Corrado Giustozzi

Audizione davanti le Commissioni riunite I e XI per l'esame del disegno di legge C.2100

Corrado Giustozzi

Advisory Group, ENISA

Considerazioni generali

Corrado Giustozzi

- Il Perimetro introduce un concetto complementare a quanto già istituito mediante il recepimento della Direttiva NIS. Mentre infatti lo scopo della NIS è quello di assicurare, a livello comune europeo, un elevato livello di sicurezza e resilienza ai servizi essenziali per il funzionamento della società civile, lo scopo del Perimetro è difendere gli interessi vitali dell'Italia innalzando il livello di protezione su tutti quei servizi da cui dipende, direttamente o indirettamente, la sicurezza nazionale.
- Molto opportunamente, dunque, la norma chiude il cerchio sulla protezione del Paese imponendo agli operatori, pubblici e privati, che erogano servizi critici per lo Stato di ottemperare a specifiche misure di prevenzione e protezione per minimizzare i rischi di incidenti, disfunzioni, interruzioni e malfunzionamenti ai propri servizi ed alle infrastrutture sottostanti.

Aspetti problematici

Corrado Giustozzi

- Potenziali conflitti sulle funzioni di vigilanza verso il settore pubblico
- Tempistiche articolate e stringenti

Potenziali conflitti riguardanti la vigilanza: contesto

Corrado Giustozzi

- La versione precedente del DL (approvata dal CdM il 19 luglio 2019) prevedeva che la responsabilità delle attività di vigilanza e controllo sul settore pubblico fosse affidata ad AgID, mentre nella versione attualmente vigente il soggetto vigilante è individuato nella Presidenza del Consiglio
- È corretto e coerente che la Presidenza del Consiglio, in continuità col suo ruolo già centrale nella cybersecurity nazionale, accentri in sé le funzioni di vigilanza e controllo sugli operatori pubblici del Perimetro
- Tuttavia lo spostamento “sulla carta” della relativa competenza, senza una più approfondita analisi del contesto operativo preesistente, introduce alcune problematiche e/o aspetti di incoerenza che andrebbero opportunamente indirizzati e risolti con previsioni di maggior dettaglio

Potenziali conflitti riguardanti la vigilanza

Corrado Giustozzi

- AgID per mandato già emette norme tecniche e svolge attività di accreditamento e vigilanza su determinati operatori che erogano servizi rilevanti per la collettività e per lo Stato:
  - Certificatori di firme digitali
  - Fornitori di servizi fiduciari (in particolare, identità digitali eIDAS-SPID)
  - Fornitori di servizi di Posta Elettronica Certificata
  - Operatori della conservazione digitale sostitutiva
- Se alcuni degli operatori appartenenti a queste categorie dovessero rientrare tra i soggetti del Perimetro si verrebbero a creare aspetti di incoerenza o conflitto riguardanti i seguenti aspetti operativi:
  - all'accreditamento di quale autorità sarebbero soggetti?
  - alla vigilanza di quale autorità sarebbero soggetti?
  - alle norme tecniche di quale autorità dovrebbero adeguarsi?

Potenziali problematiche riguardanti i tempi

Corrado Giustozzi

- Il DL stabilisce tempi piuttosto sfidanti per l'istituzione e la messa a regime di un complesso sistema di accreditamento e vigilanza
- L'AgID, così come il MiSE, possiede già le competenze tecniche, le risorse e i processi per svolgere le attività di vigilanza, che già svolge da tempi precedenti nei confronti di operatori di servizi rilevanti per lo Ststo
- Una struttura tecnica creata ex novo nella PCM potrebbe invece aver bisogno di un tempo maggiore rispetto a quanto previsto dal DL per poter acquisire le risorse, sviluppare le competenze tecniche ed operative, e mettere a punto i processi necessari per poter condurre in modo efficace le attività di vigilanza e controllo richieste dalla norma

Interazioni con altre norme da emanarsi

Corrado Giustozzi

- Per quanto riguarda le attività di notifica degli incidenti il DL riconduce gli operatori al medesimo circuito istituito ai sensi del DL 65 (recepimento della Direttiva NIS), che prevede la comunicazione allo CSIRT Italiano
- Attualmente però lo CSIRT Italiano opera in modalità provvisoria, non essendo ancora stato emanato il previsto DPCM attuativo, e dunque le attività dello CSIRT sono svolte dal CERT Nazionale (MiSE) e dal CERT-PA (AgID) che cooperano tra loro
- Se il DPCM attuativo dell'istituzione dello CSIRT Italiano non venisse emanato per tempo, l'AgID per tramite del CERT-PA si troverebbe a dover di fatto esercitare un'attività critica all'interno del Perimetro (svolgendo in parte le funzioni di CSIRT Italiano) senza tuttavia avere un ruolo all'interno dello stesso, in asimmetria rispetto alla funzione svolta dal MiSE tramite il CERT Nazionale

Corrado Giustozzi

GRAZIE PER L'ATTENZIONE