PARERE APPROVATO DALLA COMMISSIONE SULL'ATTO DEL GOVERNO N. 10

La Commissione, esaminato lo schema di decreto legislativo in titolo

premesso che:

- lo schema di decreto in esame recepisce la direttiva (UE) 2016/1148 (cosiddetta "direttiva NIS - *Network and information security*"), finalizzata ad assicurare un elevato livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione;

- in armonia con gli obiettivi e le previsioni della direttiva, lo schema, oltre che al miglioramento delle capacità nazionali in materia di *cyber security*, è volto a rafforzare la cooperazione sia a livello nazionale che nell'ambito dell'Unione europea e a promuovere meccanismi di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, con particolare riferimento agli operatori dei servizi essenziali e ai fornitori di servizi digitali,

considerato che:

- il Capo I contiene le disposizioni generali. In particolare, l'articolo 1 definisce l'oggetto e l'ambito di applicazione del decreto; l'articolo 2, ai fini del trattamento dei dati personali in applicazione delle disposizioni introdotte, richiama quanto disposto dal decreto legislativo n. 196 del 2003; l'articolo 3 chiarisce le definizioni utilizzate nel testo; l'articolo 4 prevede che le autorità competenti in materia di sicurezza delle reti e dei sistemi informativi debbano identificare, per ciascun settore e sottosettore di cui all'Allegato II allo schema, gli operatori di servizi essenziali con una sede nel territorio nazionale. Si tratta, in particolare, dei settori dell'energia, dei trasporti, del settore bancario, delle infrastrutture dei mercati finanziari, del settore sanitario, della distribuzione di acqua potabile e delle infrastrutture digitali; l'articolo 5 specifica quali siano i fattori da prendere in considerazione per determinare la rilevanza degli effetti negativi di incidenti informatici nella fornitura di servizi essenziali;

- il Capo II delinea il contesto strategico ed istituzionale preposto alla gestione delle attività finalizzate alla sicurezza delle reti. In particolare, all'articolo 6, si prevede l'adozione, da parte del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), della strategia nazionale, di sicurezza cibernetica per la tutela delle reti e dei sistemi di interesse nazionale, nonché delle linee di indirizzo per la sua attuazione; l'articolo 7 individua le autorità competenti NIS, responsabili dell'attuazione del decreto in relazione sia ai settori di cui all'Allegato II, sia ai servizi digitali specificati nell'Allegato III; con l'articolo 8 si istituisce, presso la Presidenza del Consiglio, il Gruppo di intervento per la sicurezza informatica in caso di incidente - CSIRT, che svolge le funzioni finora affidate al *Computer emergency response team* (CERT), incardinato presso il Ministero dello sviluppo economico, nonché al CERT-PA, già operante presso l'Agenzia per l'Italia digitale; l'articolo 9 disciplina la collaborazione tra le autorità competenti NIS, il punto di contatto unico e il CSIRT italiano per l'adempimento degli obblighi introdotti dallo schema;

- il Capo III disciplina la cooperazione a livello europeo. L'articolo 10, in particolare, definisce i compiti del punto di contatto unico nell'ambito della partecipazione al gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione e dell'Agenzia dell'Unione

europea per la sicurezza delle reti e dell'informazione (ENISA); l'articolo 11 prevede la partecipazione del CSIRT italiano alla rete degli analoghi organismi costituiti dagli Stati membri e dall'Unione europea;

- il Capo IV riguarda la sicurezza della rete e dei sistemi informativi degli operatori dei servizi essenziali. In particolare con l'articolo 12 vengono definiti gli obblighi degli operatori, innanzitutto in materia di sicurezza, con la previsione che essi adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi per la sicurezza della rete e dei sistemi informativi utilizzati, anche al fine di prevenire e minimizzare l'impatto di incidenti che possano compromettere la continuità dei servizi erogati; l'articolo 13 stabilisce che l'autorità competente NIS valuti il rispetto degli obblighi imposti agli operatori di servizi essenziali, nonché i relativi effetti sulla sicurezza;

- il Capo V riguarda la sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali. Con l'articolo 14, ai fornitori è imposto l'obbligo di adottare misure tecnico-organizzative che facilitino la gestione dei rischi e la riduzione dell'impatto di eventuali incidenti informatici, nonché quello di notificare gli incidenti con impatto significativo, individuati secondo parametri specificati nel testo; l'articolo 15 prevede la possibilità che, qualora sia dimostrato il mancato rispetto degli obblighi da parte dei fornitori di servizi digitali, l'autorità competente NIS possa adottare misure di vigilanza *ex post* adeguate alla natura dei servizi e delle operazioni successivamente al verificarsi di un incidente; l'articolo 16 stabilisce che un fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale e specifica che un fornitore è comunque considerato avere il proprio stabilimento principale in uno Stato membro quando ha la sua sede in tale Stato membro;

- nel Capo VI, l'articolo 17 affida alle autorità competenti NIS il compito di promuovere l'adozione di norme europee o internazionali sulla sicurezza delle reti e dei sistemi informativi senza privilegiare particolari tecnologie; l'articolo 18 riguarda invece la possibilità di notifiche volontarie di incidenti aventi un impatto rilevante sulla continuità dei servizi prestati da parte dei soggetti che non siano stati identificati come operatori di servizi essenziali o non siano fornitori di servizi digitali;

- al Capo VII gli articoli 19 e 20 individuano le autorità competenti sia per lo svolgimento delle attività di ispezione e verifica introdotte dal decreto sia per l'accertamento delle violazioni e l'irrogazione delle sanzioni amministrative; la definizione delle sanzioni amministrative è contenuta nell'articolo 21 e prevede un importo che varia da dodicimila a centocinquantamila euro, differenziato tra operatori di servizi essenziali e fornitori di servizi digitali, nonché in base al tipo di violazione; l'articolo 22 reca infine la copertura finanziaria del provvedimento,

esprime parere favorevole, con le seguenti osservazioni:

- con riferimento all'articolo 8, riguardante l'istituzione dei Gruppi di intervento per la sicurezza informatica in caso di incidente - CSIRT, si segnala la necessità di fornire ulteriori chiarimenti circa la quantificazione dell'onere relativamente all'assunzione di quindici unità di personale, nonché con riguardo ai possibili profili di onerosità relativi al trattamento accessorio di cui godrà il personale posto in posizione di comando o fuori ruolo;

- sempre con riferimento all'articolo 8, appare, inoltre, opportuno che i tecnici da assumere all'interno dei gruppi di intervento per la sicurezza informatica, in ragione della complessità e rilevanza del loro compito per la sicurezza del Paese, abbiano competenze specifiche ed esperienza, con particolare riguardo ad alcune materie: *data protection*; *disaster recovery*; resilienza; *storage*

resource management; creazione, gestione, mantenimento e rimodulazione di *business continuity plan*; *big data*; virtualizzazione; convergenza;

- con riguardo all'articolo 12, relativo agli obblighi in materia di sicurezza e notifica degli incidenti, appare necessario fornire i dati e gli elementi informativi relativi alle attività da porre in essere e ai relativi costi, nonché alle risorse già disponibili, al fine di valutare l'asserita neutralità finanziaria della disposizione;

- con riferimento all'articolo 21, che prevede un articolato sistema di sanzioni amministrative, si segnala l'opportunità di riconsiderare l'entità degli importi, con riguardo ai principi di proporzionalità e ragionevolezza, valutando altresì la possibilità di elevare il limite massimo delle sanzioni, dal momento che le grandi aziende dell'*information technology* hanno valori di capitalizzazione particolarmente elevati e usufruiscono di condizioni fiscali più favorevoli.