Parere, ai sensi dell'articolo 9, comma 1, del decreto legislativo 28 agosto 1997, n. 281, sullo schema di decreto legislativo recante il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972, e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2).

Rep. atti n. 91/CU dell'11 luglio 2024.

LA CONFERENZA UNIFICATA

Nella seduta dell'11 luglio 2024:

VISTO l'articolo 9, comma 1, del decreto legislativo 28 agosto 1997, n. 281;

VISTA la direttiva (UE) 2022/2555, del Parlamento Europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

VISTA la legge 21 febbraio 2024, n. 15, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2022-2023" e, in particolare, l'articolo 3, che detta i criteri ed i principi direttivi per l'esercizio della delega ai fini del recepimento della suddetta direttiva (UE) 2022/2555;

VISTA la nota prot. DAGL n. 5771, del 17 giugno 2024, acquisita al prot. DAR n. 10538, del 18 giugno 2024, con la quale il Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri ha trasmesso lo schema di decreto legislativo in esame, corredato delle prescritte relazioni e munito del "VISTO" del Dipartimento della Ragioneria generale dello Stato del Ministero dell'economia e delle finanze, ai fini dell'espressione del parere di questa Conferenza;

VISTA la nota prot. DAR n. 10625 del 19 giugno 2024, con la quale l'Ufficio per il coordinamento delle attività della Segreteria della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le province autonome di Trento e di Bolzano ha diramato il suddetto schema di decreto legislativo e i relativi allegati, con la contestuale convocazione di una riunione tecnica per il giorno 1° luglio 2024, posticipata, su richiesta delle Regioni, con nota prot. DAR. n. 10968 del 25 giugno 2024, al giorno 9 luglio 2024;

VISTA la nota dell'8 luglio 2024, acquisita al prot. DAR n. 11718 e diramata in pari data, con nota prot. DAR n. 11727, alle amministrazioni interessate, con la quale il Coordinamento tecnico della Commissione per l'innovazione tecnologica e la digitalizzazione della Conferenza delle Regioni e delle Province autonome ha inviato un documento recante le proposte emendative, le osservazioni e le raccomandazioni sul testo del provvedimento di cui trattasi;

CONSIDERATI gli esiti della riunione tecnica del 9 luglio 2024, nel corso della quale, a seguito di un'approfondita analisi del predetto documento regionale, il Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri si è riservato di inviare un documento recante le valutazioni di accoglibilità delle istanze regionali, mentre l'ANCI si è riservata di presentare un documento di osservazioni in sede di Conferenza Unificata e l'UPI non ha formulato rilievi sul testo del provvedimento;

VISTA la nota del 9 luglio 2024, acquisita al prot. DAR n. 11765, diramata in pari data, con nota prot. DAR 11769, alle amministrazioni interessate, con la quale il Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri ha trasmesso il documento recante le valutazioni in ordine all'accoglibilità delle richieste regionali;

CONSIDERATI gli esiti della seduta dell'11 luglio 2024 di questa Conferenza, nel corso della quale:

- le Regioni e le Province autonome di Trento e di Bolzano hanno espresso parere favorevole, con le raccomandazioni e le osservazioni di cui al documento consegnato in seduta che, allegato al presente atto (allegato 1), ne costituisce parte integrante;
- l'ANCI ha espresso parere favorevole, con le osservazioni di cui al documento allegato (allegato 2), parte integrante del presente atto, evidenziando la necessità di prevedere un piano di medio-lungo termine di investimenti, funzionale al miglioramento dei sistemi, delle procedure, della qualità e della qualifica del personale e di un piano finanziario, necessari a sostenere gli enti locali legati alla transizione verso livelli di sicurezza più elevati;
- l'UPI ha espresso parere favorevole;

CONSIDERATO che il Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri, nel prendere atto delle osservazioni formulate, ha dato assicurazioni sul prosieguo dell'attività;

ESPRIME PARERE FAVOREVOLE

nei termini di cui in premessa, ai sensi dell'articolo 9, comma 1, del decreto legislativo 28 agosto 1997, n. 281, sullo schema di decreto legislativo recante il recepimento della direttiva UE 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972, e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2).

Il Segretario
Cons. Paola D'Avena

Firmato digitalmente da
D'AVENA PAOLA
C=IT
O=PRESIDENZA CONSIGLIO DEI MINISTRI

Il Presidente
Ministro Roberto Calderoli

Firmato digitalmente da
CALDEROLI ROBERTO
C=IT
O=PRESIDENZA CONSIGLIO DEI MINISTRI

MC

11-7-2024

CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

24/88/CU10/C14

POSIZIONE SULLO SCHEMA DI DECRETO LEGISLATIVO RECANTE IL RECEPIMENTO DELLA DIRETTIVA UE 2022/2555, RELATIVA A MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA NELL'UNIONE, RECANTE MODIFICA DEL REGOLAMENTO (UE) N. 910/2014 E DELLA DIRETTIVA (UE) 2018/1972, E CHE ABROGA LA DIRETTIVA (UE) 2016/1148 (DIRETTIVA NIS 2)

Parere, ai sensi dell'articolo 9, comma 1, del decreto legislativo 28 agosto 1997, n. 281

Punto 10) Odg Conferenza Unificata

La Conferenza delle Regioni e delle Province autonome esprime parere favorevole con le seguenti raccomandazioni e osservazioni dalle quali sono state stralciate le proposte emendative ritenute accoglibili in sede tecnica:

1. si suggerisce, anche in coerenza col testo del decreto, di utilizzare nel titolo il termine "cybersicurezza" (non "cibersicurezza");
2. per assicurare un corretto svolgimento delle funzioni delle Regioni e delle Province Autonome al fine dell'efficace applicazione del presente Decreto sul territorio, appare opportuno raccomandare al Governo l'inserimento nel Decreto (ad esempio nell'Art. 9 - Strategia nazionale di cybersicurezza) di un piano di investimenti nel settore della resilienza informatica del Paese che annoveri le Regioni e le Province Autonome tra i beneficiari;
3. si sottolinea la necessità di definire in maniera univoca il termine "critico" utilizzato nel testo del Decreto di recepimento con significati potenzialmente differenti che possono compromettere la corretta interpretazione delle prescrizioni;
4. di aggiungere all'art. 3, dopo il comma 13, il seguente comma: ***13 bis). Per quanto riguarda l'ambito pubblico rientrano nell'ambito di applicazione del presente decreto i soggetti di cui all'art 1 della legge 90 del 28 giugno 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici".***

   Relazione illustrativa: Appare opportuno proporre che a tutti i soggetti a cui si applica il DL Cyber si applica anche il presente Decreto e coordinare in generale i testi dei due Atti;
5. all'Art. 3.14 (Ambito di applicazione) si ritiene utile prevedere lo status specifico delle Società Finanziarie Regionali in merito al loro comportamento, in quanto rientrano sia nell'Art. 3 c.6 sia nel Regolamento;
6. di aggiungere all'art 11, comma 5, all'elenco che definisce le modalità di collaborazione con le Regioni interessate: ***"a) numero 1, c) numeri 1, 2, 6, h).";***
   Relazione illustrativa: Appare opportuno che gli ambiti di collaborazione tra le Autorità di Settore e le Regioni siano estesi a ulteriori settori di competenza diretta/indiretta delle Regioni (ICT, infrastrutture digitali, servizi postali e corrieri, fornitori di servizi digitali, attività di interesse culturale) non presenti nel testo originale;

7. di inserire, all'art. 13, comma 2, dopo le parole *"...ai fini del presente decreto"* le seguenti ***"anche tramite il coinvolgimento degli CSIRT regionali laddove costituiti secondo le linee guida ACN"***;

   Relazione illustrativa: Considerando che un numero cospicuo di Regioni hanno costituito lo CSIRT Regionale con finanziamenti PNRR e che questi hanno una consuetudine di rapporti con le realtà del territorio, appare opportuno prevedere il loro coinvolgimento nella gestione delle crisi soprattutto in eventi che impattano un alto numero di soggetti potenzialmente oltrepassando le capacità di risposta di ACN;
8. in merito all'Art. 16.3 (Divulgazione coordinata delle vulnerabilità) si ritiene utile siano disciplinati i test di introduzione in un sistema informatico o telematico protetto da misure di sicurezza effettuati ai soli fini di verifica e segnalazione delle vulnerabilità, con l'obiettivo del miglioramento continuo della sicurezza dei sistemi e delle reti, e non causando nocumento ai sistemi stessi. Appare in particolare opportuno valutare tale aspetto in merito all'Art. 615 ter del Codice Penale (Accesso abusivo ad un sistema informatico e telematico) e indicare quale sono le condizioni alle quali la persona fisica o giuridica segnalante deve attenersi per svolgere la segnalazione;
9. di aggiungere, all'art. 25, dopo il comma 1, il seguente comma: "***1-bis. La notifica degli incidenti di cui al comma precedente vale anche, come notifica preliminare ai sensi dell'art. 33 comma 4 del Reg. UE 679/2016".***
   Relazione illustrativa: L'art. 25 (*Obblighi in materia di notifica di incidente*) individua nel dettaglio gli obblighi che devono essere eseguiti in materia di notifica di incidente. In particolare, sono previsti:
   - una pre-notifica, entro 24 ore da quando i soggetti sono venuti a conoscenza dell'incidente significativo;
   - una notifica entro 72 ore;
   - una eventuale relazione intermedia, su richiesta del CSIRT Italia;
   - una relazione finale, entro un mese dalla trasmissione della notifica.

   Inoltre, all'art. 26, viene introdotta la possibilità di procedere alla trasmissione, su base volontaria, al CSIRT Italia di informazioni relative a incidenti, minacce informatiche e quasi incidenti, per i quali non vige l'obbligo di notifica. Da un punto di vista pratico si potrebbe migliorare l'efficienza organizzativa consolidando le notifiche da effettuare al Garante (entro 72 dal momento in cui il Titolare ne viene a conoscenza come previsto dall'art. 33 GDPR) e al CSIRT in un unico punto centrale;
10. all'Art. 34, comma 7 (Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione) si ritiene utile sia chiarito come si determinano le caratteristiche di indipendenza ed aggiungere caratteristiche di competenza/qualità del servizio;
11. All'Art. 38 (Sanzioni amministrative) si ritiene di raccomandare che ai soggetti comunque ricompresi nella nozione di PA adottata (elenco ISTAT) si applicano le sanzioni ridotte (tra 25.000 e 125.000 se essenziali, un terzo se importanti) anche se ricadono in altri Settori, specificando la nozione di pubblica amministrazione adottata anche in coerenza con l'art. 3. C.6.

12. all'art. 44, il comma 3 è soppresso e sostituito con il seguente comma ***"3. il Governo si impegna di concerto con la Conferenza Stato Regioni, per le Pubbliche amministrazioni, a individuare le risorse necessarie all'applicazione della normativa in oggetto e le modalità di erogazione agli enti interessati."***
Relazione illustrativa: Si fa presente che l'attuazione di quanto previsto dal Decreto di recepimento della Direttiva NIS 2 non può aver luogo in una situazione di invarianza finanziaria. Si propone di aggiungere, con riferimento alle Pubbliche Amministrazioni, che il Governo si impegna di concerto con la Conferenza Stato Regioni, a individuare le risorse necessarie all'applicazione della normativa in oggetto e le modalità di erogazione agli enti interessati.

OSSERVAZIONI

La Conferenza delle Regioni e delle Province autonome sottolinea la necessità di approfondire la tematica relativamente agli aspetti qui di seguito evidenziati:

- i proventi delle sanzioni confluiscono tra le entrate dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 11, comma 2, lettera f), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109." Si potrebbe considerare, anche al fine di evitare conflitti di interesse tra l'Ente chiamato ad irrogare le sanzioni e il beneficiario delle stesse, che i proventi confluiscano in un fondo, eventualmente gestito da ACN stessa, le cui risorse annualmente siano messo a disposizione delle Amministrazioni, ad esempio attraverso dei bandi, ai fini dell'implementazione delle politiche di cybersicurezza;
- art. 11 comma 5 - Si osserva la difficoltà di rispetto della data indicata per la definizione delle modalità di collaborazione in Conferenza Unificata;
- art. 12 comma 2 si suggerisce di prevedere tre rappresentanti delle Regioni anziché due e di prevedere almeno un rappresentante dei Comuni, o, in subordine, prevedere al comma 4 la convocazione su richiesta di almeno due componenti delle Regioni, anziché tre;
- art. 24, commi 1, 2, 3 - Le misure da adottare sembrano fare riferimento al concetto di accountability [adeguatezza e proporzionalità], in analogia con quanto fatto per il GDPR; si chiede di precisare se il comma 1 va letto in tale senso, anche alla luce del successivo comma 2, che prevede comunque delle "misure minime" - tra l'altro, probabilmente eccessive se applicate in tutti gli ambiti e per tutte le tipologie di soggetti - che sembrerebbero contraddire proprio la logica dell'accountability; si evidenzia, inoltre, che potrebbe non essere agevole effettuare delle valutazioni di adeguatezza sulle forniture;
- art. 25, commi 4 e 5 - Sarebbe opportuno definire meglio il concetto di "perturbazione", e se la valutazione richiesta [gravità, considerevole] siano da ricondurre sempre al concetto di accountability;
- art. 32, commi 1 e 2 - Si propone di riscrivere la parte relativa agli specifici obblighi e alla loro eventuale non applicazione, in quanto non di immediata comprensione.

Roma, 11 luglio 2024

11-7-2024

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Conferenza Unificata

CONFERENZA UNIFICATA

11 luglio 2024

Punto 10) all'o.d.g.:

PARERE, AI SENSI DELL'ARTICOLO 71, COMMA 1 DEL D.LGS. 7 MARZO 2005, N. 82, SULLO SCHEMA DI DECRETO LEGISLATIVO DI "RECEPIMENTO DELLA DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO RELATIVA A MISURE PER UN LIVELLO COMUNE ELEVATO DI CYBERSICUREZZA NELL'UNIONE, RECANTE MODIFICA DEL REGOLAMENTO (UE) N. 910/2014 E DELLA DIRETTIVA (UE) 2018/1972 E CHE ABROGA LA DIRETTIVA (UE) 2016/1148 (DIRETTIVA NIS2)"

La sicurezza informatica è ormai un tema ineludibile per tutte le Pubbliche Amministrazioni, di qualunque dimensione e livello amministrativo: il progressivo intensificarsi di attacchi di diversa natura, che siano finalizzati alla messa fuori uso dei sistemi informativi o all'estrazione fraudolenta di dati, rende ineludibile un rafforzamento delle difese cibernetiche, da attuarsi a livello regolamentare e, conseguentemente, operativo a livello di singolo ente.

Il tema, di conseguenza, assume centralità anche per i Comuni, le loro forme associate e le Città metropolitane che, pur gestendo dati i quali, secondo la classificazione della Strategia Nazionale di Cybersicurezza 2022-2026, vengono identificati "ordinari" e non "critici" o "strategici", sempre più spesso sono oggetto di attacchi ai propri sistemi informativi che causano grandi problemi alla gestione dell'attività amministrativa e all'erogazione dei servizi, fino a causarne il blocco per periodi prolungati.

In questo scenario, si inserisce il Decreto in esame, di recepimento della Direttiva (UE) 2022/2555 del Parlamento europeo che mira ad una omogeneizzazione delle misure di sicurezza cibernetica a livello degli Stati membri, riprendendo il percorso già tracciato con la Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" recentemente emanata, che vuole indirizzare e sensibilizzare anche le Città Metropolitane, i Comuni con popolazione superiore a 100.000 abitanti, o comunque capoluogo di Regione, e loro in-house dedicate, in questo caso specifico in esame, alla gestione

di servizi e sistemi informatici dedicati a settori individuati come altamente critici ai sensi degli Allegati I e II del decreto in esame.

Va detto infatti che, allo stato attuale, pur in presenza di casi virtuosi di singole amministrazioni comunali capaci di difendersi e rispondere agli attacchi in maniera efficace, per gli enti locali permane una generalizzata difficoltà ad attrezzarsi adeguatamente. I motivi principali che ostacolano l'adozione di adeguate misure di sicurezza, riassunti di seguito, non trovano, tuttavia, riscontro positivo nel testo in esame, rimanendo irrisolti, a meno dell'adozione di misure di supporto successive o in fase di decretazione attuativa:

- la carenza di risorse umane dipendenti con competenze tecniche adeguate, unita alla difficoltà a reperirne sul mercato di così specialistiche, anche a causa della bassa appetibilità, in termini retributivi, delle posizioni di lavoro all'interno dei Comuni;
- la ristrettezza di risorse di bilancio da dedicare a interventi organizzativi e sui sistemi informativi;
- l'impossibilità, quindi, di rispettare i dettami normativi e attuare le disposizioni previste ad invarianza finanziaria e di risorse umane, sia per le figure professionali richieste, sia per gli inevitabili adeguamenti informatici o rinnovi di licenze a nuove condizioni, necessari a rafforzare la resilienza cibernetica.
-

TUTTO CIO' PREMESSO

L'ANCI

ESPRIME

PARERE FAVOREVOLE sullo schema di decreto legislativo di "Recepimento della direttiva (UE) 2022/2555 del Parlamento europeo relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2)"

CON LE SEGUENTI RACCOMANDAZIONI:

1. Il Governo si impegni ad individuare le risorse necessarie all'applicazione della normativa in oggetto e le modalità di erogazione ai soggetti interessati, con particolare riguardo alle Pubbliche Amministrazioni locali, approfittando della disponibilità dei fondi PNRR in questa fase, ma delineando fin da ora un piano di investimenti che consenta la sostenibilità degli interventi anche successivamente.
2. Venga estesa anche ai Comuni la partecipazione al Tavolo per l'attuazione della disciplina NIS, modificando in particolare l'art. 12 comma 2 inserendo

un rappresentante aggiuntivo espressione dei Comuni, designato dalla Conferenza Unificata di cui al Dlgs 28 agosto 1997, n. 281, anziché della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano.

3. Vengano coinvolti i Comuni, ricompresi nel perimetro di attuazione del presento decreto, nella fase di definizione degli atti attuativi e regolamentari, prevedendo un parere della Conferenza Unificata di cui al Dlgs 28 agosto 1997, n. 281, laddove sia già previsto un confronto con gli enti territoriali.
4. Sia garantito il coordinamento e l'armonizzazione con le normative settoriali o comunque impattate dall'attuazione del presente decreto, in ottica di coerenza e semplificazione, al fine di facilitare la comprensione delle attività da svolgersi e conseguenti sanzioni in caso di inadempienza, a carico dei soggetti individuati dalla norma in esame.