

**POSIZIONE SULLO SCHEMA DECRETO LEGISLATIVO RECANTE
ATTUAZIONE DELLA DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO
EUROPEO E DEL CONSIGLIO DEL 6 LUGLIO 2016, RECANTE MISURE
PER UN LIVELLO COMUNE ELEVATO DI SICUREZZA DELLE RETI E DEI
SISTEMI INFORMATIVI NELL'UNIONE**

Parere, ai sensi dell'articolo 9, del decreto legislativo 28 agosto 1997, n. 281

Punto 8) O.d.g. Conferenza Unificata

Premessa

Le Regioni e Province Autonome condividono l'esigenza e l'obbligo a fronte della Direttiva Europea di strutturare un sistema nazionale che possa garantire un adeguato livello di sicurezza delle reti e dei sistemi informativi **a partire dai servizi essenziali**, tuttavia ritengono che tale strutturazione si debba ispirare ad alcuni principi fondamentali:

- permettere la sostenibilità attuativa nelle amministrazioni coinvolte direttamente o indirettamente dagli effetti del decreto;
- migliorare la semplicità organizzativa e garantire una governance adeguata;
- orientare il sistema sanzionatorio ad essere efficace per i soggetti che governano i sistemi informativi dei servizi essenziali.

Rispetto ai principi indicati la proposta del governo sembra non offrire tutte le rassicurazioni attese, per questo il presente documento intende offrire alcuni contributi che possano maggiormente orientare lo schema di decreto nelle direttrici auspiccate.

Criticità principali

Le Regioni e Province Autonome ritengono che rispetto ai principi indicati il testo proposto di decreto debba risolvere alcune criticità fondamentali:

- in merito alla sostenibilità attuativa nelle amministrazioni coinvolte direttamente o indirettamente dagli effetti del decreto appare che lo schema di decreto in esame agisca in modo non perfettamente completo sulle prime e non ritenga necessario intervenire sulle seconde. Per le Regioni e Province Autonome al contrario è fondamentale agire sulle leve finanziarie di tutte le amministrazioni coinvolte. In particolare per le amministrazioni coinvolte direttamente è necessario garantire le risorse oltre che per le strutture centrali, così come già previsto dal decreto, anche per le strutture regionali coinvolte nella co-gestione, in particolare per l'individuazione degli operatori di servizi essenziali, dei Nis Sanità e Ambiente

(articolo 4 comma 1 e articolo 7 comma 1), risorse necessarie per lo svolgimento delle attività di coordinamento e raccordo con il Ministero della Salute e con il Ministero dell'Ambiente. Per le attività indirette il decreto richiede da parte di tutti i soggetti coinvolti nell'erogazione dei servizi essenziali ed in particolare delle Pubbliche Amministrazioni ai diversi livelli istituzionali, un grande sforzo organizzativo ed economico per garantire e possibilmente migliorare continuamente il livello di sicurezza dei sistemi interessati e per garantire le funzionalità di alert e di rilevazione degli incidenti per dare le tempestive notifiche previste, per questo quanto previsto al comma 2 dell'articolo 22, per cui dall'attuazione del decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica, ad eccezione di quanto previsto agli articoli 7 ed 8, non pare essere coerente, soprattutto in considerazione dei vincoli imposti nell'ambito della finanza pubblica da parte della legge finanziaria 2016 articolo 1 commi 512-520 che al contrario impongono una razionalizzazione della spesa ICT. Si ritiene pertanto necessario che il comma 2 dell'articolo 22 venga rivisto al fine di contenere espliciti riferimenti coerenti con la norma vigente e con le circolari interpretative di AgID e del MEF che consentano nel rispetto dei vincoli di bilancio e di spesa pubblica previsti, la possibilità di effettuare gli investimenti necessari a garantire gli adeguati livelli di sicurezza e la relativa organizzazione conformi ai dettami del presente decreto e dei successivi regolamenti e linee guida previsti. Inoltre si sottolinea la necessità, soprattutto in ambito sanitario, nel dar seguito ai necessari DM o accordi richiamati nello schema del decreto (articolo 4 comma 1 e articolo 19 comma 2), di definire - in maniera omogenea nel territorio – un piano di attuazione che illustri le misure sostenibili per l'attuazione e identifichi (ove applicabile) le fonti di copertura economico-finanziaria a disposizione. Si propone, pertanto, di valutare l'inserimento nello schema di decreto di un richiamo relativo alla necessità di definire per l'attuazione delle “misure sostenibili”.

- in merito all'organizzazione ed alla governance, essendo già in essere prima del decreto il DIS, il CERT e il CERT-PA, ed essendo prevista l'individuazione dei NIS, secondo le indicazioni europee (energia, trasporti, finanza, sanità e ambiente), oltre al comitato di coordinamento per la cooperazione nazionale presso la Presidenza del Consiglio dei Ministri (articolo 9), si ritiene che l'istituzione del CSIRT presso la Presidenza del Consiglio dei Ministri prevista dall'articolo 8 del decreto non faciliti la semplificazione e razionalizzazione ed immediata operatività del Csirt stesso e delle politiche del digitale in generale e quindi pur prendendo atto delle scelte governative si chiede e si raccomanda una riflessione aggiuntiva in merito. Così come si invita a riflettere sull'opportunità di un unico Csirt centrale che possa quindi configurarsi come un possibile single point of failure e se non sia piuttosto opportuno un minimo di strutturazione territoriale, sia per assecondare meglio alcuni servizi essenziali che sono a carattere fortemente territoriale (sanità e ambiente), sia per garantire più facilmente quelle caratteristiche di resilienza della struttura di comunicazione sulla sicurezza previste dalla direttiva europea;

- in merito al sistema sanzionatorio, premesso che gli importi delle sanzioni sono decisamente elevati, si sottolinea come gli stessi possano impattare negativamente sulle strutture pubbliche individuate quali operatori pubblici di servizi essenziali (sanità ad esempio), si richiede pertanto di rivalutare il dimensionamento degli importi o in subordine di prevedere un periodo iniziale di 12 o 24 mesi di riduzione in percentuale degli importi minimi e massimi previsti. Inoltre si propone di valutare l'opportunità/necessità di esplicitare le modalità di utilizzo delle eventuali sanzioni, ad esempio prevedendo il vincolo di utilizzo per interventi attuativi (informazione, formazione, disseminazione) per misure di sicurezza nel medesimo settore/ambito e competenza territoriale ove la sanzione è stata elevata.

Coerentemente con i principi sopra menzionati si propongono di seguito alcuni emendamenti puntuali:

- **Nelle premesse del decreto:**
 - **Inserire:** “Visto il decreto legislativo 23 giugno 2011, n.118, relativo alle disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42.”
- **Art. 7 comma 6:**
 - **Eliminare “essi” al termine del comma, controllare ripetizione “le autorità l’autorità”;**
- **Art. 7 comma 8:**
 - Sostituire “1.000.000” con “1.300.000”
- **Art.21 comma 10:**
 - Aggiungere: “10. Le sanzioni amministrative previste ai commi precedenti sono ridotte nei primi 12 mesi in una misura percentuale del ??%.”
- **Art.21 comma 11:**
 - Aggiungere: “11. Le entrate derivanti dalle sanzioni amministrative previste ai commi precedenti, sono destinate a iniziative a vantaggio del miglioramento della sicurezza dei sistemi informativi. Tali entrate affluiscono, nel rispetto dei vincoli di perimetrazione in materia di sanità, ad appositi capitoli/articoli di entrata del bilancio delle amministrazioni competenti territorialmente. Il Ministero dell’economia e delle finanze, per le sanzioni comminate dalle amministrazioni centrali dello Stato con proprio decreto ministeriale le può riassegnare a un fondo apposito iscritto nello stato di previsione del Ministero dello sviluppo economico per destinarle ad iniziative, individuate annualmente con decreto del Ministero dello sviluppo economico, finalizzate al miglioramento della sicurezza dei sistemi informativi dei servizi essenziali. Le Regioni e Province Autonome

per quanto di propria competenza assumono analoghi atti con le stesse finalità a favore dei soggetti erogatori di servizi essenziali sul proprio territorio.”

- **Art.22 comma 1:**
 - Sostituire gli importi “5.000.000” con “5.300.000” e “3.000.000” con “3.300.000”.
- **Art.22 comma 1-bis:**
 - Aggiungere dopo comma 1:”1-bis Le spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 7, 8 **e 12** del presente decreto e più in generale le spese ICT sostenute per l’adeguamento dei sistemi informativi al presente decreto sono coerenti con il piano triennale ICT della PA ai sensi dei commi 512-520 della legge 208/2015.”.

Nell’ambito della relazione tecnica in relazione all’articolo 7 sono da aggiungere, in riferimento all’allegata breve relazione tecnica, i seguenti periodi:

“f) con riferimento al coordinamento delle Regioni e Province Autonome in materia di sanità:

- Euro 70.000 per l’acquisto di beni e servizi, tra i quali strumentazione informatica utile per l’implementazione;
- Euro 50.000 per attività di ispezione/analisi in loco alle infrastrutture informatiche;
- Euro 30.000 per attività di formazione/aggiornamento del personale addetto al settore;
- L’onere complessivo è pari a 150.000 euro a decorrere dal 2018;

g) con riferimento al coordinamento delle Regioni e Province Autonome in materia di ambiente/acque:

- Euro 70.000 per l’acquisto di beni e servizi, tra i quali strumentazione informatica utile per l’implementazione;
- Euro 50.000 per attività di ispezione/analisi in loco alle infrastrutture informatiche;
- Euro 30.000 per attività di formazione/aggiornamento del personale addetto al settore;
- L’onere complessivo è pari a 150.000 euro a decorrere dal 2018.”

Allegato 1 - Relazione tecnica per i servizi di coordinamento dei NIS salute e ambiente

Premessa

Come previsto dall'articolo 7 comma 1 lettere d) ed e) dello schema di decreto legislativo recante attuazione della direttiva (UE) 2016/1148 del parlamento europeo e del consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'unione, le Regioni e Province Autonome collaborano con i Ministeri della Salute e dell'Ambiente alle attività in capo ai rispettivi NIS.

In particolare è prevista una attività nel corso del 2018 per l'individuazione dei soggetti erogatori di servizi essenziali e successivamente il coordinamento delle attività ispettive di verifica delle misure di sicurezza adottate.

Pertanto la presente stima delle attività e dei relativi costi potrà essere fatta puntualmente solo dopo la definizione puntuale dell'ambito e delle funzioni da svolgere da parte della struttura di coordinamento, tuttavia in prima approssimazione sulla base delle esperienze pregresse e sul fatto che il coordinamento dovrà esplicarsi su una rete territoriale che prevederà inevitabilmente alcuni centri di competenza sovra regionale è possibile ipotizzare un piano attività e relativi costi riportato di seguito.

Piano attività

Il coordinamento dovrà esplicare le attività di:

- Gestione delle attività amministrative, attraverso beni e servizi, di supporto al Ministero della salute ed alla rete dei centri territoriali dei servizi sanitari ed ambientali per le attività di individuazione dei servizi essenziali;
- supporto tecnico dei centri territoriali per le attività di verifica ed ispezione delle misure di sicurezza adottate;
- dovrà garantire misure minime di formazione, qualificazione ed aggiornamento delle risorse impegnate nelle attività di coordinamento;
- dovrà svolgere sul territorio attività di ispezione e verifica.

Alla luce delle attività indicate, ipotizzando la possibilità negli anni di diminuire le spese per beni e servizi ed aumentare le spese per le attività ispettive, si prevede che ciascuno dei due coordinamenti debba sostenere le seguenti spese annualmente a partire dal 2018:

- Euro 70.000 per l'acquisto di beni e servizi, tra i quali strumentazione e servizi informatici utili per l'implementazione;
- Euro 50.000 per attività di ispezione/analisi in loco alle infrastrutture informatiche;
- Euro 30.000 per attività di formazione/aggiornamento del personale addetto al settore;

L'onere complessivo è pari a 150.000 euro a decorrere dal 2018.

Roma, 19 aprile 2018