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