Parere sullo schema decreto del Ministero degli Affari esteri e della cooperazione internazionale sulla sperimentazione da parte del Maeci del voto elettronico in occasione del rinnovo dei Comitati degli italiani all'estero 2021 (Com.It.Es.) - 19 novembre 2021 [9721434]

[doc. web n. 9721434]

Parere sullo schema decreto del Ministero degli Affari esteri e della cooperazione internazionale sulla sperimentazione da parte del Maeci del voto elettronico in occasione del rinnovo dei Comitati degli italiani all'estero 2021 (Com.It.Es.) - 19 novembre 2021

Registro dei provvedimenti
n. 405 del 19 novembre 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTA la legge 23 ottobre 2003, n. 286, recante "Norme relative alla disciplina dei Comitati degli italiani all'estero";

VISTO il decreto del Presidente della Repubblica 29 dicembre 2003, n. 395, recante il Regolamento di attuazione della legge 23 ottobre 2003, n. 286, per la disciplina dei Comitati degli italiani all'estero;

VISTO il decreto legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" e in particolare l'articolo 9, il quale prevede che le amministrazioni competenti "favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili e migliorare la qualità dei propri atti, anche attraverso l'utilizzo, ove previsto e nell'ambito delle risorse disponibili a legislazione vigente, di forme di consultazione preventiva per via telematica sugli schemi di atto da adottare

VISTO il decreto-legge 30 maggio 2012, n. 67, recante "Disposizioni urgenti per il rinnovo dei Comitati e del Consiglio generale degli italiani all'estero", convertito con modificazioni dalla Legge

23 luglio 2012, n. 118, il quale prevede l'introduzione di modalità di votazione e scrutinio per il rinnovo dei Comitati degli italiani all'estero (di seguito "COM.IT.ES") mediante l'utilizzo di tecnologia informatica, da disciplinarsi con apposito regolamento;

VISTA la legge 30 dicembre 2020, n. 178, recante il "Bilancio di previsione dello stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023" e, in particolare, l'articolo 1, comma 648, che autorizza la spesa di 9 milioni di euro per lo svolgimento delle elezioni per il rinnovo dei COM.IT.ES. e del Consiglio generale degli italiani all'estero, nonché per l'introduzione in via sperimentale di modalità di espressione del voto in via digitale per lo svolgimento delle medesime elezioni;

VISTA la Raccomandazione CM/Rec (2017) 5 del 14 giugno 2017 del Comitato dei Ministri del Consiglio d'Europa sulle norme relative al voto elettronico, che in considerazione delle preoccupazioni sui potenziali problemi di sicurezza, affidabilità o trasparenza dei sistemi utilizzati per il voto elettronico, ha richiamato l'attenzione sulla necessità che si rispettino i principi delle elezioni democratiche e, in particolare, la segretezza del voto in tutte le fasi della procedura (19), che si trattino i soli dati personali necessari ai fini delle consultazioni elettorali (20), si garantiscano la sicurezza dei dati di autenticazione dei improprio da parte di soggetti non autorizzati (21), non sia fornita all'elettore prova del contenuto del voto espresso al fine di evitarne l'utilizzo improprio da parte di terzi (23), sia impossibile, nella fase di scrutinio, ricostruire un legame tra il voto non sigillato e l'elettore (26), i soggetti cui è affidata la responsabilità della procedura di voto individuino i soggetti autorizzati ad accedere ai sistemi (41), assicurino il corretto funzionamento del sistema di voto (42), provvedano ad effettuare aggiornamenti e manutenzione (43), rispettino opportune misure di sicurezza e gestiscano gli incidenti di sicurezza (44-47), assicurino l'integrità dei dati e la protezione dei dati personali (48), assicurino l'identificazione dei votanti (49);

VISTI il parere del Garante europeo sulla protezione dei dati personali sul pacchetto di misure della Commissione per assicurare elezioni europee libere e corrette (Opinion 10/2018 on the Commission Package on free and fair European elections), e il documento dell'Agenzia Europea per la cyber sicurezza (European Union Agency for Network and Information Security-ENISA-, Opinion paper 02/2019, Election cybersecurity: challenges and opportunities), che, nel richiamare l'attenzione sull'elevato livello di rischio che incombe, nel contesto attuale, su tutti i sistemi informativi utilizzati per l'intero ciclo di gestione delle consultazioni elettorali (dalla tenuta delle liste elettorali allo scrutinio e compilazione dei risultati delle votazioni), derivante da attacchi presunti o reali all'integrità, riservatezza o disponibilità di tali sistemi e reti (che possono utilizzati per minare la credibilità e mettere in dubbio la legittimità del voto) sottolineano che tali rischi sono molto più elevati quando il processo di voto è svolto per via elettronica, evidenziano che i sistemi di voto elettronico generalmente utilizzati, in paesi terzi e nell'UE, presentano vulnerabilità significative e che è rilevante la distinzione tra sistemi di voto elettronico online e offline (cd. ballot stations), in quanto è probabile che i primi comportino un livello di rischio per la sicurezza informatica più elevato rispetto ai secondi; condividono, infine, la raccomandazione agli Stati membri di effettuare una valutazione completa dei rischi associati alle elezioni del Parlamento europeo al fine di identificare potenziali incidenti informatici che potrebbero pregiudicare l'integrità del processo elettorale;

VISTE le Linee guida del Ministero dell'Interno per la sperimentazione di modalità di espressione del voto in via digitale per le elezioni politiche ed europee e per i referendum previsti dagli articoli 75 e 138 della Costituzione limitata a modelli che garantiscano il concreto esercizio del diritto di voto degli italiani all'estero e degli elettori che, per motivi di lavoro, studio o cure mediche, si trovino in un comune di una regione diversa da quella del comune nelle cui liste elettorali risultano iscritti, approvate con decreto del Ministro dell'Interno di concerto con il Ministro per l'Innovazione tecnologica e la Transizione Digitale in data 9 luglio 2021, sulle quali non è stata consultata questa Autorità;

VISTE le note del XX del XX e XX, con le quali il Ministero degli Affari Esteri e della Cooperazione Internazionale (di seguito “Maeci”) ha trasmesso lo schema di decreto in esame, la valutazione di impatto sulla protezione dei dati personali effettuata, ai sensi dell’art. 35 del Regolamento, nonché la documentazione tecnica relativa alle specifiche funzionali e all’architettura tecnico applicativa relativa alla soluzione tecnologica adottata per la sperimentazione del voto elettronico in occasione delle elezioni per il rinnovo dei Comitati degli italiani all’estero che si svolgono entro il 31 dicembre 2021 (di seguito COM.IT.ES 2021);

CONSIDERATO che lo schema di decreto in esame prevede, in particolare, che la sperimentazione del voto elettronico:

- è finalizzata ad acquisire elementi per una analisi tecnico-informativa sulla percorribilità futura del voto elettronico, non è produttiva di effetti giuridici ed è volta a valutare compiutamente se il sistema informatico a tal fine predisposto garantisca il rispetto dei principi di personalità, eguaglianza, libertà e segretezza del voto previsti dall’articolo 48 della Costituzione (art. 2);

- si terrà in occasione delle elezioni dei COM.IT.ES 2021 e riguarderà l’elezione di un campione di 11 Comitati, i cui elettori saranno raggiunti da una campagna informativa effettuata dagli uffici consolari di riferimento, conformemente alle istruzioni diramate dall’amministrazione centrale (art. 3);

- si svolgerà con le seguenti modalità:

  gli elettori sono ammessi, su base volontaria, alla sperimentazione del voto elettronico;

  le istruzioni tecniche per votare e il link per accedere al portale “IOvoto” (portale web creato per supportare la sperimentazione del voto elettronico per le elezioni dei COM.IT.ES 2021) sono pubblicati sul portale “Fast-It” (il portale dei servizi consolari “Farnesina Servizi Telematici per Italiani all'estero”) e sul sito dell’ufficio consolare di riferimento entro il giorno precedente l’inizio delle votazioni elettroniche;

  per ragioni di sicurezza informatica l’ambito temporale nel quale gli elettori possono partecipare alla sperimentazione del voto elettronico da remoto è limitato dal decimo giorno anteriore al termine stabilito per le votazioni e fino alle ore 23:59:59 (ora locale) del giorno stabilito per le elezioni (art. 4);

  l’elettore accede al portale “IOvoto” da un dispositivo informatico personale mediante le credenziali di secondo livello rilasciate dal Sistema pubblico di identità digitale (SPID);

  completata l’autenticazione, l’elettore conferma di aver letto l’informativa sul trattamento dei propri dati personali e autorizza il trattamento ai fini del voto elettronico;

  verificata la presenza dell’elettore nell’elenco degli elettori che hanno presentato valida richiesta di iscrizione nel medesimo elenco tramite il portale “Fast-It”, il sistema assegna automaticamente allo stesso, ad esclusivo uso procedurale interno, un codice di convalida univoco e personale (validation number), volto a disgiungere il voto espresso dall’identificazione dell’elettore;

  una volta espresso il voto, il sistema informatico riproduce sullo schermo la selezione operata, ne richiede conferma e, in caso negativo, consente di ripetere la procedura;

  dopo la conferma, il voto è trasmesso tramite la rete Internet in modalità criptata alla banca dati preposta, dove è disaccoppiato da ogni riferimento dell’elettore e rimane crittografato e sigillato fino al momento dello spoglio elettronico; dopo la conferma del

voto, il voto non è ripetibile e l'elettore riceve tramite il sistema di voto un'attestazione in formato elettronico dell'avvenuto voto sperimentale, la quale non mostra il voto e le preferenze espresse (art. 5);

- per quanto riguarda la fase dello scrutinio, dopo la conclusione delle operazioni di voto in tutte le circoscrizioni interessate, una Commissione composta di 5 membri designata dalle Direzioni generali del Ministero coinvolte nella sperimentazione, compie, mediante accesso al portale "IOvoto", le seguenti operazioni:

per ciascuno dei COM.IT.ES. accerta che abbiano partecipato al voto elettronico almeno venti elettori; per i Comitati per i quali ha partecipato un numero di elettori pari o inferiore a venti, interrompe le operazioni di spoglio;

in relazione ai Comitati per i quali hanno partecipato al voto elettronico almeno venti elettori, visualizza i voti elettronici espressi, accerta il numero dei votanti, delle schede bianche e dei voti validamente espressi per ciascuna lista e per ciascun candidato, redige il verbale delle operazioni effettuate, corredate dai report acquisiti dal portale "IOvoto" e dei relativi esiti (art. 5);

- per quanto riguarda i profili tecnici:

il sistema sperimentale per il voto elettronico da remoto è ospitato presso un Cloud Service Provider qualificato dall'Agenzia per l'Italia digitale; nelle more della piena operatività del perimetro di sicurezza nazionale cibernetica e del polo strategico nazionale (o cloud pubblico), il Ministero ha individuato un Cloud Service Provider con i necessari requisiti di affidabilità e sicurezza dal punto di vista infrastrutturale e organizzativo, non potendo disporre, allo stato, di risorse disponibili procedere ad una modifica dell'infrastruttura informatica del Ministero tale da garantire i requisiti sopra menzionati (art. 5);

il codice sorgente dell'applicazione e i dettagli implementativi e infrastrutturali sono pubblicati su siti aperti almeno trenta giorni prima della data di inizio delle operazioni di voto elettronico (art. 7);

il sistema di voto elettronico gestito dal Maeci tratta esclusivamente i dati personali necessari per lo svolgimento delle elezioni elettroniche, che sono conservati, mantenendo la separazione tra i dati personali ed il voto espresso, sul cloud del fornitore di servizi fino a un massimo di novanta giorni ai fini della valutazione tecnica della sperimentazione, e allo scadere di tale termine e fino a un massimo di sei mesi, sul data center del Maeci, ai fini dell'analisi complessiva della sperimentazione, tenuto conto delle valutazioni tecniche effettuate dal fornitore (art. 8);

prima della sperimentazione sono svolte sessioni di voto fittizio, gestite e valutate dalle Direzioni generali del Ministero coinvolte (art. 7);

al termine della sperimentazione le predette Direzioni generali effettuano l'analisi funzionale e tecnica e redigono una relazione congiunta riguardante gli esiti della sperimentazione e la percorribilità futura della modalità di voto elettronico, pubblicata sul sito istituzionale del Ministero e trasmessa alle amministrazioni incaricate di redigere le linee guida per la sperimentazione del voto elettronico ai sensi dell'articolo 1, commi 627 e 628, della legge 27 dicembre 2019, n. 160 (art. 6);

RILEVATO che, sulla base della documentazione trasmessa unitamente allo schema di decreto - valutazione di impatto sulla protezione dei dati personali, documentazione relativa alle specifiche funzionali e architettura tecnico applicativa del portale per il voto elettronico - gli aspetti tecnici

sono stati ulteriormente descritti come di seguito:

il Portale “IOVoto” è ospitato all’interno della infrastruttura Cloud di Oracle presso il Data Center Oracle di Francoforte;

il portale “IOvoto” - al fine di creare una procedura con garanzie di segretezza analoghe a quelle assicurate mediante il voto espresso presso il seggio elettorale - fa uso di due applicativi distinti (“APP A” e “APP B”) che, mantenendo separati i dati dell’espressione di voto dai dati relativi agli elettori, disaccoppiano l’identità dell’elettore dal voto espresso, in quanto “APP B”, dove è indicata la preferenza, non conosce in nessun modo a quale utente sia stato attribuito un particolare validation number; e “APP A”, dove viene autenticato l’utente, non conosce in nessun modo quale sia il voto espresso;

il portale prevede anche una terza applicazione, BackOffice, ad uso esclusivo degli operatori MAECI abilitati, che permette di erogare la documentazione relativa ai risultati del voto;

i dati utilizzati sono memorizzati in due layer distinti in tecnologia blockchain dedicati, rispettivamente, all’applicativo A ed all’applicativo B. I dati anagrafici sono memorizzati esclusivamente nella blockchain dedicata all’applicativo A, per garantire la segretezza del voto;

il validation number è costituito da una stringa numerica di 8 cifre (generata randomicamente e con controllo anti-collisione), creata nel momento in cui un utente autenticato accede alla piattaforma di voto;

il valore hash del validation number è memorizzato in blockchain, in modo da consentire a “APP B” di verificare la validità del validation number presentato dall’utente anonimo in fase di procedura di voto;

i dati sono protetti mediante cifratura sia at rest (dati residenti sull’infrastruttura cloud e dati utilizzati dalle applicazioni) sia in transit (dati scambiati con il dispositivo utilizzato dall’elettore);

le chiavi di cifratura sono nella disponibilità esclusiva del Maeci;

gli elettori accedono al portale tramite identità SPID di livello 2, al fine di garantire la corretta identificazione dell’elettore

CONSIDERATO che il Maeci si accinge, seppure in via sperimentale e senza validità giuridica, a trattare i dati degli interessati nell’ambito di un procedimento di voto, e che gli esiti della sperimentazione costituiranno una base per impostare eventuali future iniziative di voto elettronico, si ritiene utile evidenziare i seguenti profili di criticità, anche al fine di indirizzare le analisi che verranno effettuate nell’ambito della sperimentazione:

- con riferimento alla previsione dell’autorizzazione del trattamento dei dati personali ai fini del voto elettronico (art. 5) si evidenzia che il consenso dell’elettore alla partecipazione alla sperimentazione - prevista facoltativamente e senza alcuna conseguenza sul diritto di voto, (artt. 2 e 5, comma 2, lett. a)

- non deve essere confuso con il consenso al trattamento dei dati personali previsto dal Regolamento, quale base giuridica del trattamento; il considerando 43 del Regolamento indica infatti chiaramente che è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, ritenendo che esistano altre basi legittime, in linea di

principio più appropriate, per il trattamento da parte delle autorità pubbliche. Nel caso in esame, infatti, tale base giuridica deve essere ricondotta alle disposizioni legislative che introducono la sperimentazione del voto elettronico nonché al presente schema di decreto che ne disciplina le modalità e che espressamente dispone che la partecipazione dell'elettore sia facoltativa.

- con riferimento all'utilizzo delle medesime liste elettorali di candidati del procedimento elettorale per il rinnovo dei COM.IT.ES. (art. 5), trattandosi di una iniziativa sperimentale che in ogni caso non è volta a verificare la corrispondenza con il voto reale, benchè siano adottate talune garanzie per assicurare la segretezza del voto e, in particolare, quelle che prevedono l'esclusione dallo scrutinio delle sezioni con meno di 20 votanti, si suggerisce di prevedere che tale sperimentazione sia svolta ricorrendo a liste elettorali di fantasia; in alternativa a tale ipotesi, si suggerisce che nella campagna informativa o nelle istruzioni di voto, i partecipanti siano invitati ad indicare un voto diverso rispetto a quello espresso nella consultazione elettorale;

- con riferimento alle modalità di comunicazione all'elettore del validation number, nel rilevare dei disallineamenti nella documentazione esaminata - tali per cui non è chiaro se tale invio avvenga tramite posta elettronica o avvenga per il tramite delle applicazioni utilizzate per la sperimentazione - si ritiene che l'invio per posta elettronica del validation number non costituisca una misura idonea a garantire la riservatezza di tale codice di controllo e quindi ad impedire la votazione da parte di soggetti non aventi diritto, in violazione del principio di personalità del voto;

- relativamente alle modalità di accesso alle applicazioni di voto da parte degli elettori che partecipano alla sperimentazione, si osserva che non sono state adeguatamente considerate le potenziali criticità legate all'uso di dispositivi elettronici personali (pc, smartphone, tablet) o postazioni condivise (internet point pubblici), che non possono, a priori, garantire idonei livelli di sicurezza e di protezione del dispositivo stesso, né assicurare un utilizzo esclusivo da parte del votante;

- per quanto riguarda la necessità di identificare in modo certo l'elettore e di garantire, allo stesso tempo, la segretezza del voto, si ritiene opportuno che, in sede di analisi della sperimentazione, siano considerate tutte le possibili forme di tracciamento del processo di voto dell'elettore che possono essere rinvenute nei sistemi informativi coinvolti nonché l'eventualità di re-identificazione di un interessato anche attraverso informazioni apparentemente anonime (c.d. "single-out") in caso, ad esempio, di voto espresso in determinate fasce orarie o da determinate località;

- con riferimento, in particolare, alla previsione dell'invio all'elettore di un'attestazione in formato elettronico dell'avvenuto voto sperimentale – che non mostra il voto e le preferenze espresse - occorre prevedere idonee garanzie tese ad evitare che il timing dell'invio/ricezione del messaggio non sia utile a re-identificare il votante mediante l'associazione con il timing del voto espresso;

- in merito all'utilizzo di SPID, si evidenzia che la tracciatura dei servizi acceduti, che i Gestori dell'identità digitale (c.d. Provider SPID) sono tenuti ad effettuare ai sensi del Regolamento recante le Regole tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014) (c.d. Regole tecniche SPID) potrebbe costituire un pregiudizio per gli interessati in quanto rende possibile per l'Identity Provider rilevare chi ha esercitato il voto in determinate tornate elettorali. Si invita pertanto il Maeci ad esaminare tale problematica ed a individuare soluzioni tecnico-organizzative che, garantendo il rispetto della normativa tecnica SPID, possano ridurre il rischio per i diritti e le libertà fondamentali degli interessati;

RITENUTA la necessità che il Maeci, in sede di analisi della sperimentazione, tenga conto delle criticità sopra evidenziate, nonché di tutti i possibili rischi incombenti, più in generale, sulle procedure di voto elettronico evidenziati anche nei documenti adottati in ambito europeo e sopra richiamati;

CONSIDERATO che il Maeci ha effettuato la valutazione di impatto sai sensi dell'art. 35 del Regolamento, in quanto i trattamenti di dati personali effettuati nel contesto della sperimentazione del voto elettronico per il rinnovo dei COM.IT.ES. 2021 riguardano un numero di interessati potenzialmente elevato rispetto alla popolazione di riferimento, una portata geografica consistente, il trattamento di dati particolari come le opinioni politiche e l'utilizzo innovativo di soluzioni tecnologiche quali la Blockchain;

RILEVATO che la predetta valutazione di impatto reputa che il rischio residuo dopo l'adozione delle ulteriori misure per mitigare i rischi elevati presentati dal trattamento sia complessivamente basso o trascurabile;

RILEVATO che lo schema di decreto in esame tiene conto delle indicazioni fornite dall'Ufficio nel corso delle interlocuzioni informali con il Maeci, che hanno riguardato, in particolare:

- la necessità di alcune integrazioni al testo del decreto volte ad esplicitare il ruolo svolto dal Ministero e dagli altri soggetti coinvolti (es. Cloud service provider, altri) nel trattamento dei dati personali connessi alla sperimentazione;

- la necessità che il termine di conservazione dei dati, sia da parte del Cloud Service Provider individuato che da parte del Maeci, sia indicato e giustificato dallo svolgimento di specifiche finalità che è opportuno siano esplicitate anche nel testo del decreto, e non solo nella documentazione tecnica;

- alcune misure tecniche, volte a garantire il corretto trattamento e la sicurezza dei dati personali dei votanti;

- le misure aggiuntive che il Maeci, avendo individuato un responsabile del trattamento (Cloud service Provider) che fa parte di un gruppo la cui società capogruppo ha sede negli Stati Uniti, in qualità di esportatore è tenuto ad adottare, in caso di trasferimento di dati personali in paesi al di fuori dell'Unione Europea al fine di garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dal Regolamento (cfr. le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", adottate dal Comitato europeo per la protezione dei dati il 10 novembre 2020), consistenti nella cifratura dei dati personali trattati da parte del responsabile del trattamento, con chiavi di cifratura nella disponibilità esclusiva del Maeci;

RITENUTO pertanto di esprime parere favorevole in merito allo schema esaminato, ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. c), del Regolamento, risultando conforme ai principi stabiliti in materia di protezione dei dati personali dal Regolamento e dal Codice;

RITENUTO altresì, alla luce di quanto osservato, che le criticità sopra evidenziate in ordine ai profili di protezione dei dati personali, dovranno, all'esito del completamento della fase sperimentale oggetto del presente parere, essere tenute nella massima considerazione ai fini dell'analisi tecnico organizzativa in ordine alla percorribilità futura del voto elettronico;

CONSIDERATO che la sperimentazione del voto con modalità elettroniche dovrà essere avviata a decorrere dal 24 novembre 2021, decimo giorno anteriore al termine stabilito per le votazioni per il rinnovo dei Com.It.Es. del 3 dicembre 2021, affiancandosi al tradizionale voto per corrispondenza con scheda cartacea;

RITENUTO, quindi, che ricorrono i presupposti per l'applicazione dell'art. 5, comma 8, del regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante, il quale prevede che «Nei casi di particolare urgenza e di indifferibilità che non permettono la convocazione in tempo utile del Garante, il presidente può adottare i provvedimenti di competenza dell'organo, i quali cessano di avere efficacia sin dal momento della loro adozione se non sono ratificati dal Garante nella prima riunione utile, da convocarsi non oltre il trentesimo giorno»;

Vista la documentazione in atti

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. c), del Regolamento, esprime parere favorevole sullo schema di decreto del Ministero degli affari esteri e della cooperazione internazionale concernente la sperimentazione del voto elettronico in occasione delle elezioni per il rinnovo dei Comitati degli italiani all'estero che si svolgono entro il 31 dicembre 2021.

Roma, 19 novembre 2021

IL PRESIDENTE
Stanzione