Servizio studi del Senato

Elementi di valutazione sui progetti di atti legislativi dell'UE

N. 16

ELEMENTI PER LA VALUTAZIONE DEL RISPETTO DEL PRINCIPIO DI SUSSIDIARIETÀ E DI PROPORZIONALITÀ

TITOLO ATTO:	Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148
NUMERO ATTO	COM(2020) 823
NUMERO PROCEDURA	2020/0359 (COD)
AUTORE	Commissione europea
DATA DELL'ATTO	16/12/2020
DATA DI TRASMISSIONE	19/01/2021
SCADENZA OTTO SETTIMANE	17/03/2021
ASSEGNATO IL	20/01/2021
DEFERIMENTO PER MERITO	8ª Commissione permanente
OGGETTO	La proposta abroga la direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS) - il primo strumento legislativo a livello dell'UE sulla cibersicurezza - e prevede misure giuridiche volte a incrementare il livello complessivo di cibersicurezza nell'Unione.
BASE GIURIDICA	Articolo 114 del Trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali.
PRINCIPI DI SUSSIDIARIETÀ E PROPORZIONALITÀ	Come evidenziato dalla Commissione europea la proposta in esame è conforme al principio di **sussidiarietà** in termini di: necessità dell'intervento delle istituzioni dell'Unione in quanto l'obiettivo della direttiva, vale a dire conseguire un elevato livello comune di cibersicurezza nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a causa degli effetti transfrontalieri dell'azione prevista, può essere conseguito meglio a livello dell'Unione, in conformità al principio di sussidiarietà sancito dall'articolo 5 del Trattato sull'Unione europea (TUE);

valore aggiunto per l'Unione per le potenzialità degli interventi dell'UE volti a migliorare e agevolare strategie nazionali efficaci, anche per quanto concerne la protezione dei dati e della vita privata.

La Commissione europea dichiara la proposta conforme al principio di **proporzionalità** poiché si limita a quanto necessario per il raggiungimento degli obiettivi prefissati.

*Ai sensi dell'art. 6 della legge n. 234/2012, la presente proposta è stata **segnalata dal Governo fra gli atti dell'Unione di particolare interesse nazionale.** Non risulta ancora pervenuta la relazione governativa prevista dall'art. 6, comma 5, della medesima legge.*

1) CONTESTO NORMATIVO

La proposta fa parte di un insieme più ampio di strumenti giuridici e di iniziative a livello dell'Unione volte ad aumentare la resilienza di soggetti pubblici e privati alle minacce nel settore della cibersicurezza. Si segnalano in particolare: la direttiva (UE) 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche (le cui disposizioni relative alla cibersicurezza saranno sostituite con le disposizioni della proposta in esame); la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario (COM(2020)595); la proposta di direttiva sulla resilienza dei soggetti critici (COM(2020)365); la strategia dell'UE per l'Unione della sicurezza (COM(2020)605).

2) SINTESI DELLE MISURE PROPOSTE

La Commissione propone l'abrogazione della direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informatici nell'Unione (direttiva NIS) con l'intento di modernizzare il quadro giuridico esistente alla luce della crescente digitalizzazione del mercato interno e della rapida evoluzione delle minacce alla cibersicurezza, fenomeni che si sono ulteriormente amplificati dall'inizio della crisi COVID-19.

La valutazione del funzionamento della direttiva NIS, condotta ai fini della valutazione d'impatto (cfr. SWD(2020)344 e SWD(2020)345), ha identificato i seguenti problemi: 1) il basso livello di ciberresilienza delle imprese operanti nell'UE; 2) i diversi livelli di resilienza fra Stati membri e fra settori; 3) il basso livello di "consapevolezza situazionale comune" e la mancanza di una risposta comune alle crisi. La maggioranza delle autorità competenti e delle imprese si è mostrata favorevole a una revisione della direttiva NIS. Secondo le stime fornite dalla Commissione europea, l'opzione strategica prescelta apporterebbe una riduzione, pari a 11,3 miliardi di euro, dei costi degli incidenti di cibersicurezza.

Principali obiettivi del riesame sono:

1. **aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea**;
2. **ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva vigente** (obiettivo specifico sarà quello di garantire lo stesso regime normativo e un livello comparabile di risorse fra gli Stati membri);
3. **migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta** (l'opzione strategica prescelta prevede meccanismi volti a promuovere una maggiore fiducia fra Stati membri incentivando la condivisione di informazioni e garantendo un approccio maggiormente operativo, attraverso la designazione delle autorità nazionali competenti responsabili della gestione di incidenti e crisi su vasta scala).

La proposta è strutturata attorno a diversi settori di intervento principali: **a)** fa obbligo agli Stati membri di adottare una strategia nazionale per la cibersicurezza (artt. da 5 a 11) e di designare autorità nazionali competenti, punti di contatto unici e *team* di risposta agli incidenti di sicurezza informatica - CSIRT (artt. da 12 a 16); **b)** stabilisce obblighi di gestione e segnalazione dei rischi di cibersicurezza per i soggetti indicati come "soggetti essenziali" all'allegato I e come "soggetti importanti" all'allegato II (artt. da 17 a 23); **c)** stabilisce obblighi in materia di condivisione delle informazioni sulla cibersicurezza (artt. 26 e 27).

Prevede inoltre che alcuni tipi di soggetti (fornitori di servizi DNS, registri dei nomi di dominio di primo livello, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center* e fornitori di reti di distribuzione dei contenuti, nonché alcuni fornitori di servizi digitali) siano sottoposti alla giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrà creare e mantenere un registro dei soggetti di quest'ultimo tipo (artt. 24 e 25). Gli artt. da 28 a 34 definiscono infine gli aspetti relativi alla vigilanza e all'imposizione di sanzioni.

---

12 febbraio 2021

A cura di: Viviana Di Felice