalità utili ad applicare ai voti un algoritmo di crittografia RSA per crittografare i voti in entrata e de-crittografarli nella fase di scrutinio. È opportuno ricordare a questo proposito che l'algoritmo RSA pur essendo in linea teorica relativamente sicuro è suscettibile di numerosissime vulnerabilità nelle soluzioni software che lo implementano (cfr. il database CVE, universalmente adottato, sub voce RSA: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rsa). Com'è noto, nell'impiego di funzioni crittografiche le vulnerabilità sono generalmente presenti non tanto nel sistema software di gestione (la soluzione de quo), ma nelle librerie medesime che quel software impiega. L'analisi del rischio deve necessariamente tenerne conto e prevedere, come mitigation, l'adozione di un formal threat model (analisi formale dei modelli di attacco) e, se possibile, di meccanismi di sicurezza matematicamente dimostrabile (c.d. provable security).

Va inoltre osservato che un meccanismo che consenta la de-crittazione dei voti, e che sia quindi reversibile, indipendentemente dall'algoritmo di cifratura adottato, non può considerarsi una garanzia adeguata perché determina l'esistenza di una c.d. "superficie di attacco", laddove invece il voto espresso non deve essere riconducibile all'elettore in nessun caso. Come già ricordato nella Relazione, infatti, il requisito in oggetto si scinde nelle due specie seguenti, così come riconosciuti in letteratura:

> *Collusion-free vote secrecy*: la segretezza del voto deve essere garantita anche se tutti i mezzi elettorali (ad esempio, schede votate) e le chiavi di sicurezza sono rese note da un attacco o

da un errore. In altri termini, la segretezza del voto non deve dipendere solo dal protocollo di comunicazione e da ipotesi crittografiche.

Fail-safe voter privacy: La privacy degli elettori deve essere assicurata anche se l'intero sistema di voto telematico non funziona correttamente o è costretto a funzionare in modo improprio ovvero le procedure elettorali sono viziate, senza limiti di tempo.

Perché tali requisiti siano rispettati, è opportuno adottare schemi di crittografia omomorfa o a conoscenza zero che consente lo scrutinio dei voti senza alcuna necessità di de-crittografare gli stessi.

2) identificazione certa delle credenziali degli elettori

Si è già indicata l'opportunità di adottare schemi di identificazione certa degli elettori conformi alla normativa eIDAS (SPID, CIE) o quanto meno di tipo SSI (self-sovereign identity). Tali schemi dovranno poi essere abbinati a protocolli a conoscenza zero (zero-knowledge protocols) che consentano l'anonimità pur in presenza di identificazione certa. Le soluzioni presentate non risultano rispondere a questo requisito. L'obiezione posta, che "i criteri di identificazione a due fattori sono utilizzati da una molteplicità di enti pubblici in attesa di un passaggio all'utilizzo diffuso dello SPID" (cfr. ad esempio Protocollo n° OMCEO LATINA. Appr. Tecnico Procedurali in data 20/10/2020) potrebbe essere accolta per sistemi già in essere (ferme restando le disposizioni in materia di identità digitale del decreto-legge 16 luglio 2020, n. 76, convertito nella legge 11 settembre 2020, n. 120, recante: «Misure urgenti per la semplificazione e l'innovazione digitale.»), non certo per un sistema di nuova adozione.

3) unicità del voto

L'unicità del voto è correlata all'identificazione certa delle credenziali degli elettori, che ne un prerequisito.

4) sorgente aperto

A corredo di tali considerazioni, si ribadisce inoltre l'opportunità di acquisire o quanto meno valutare soluzioni software a sorgente aperto, ex artt. 68 e 69 del Codice dell'Amministrazione Digitale, nonché delle Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni in attuazione dei medesimi artt.

Conclusioni

Le soluzioni di voto telematico proposte si ritengono non interamente adeguate a rispondere ai requisiti di identità certa dei votanti, segretezza e anonimità del voto, unicità e immodificabilità del voto, auditabilità e trasparenza dei sistemi, del codice sorgente e delle procedure.