Anitec-Assinform

Memoria

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione

Audizione alla Camera dei deputati, commissioni riunite I – Affari Costituzionali e IX – Trasporti

A cura di
Anitec-Assinform – Associazione dell'industria italiana dell'Information and Communication Technology (ICT)

15 luglio 2024

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967


Anitec-Assinform

Anitec-Assinform

Sommario

INTRODUZIONE

Il decreto legislativo in esame recepisce nell'ordinamento italiano la direttiva NIS 2, aggiornando la disciplina NIS esistente.

La direttiva è stata approvata a livello europeo in un contesto di aumento esponenziale degli attacchi informatici, a seguito in particolare dell'accelerazione alla trasformazione digitale operata durante la pandemia e della guerra in Ucraina, che ha aumentato le minacce ibride agli operatori economici essenziali in Europa.

I dati CLUSIT mostrano come, dal 2018 al 2022, il numero annuale di cyberattacchi a livello mondiale sia aumentato del 60%. Crescono soprattutto gli attacchi gravi – che causano cospicue perdite economiche e di dati per le vittime. Nel primo semestre del 2023 in Italia si sono registrati 132 attacchi gravi, ben nove volte tanto lo stesso dato per il 2018 (15). Risulta particolarmente colpita la pubblica amministrazione, che subisce il 23% degli attacchi totali, seguita dal settore manufatturiero.

La direttiva in questione adotta un approccio di sistema, ponendosi come obiettivo la messa in sicurezza dei soggetti più importanti nella fornitura di prodotti e servizi, attraverso misure di gestione del rischio più stringenti, obblighi di segnalazione degli incidenti avvenuti, la definizione di quadri nazionali di gestione della sicurezza informatica e sanzioni più dure per i soggetti inadempienti.

A prescindere dalle considerazioni sul contenuto del decreto, l'ambizione della direttiva impone una riflessione a parte sulle risorse finanziarie e umane da impiegare nella fase di implementazione. Saranno necessari grossi investimenti da parte delle imprese, per i quali si potrebbero prevedere incentivi e facilitazioni. Allo stesso modo, sarà opportuno valutare come sviluppare le competenze necessarie ad implementare correttamente le misure di gestione del rischio informatico; ci sono ampi spazi di miglioramento sia nelle conoscenze cyber di base degli occupati in Italia, che nella formazione di personale specializzato.

Anitec-Assinform

Il decreto legislativo vuole recepire fedelmente le disposizioni della direttiva, mantenendo però un approccio più flessibile e basato sul rischio, con l'obiettivo dichiarato di non generare costi di compliance eccessivi per gli operatori e selezionare delle priorità chiare di intervento per l'Agenzia per la Cybersicurezza Nazionale (ACN), che sarà chiamata ad applicare le disposizioni del decreto. ACN avrà dunque ampi spazi di discrezionalità nel determinare criteri e modalità di implementazione della direttiva.

Questo approccio ha il merito di potersi adattare facilmente all'evoluzione delle tecnologie e delle minacce di cibersicurezza. Si pone, tuttavia, la necessità di garantire nel corso del tempo la certezza per gli operatori delle misure di adempimento a cui devono sottostare, oltre che dare loro supporto nell'applicazione delle previsioni.

Anitec-Assinform può essere un interlocutore importante per l'Autorità nell'applicazione della direttiva, favorendo la conoscenza del provvedimento sul tessuto industriale italiano, mettendo a disposizione le forti competenze in materia di cybersecurity dei propri associati per individuare certificazioni e specifiche tecniche che possono orientare le scelte dei soggetti interessati, e facilitando l'applicazione del decreto da parte delle imprese dei servizi digitali, le quali sono fondamentali per la sicurezza informatica in tutta Europa.

1. CAPO I – DISPOSIZIONI GENERALI

Il primo capo del decreto stabilisce in particolare il campo di applicazione del provvedimento, per poi classificare i soggetti interessati a seconda della priorità che la loro sicurezza informatica assume ai fini della direttiva.

Si noterà che, se da una parte il legislatore ha utilizzato a pieno il margine di allargamento del campo applicativo concesso dal testo della direttiva europea, dall'altra ha lasciato volutamente ampi spazi di discrezionalità alla legislazione secondaria, che sarà prerogativa soprattutto di ACN e della Presidenza del Consiglio dei ministri.

1.1. Ambito di applicazione

Lo schema di regolamento identifica all'articolo 3 un campo di applicazione ampliato rispetto a quanto delineato dalla direttiva. Sono infatti soggette alle disposizioni del decreto:

- Le medie e grandi imprese dei settori di cui negli allegati I e II;
- Le pubbliche amministrazioni elencate nell'allegato III, indipendentemente dalle dimensioni;
- Altre categorie di imprese e organizzazioni individuate nell'allegato IV, indipendentemente dalle dimensioni: i trasporti pubblici locali, gli istituti di istruzione che svolgono attività di ricerca, i soggetti che svolgono attività culturali, le società a controllo pubblico o partecipate.

La direttiva prevede infatti la possibilità per gli Stati membri di allargare il campo di applicazione a tutti i livelli delle pubbliche amministrazioni, enti collegati e istituti di istruzione.

Oltre a quanto esposto sopra, il dlgs introduce diverse norme aggiuntive di definizione del campo di applicazione. A questo proposito, si riscontra un ampio ricorso a normazione secondaria per la definizione della portata finale del decreto. Siccome la direttiva NIS 2 si pone come obiettivo la sicurezza informatica a livello sistemico per l'economia europea, i soggetti del provvedimento dovranno

intervenire non solo sui processi interni, ma anche sull'intera catena di approvvigionamento.

1.1.1. Soggetti critici ai sensi della direttiva CER

Secondo l'art. 3, co. 5, lettera a), i soggetti critici ai sensi del dlgs di recepimento della Direttiva sulla Resilienza dei Soggetti Critici (CER), sono soggetti alle disposizioni della direttiva NIS 2 indipendentemente dalla loro dimensione.

La CER stabilisce delle misure per assicurare che i soggetti critici possano fornire i loro servizi con continuità, prendendo misure contro possibili disastri naturali, emergenze sanitarie, e attacchi informatici. I soggetti critici secondo la CER dovranno essere identificati dai ministeri competenti tra le imprese di alcuni settori ritenuti fondamentali, sulla base dell'importanza dei soggetti per la continuità delle operazioni del settore e la fornitura di beni essenziali.

I settori sottoposti alla CER per la maggior parte coincidono con i settori indicati dagli allegati I e II del dlgs di recepimento della NIS 2. Perciò ad oggi pare improbabile che categorie di soggetti critici ai sensi della CER non siano già coperti dagli altri criteri di applicazione della NIS 2.

1.1.2. Criterio di proporzionalità su dimensione delle imprese

L'art. 3, comma 4 stabilisce che ai fini del dlgs si applica la definizione di media o grande impresa di cui alla raccomandazione 2003/361/CE. Un'impresa si definisce dunque media se occupa tra le 50 e le 250 persone e realizza un fatturato annuo tra i 10 e i 50 milioni di euro. Sotto e sopra queste soglie si definiscono, rispettivamente, le piccole e le grandi imprese.

Il legislatore ha però predisposto una clausola di salvaguardia alle definizioni sulla base di un criterio di proporzionalità: l'applicazione della raccomandazione UE deve tenere "conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce". In questo modo, il dlgs sembra indicare che sarà possibile una deroga per le imprese che, sebbene superino i massimali per le piccole imprese, non costituiscano un pericolo di sicurezza informatica del

proprio settore o catena del valore a causa della propria indipendenza da clienti e fornitori.

I criteri di applicazione della clausola di salvaguardia dovranno essere definiti da un decreto del Presidente del Consiglio dei ministri, su proposta dell'ACN e sentito il Tavolo per l'attuazione della disciplina NIS.

1.1.3. Servizi della società dell'informazione

L'art. 3 comma 5 dello Schema di Regolamento identifica inoltre, sulla base delle indicazioni della direttiva, delle categorie di imprese dei servizi della società dell'informazione particolarmente importanti per la sicurezza informatica a livello sistemico. A queste imprese si applica la direttiva NIS 2, indipendentemente dalle loro dimensioni:

- Reti pubbliche di comunicazione elettronica e servizi di comunicazione elettronica accessibili al pubblico;
- Servizi fiduciari;
- Registri TLD e servizi DNS;
- Servizi di registrazione dei nomi di dominio.

1.1.4. Operatori di servizi essenziali e imprese di sicurezza informatica collegate a imprese soggette alla direttiva

Infine, saranno incluse nel campo di applicazione della direttiva NIS 2 tutte le imprese, indipendentemente dalle dimensioni, che:

- sono definite essenziali ai sensi del dlgs 65/2018, che recepiva la prima direttiva NIS.
- sono fornitori di servizi essenziali, ovvero il loro funzionamento è fondamentale per ragioni economiche, sociali, di sicurezza o salute pubblica; questi soggetti saranno poi individuati dall'ACN, su proposta delle Autorità di settore definite dal decreto;
- sono fondamentali per la sicurezza informatica di un soggetto coperto dal decreto. Questi soggetti dovranno essere identificati da decreto del Presidente del Consiglio dei ministri.

1.2. Giurisdizione

L'articolo 5 stabilisce i criteri per stabilire se un'azienda non ricade sotto la giurisdizione italiana:

- se il soggetto è un fornitore di reti pubbliche di comunicazione o un fornitore di servizi di comunicazione elettronica accessibili al pubblico, sarà sotto la giurisdizione dello Stato membro in cui fornisce i servizi;
- se offre altri servizi digitali: di sistema dei nomi di dominio DNS, di registro dei nomi di dominio di primo livello, di registrazione dei nomi di dominio, di cloud computing, data center, reti di distribuzione dei contenuti, servizi gestiti, servizi di sicurezza gestiti, mercati online, motori di ricerca online o infine social network. In questo caso è sottoposto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale nell'Unione;
- se fa parte della pubblica amministrazione di un altro Stato membro.

Lo stabilimento principale nell'Unione è definito come lo stabilimento in cui sono adottate le misure di gestione del rischio di sicurezza informatica; se non fosse possibile determinarlo, è considerato quello in cui vengono effettuate le operazioni di sicurezza informatica; in ultima istanza, il decreto definisce lo stabilimento principale come quello con il maggior numero di dipendenti nell'Unione.

1.3. Definizione di soggetti essenziali e importanti

I soggetti nel campo di applicazione della direttiva si differenziano tra essenziali e importanti. Sono dunque considerati essenziali:

- Le grandi imprese attive nei settori di cui all'allegato I
- I soggetti critici come individuati dalla direttiva CER
- I fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico, se medie o grandi imprese
- I servizi fiduciari qualificati, i registri TLD, i servizi DNS

- Le pubbliche amministrazioni centrali.

Tutti gli altri soggetti inclusi nel campo di applicazione sono considerati invece importanti. La suddivisione operata dal dlgs ricalca i criteri indicati dalla direttiva, rinunciando ad ampliare l'elenco degli essenziali.

La differenziazione tra soggetti essenziali e importanti si applica importante soprattutto nella definizione delle misure di vigilanza e di sanzione sulla compliance alla direttiva. Ma potrà essere utilizzata dall'ACN anche per definire la proporzionalità degli obblighi di gestione del rischio e di segnalazione degli incidenti imposti ai soggetti interessati, come si vedrà in seguito.

La divisione tra essenziali e importanti sarà curata dall'ACN annualmente, sulla base delle seguenti tempistiche:

- 1° gennaio/28 febbraio: le imprese si registrano/aggiornano le proprie informazioni su una piattaforma creata appositamente da ACN, comunicando la propria ragione sociale, i settori in cui opera e i propri contatti;
- Entro il 31 marzo: ACN prepara l'elenco dei soggetti sottoposti alla NIS 2, suddividendoli tra essenziali e importanti; procede poi a comunicare il proprio status alle singole imprese;
- 15 aprile/31 maggio: i soggetti aggiornano in particolare le informazioni sulla piattaforma in merito ai propri nomi di dominio, l'elenco degli Stati membri in cui forniscono servizi interessati dal dlgs, gli individui responsabili dell'applicazione della direttiva.

I fornitori di servizi digitali sono tenuti inoltre a comunicare, ai fini di determinarne la giurisdizione, l'indirizzo della propria sede principale o del suo rappresentante in UE. L'ACN, nel momento della preparazione dell'elenco dei soggetti essenziali e importanti, identifica, sulla base di criteri stabiliti tramite DPCM, i soggetti che impatto sulla efficienza dello strumento militare e sulla tutela della difesa dello Stato, e la comunica al Ministero della difesa.

Osservazioni

L'ampio margine di discrezionalità previsto dal presente Capo permette flessibilità e capacità di adattamento dell'ambito di

applicazione alle dinamiche in continua evoluzione della sicurezza informatica.

Per assicurare la riuscita della nuova disciplina NIS, risulta ora fondamentale un'implementazione chiara e univoca, per evitare che le imprese debbano rivedere più volte i propri piani di cibersicurezza.

Sarà necessario un efficace coordinamento tra ACN, ministeri, Presidenza del Consiglio dei ministri e gli altri enti che interverranno sulle norme dell'art. 3 del dlgs, per garantire la certezza giuridica, ed evitare discrepanze tra le date di definizione dei criteri aggiuntivi per il campo di applicazione.

Se infatti, come giustamente riconosciuto dall'impostazione del decreto, la sicurezza informatica necessita di misure sistemiche e orizzontali, una implementazione eccessivamente imprevedibile e scaglionata nel tempo rischierebbe di ridurre la capacità dei settori chiave di attivare le misure di sicurezza lungo tutta la catena del valore.

L'ambito di discrezionalità che potenzialmente avrà l'impatto maggiore è la definizione dei criteri che stabiliscono le modalità di inclusione nel campo di applicazione dei fornitori di soggetti essenziali o importanti. Il ruolo di ACN in questo caso sarà fondamentale per monitorare e adattare le disposizioni a catene del valore in continua evoluzione.

Per quanto riguarda la procedura di definizione dei soggetti NIS2 essenziali e importanti, si prefigura dunque un aggiornamento annuale della posizione di compliance dei soggetti della direttiva. Il processo risulta gravoso e potrebbe creare incertezza giuridica soprattutto per i piccoli operatori o le startup, che sono maggiormente soggetti a cambiamenti della propria dimensione e del proprio settore di attività. Sarebbe opportuno prevedere una proporzionalità dovuta alla dimensione e al rischio per gli obblighi di aggiornamento della propria posizione di compliance.

Le previsioni di definizione della giurisdizione italiana, in linea con quanto stabilito dalla direttiva, necessiteranno di ampia cooperazione e coordinamento tra Stati membri. È importante evitare il rischio di una potenziale disuguaglianza di trattamento fra competitor che potrebbero trovarsi a sottostare a indicazioni più o meno rigide in base alla specifica giurisdizione dello Stato membro di riferimento in cui operano.

Si rileva infine che il decreto non fornisce informazioni circa la tempistica di pubblicazione della piattaforma per la registrazione predisposta da ACN. Siccome la direttiva prevede la comunicazione della lista di soggetti essenziali e importanti alla Commissione europea entro il 17 aprile 2025, e visto il potenziale trasformativo degli obblighi di cui al presente decreto sui soggetti interessati, si raccomanda una rapida pubblicazione della piattaforma di registrazione.

2. CAPO II: QUADRO NAZIONALE DI SICUREZZA INFORMATICA

Il Quadro nazionale di sicurezza informatica proposto dal decreto segue l'impostazione indicata dalla direttiva, istituendo la programmazione e i ruoli delle attività e processi che dovranno essere attuati per l'applicazione dei provvedimenti della NIS 2.

2.1. Strategia nazionale di cibersicurezza

Il decreto stabilisce i contenuti per la Strategia nazionale di cibersicurezza, che definisce gli obiettivi strategici e le risorse necessarie per conseguirli, oltre a adottare misure per garantire la cybersicurezza.

L'ACN ha già adottato una Strategia nazionale, valida per il periodo 2022-2026, sulla base dei principi contenuti nel testo della direttiva. Tra le misure previste dalla Strategia, si sottolineano in particolare la sicurezza informatica nella catena di approvvigionamento dei prodotti TIC per i soggetti NIS2, ma anche la promozione dello sviluppo e dell'integrazione di tecnologie avanzate rilevanti per la gestione dei rischi di sicurezza informatica.

2.2. Piano nazionale di risposta agli incidenti e alla crisi informatiche

Nell'ambito del Quadro nazionale di sicurezza informatica, è prevista l'adozione di un Piano nazionale di risposta agli incidenti e alla crisi informatiche su vasta scala.

Il Piano è istituito entro dodici mesi dall'entrata in vigore del decreto, con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Autorità nazionale di gestione delle crisi informatiche. quindi l'ACN, ad esclusione dei temi di sicurezza nazionale su cui interviene il Ministero della difesa.

Il DPCM stabilirà obiettivi e modalità di gestione degli incidenti e crisi informatiche, indicando in particolare i pertinenti portatori di interessi del settore pubblico e privato. I DPCM in questione non saranno pubblicati, a causa della sensibilità delle informazioni in essi contenuti.

2.3. Autorità di settore

Le autorità di settore identificate dal dlgs rispecchiano l'impostazione determinata in passato per altre misure, come il decreto-legge 82/2021. Rimane il ruolo dell'ACN come Autorità nazionale competente NIS e Single Point of Contact. Il Ministero della difesa è invece Autorità nazionale competente NIS solo per la parte relativa alla difesa dello Stato. Allo stesso modo, ACN e Ministero della difesa sono nominate Autorità nazionali di gestione delle crisi informatiche, con la stessa suddivisione delle competenze.

Le Autorità di settore saranno:

Autorità	Settore	Riferimento
Presidenza del Consiglio dei ministri	Gestione dei servizi TIC	Allegato I, numero 9
	Spazio	Allegato I, numero 10
	Pubbliche amministrazioni come identificate ai sensi dall'art. 1, co. 3 della legge 196/2009 o da ulteriori DPCM ex art. 40 del dlgs	Art. 3, co. 6 e 7
	Società in-house, partecipate o a controllo pubblico	Allegato IV, numero 4
Ministero dell'economia e delle finanze	Bancario	Allegato I, numero 3
	Infrastrutture dei mercati finanziari	Allegato I, numero 4
	Infrastrutture digitali	Allegato I, numero 8
	Servizi postali e corriere	Allegato II, numero 1

Ministero delle Imprese e del Made in Italy	Fabbricazione, produzione e distribuzione di sostanze chimiche	Allegato II, numero III
	Fabbricazione di computer e prodotti di elettronica e ottica	Allegato II, numero 5, lettera b)
	Fabbricazione di apparecchiature elettriche	Allegato II, numero 5, lettera c)
	Fabbricazione di macchinari a apparecchiature n.c.a.	Allegato II, numero 5, lettera d)
	Fabbricazione di autoveicoli, rimorchi e semirimorchi	Allegato II, numero 5, lettera e)
	Fabbricazione di altri mezzi di trasporto	Allegato II, numero 5, lettera f)
	Fornitori di servizi digitali	Allegato II, numero 6
Ministero dell'agricoltura, della sovranità alimentare e delle foreste	Produzione, trasformazione e distribuzione di alimenti	Allegato II, numero 4
Ministero dell'ambiente e della sicurezza energetica	Energia	Allegato I, numero 1
	Fornitura e distribuzione di acqua potabile	Allegato I, numero 6
	Acque reflue	Allegato I, numero 7
	Gestione rifiuti	Allegato II, numero 2
Ministero delle infrastrutture e dei trasporti	Trasporti	Allegato I, numero 2
	Servizi di trasporto pubblico locale	Allegato IV, numero 1
	Ricerca	Allegato II, numero 7

Ministero dell'università e della ricerca	Istituti di istruzione che svolgono attività di ricerca	Allegato IV, numero 2
Ministero della cultura	Attività di interesse culturale	Allegato IV, numero 3
Ministero della salute	Settore sanitario	Allegato I, numero 5
	Fabbricazione di dispositivi medici e dispositivi medico-diagnostici in vitro	Allegato II, numero 5, lettera a)

Le Autorità di settore NIS istituiscono inoltre dei tavoli settoriali, il cui scopo è assicurare l'implementazione corretta e proporzionata degli obblighi del presente decreto, nonché delle attività di vigilanza ed esecuzione.

2.4. Tavolo di lavoro per l'attuazione della disciplina NIS

L'art. 12 del dlgs costituisce in via permanente il Tavolo per l'attuazione della disciplina NIS, che sarà presieduto dal direttore generale dell'ACN e composto dai rappresentanti di ogni autorità di settore, più due rappresentanti designati dalla Conferenza Stato-Regioni. È prevista altresì la possibilità per il Tavolo di chiamare a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati dalle previsioni della direttiva.

Il Tavolo:

- supporta l'ACN nello svolgimento delle funzioni relative all'implementazione del presente decreto;
- formula proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo ai fini dell'efficace attuazione;
- predispone una relazione annuale sull'attuazione del decreto.

2.5. CyberSecurity Incident Response Team (CSIRT)

Il CSIRT, già istituito dalla legge 109/2021, è l'organo interno all'ACN preposto alla gestione degli incidenti di sicurezza informatica per i soggetti NIS 2. In quanto tale, si occupa di:

- monitorare le minacce informatiche a livello nazionale, e su richiesta fornisce assistenza specifica in monitoraggio ai soggetti della direttiva, proporzionatamente al proprio carico di lavoro;
- divulgare informazioni ai soggetti essenziali e importanti sulla base dei risultati del monitoraggio;
- effettuare scansioni dei loro sistemi informativi, rilevandone le vulnerabilità, sia su richiesta dei soggetti che proattivamente in autonomia;
- fornire una risposta agli incidenti dei soggetti essenziali e importanti, ove possibile;
- partecipare alla rete europea degli CSIRT nazionali.

Per definire le priorità di adempimento dei compiti elencati, il CSIRT adotta un approccio basato sul rischio. È inoltre tenuto a instaurare rapporti con i pertinenti stakeholder privati per conseguire i propri obiettivi: non viene specificato meglio questo punto, ma si suppone che si tratti sia dei privati soggetti alla direttiva, che in generale le imprese fornitrici di soluzioni e servizi di cybersecurity.

Il CSIRT ha poi un'altra funzione fondamentale: è coordinatore della divulgazione coordinata delle vulnerabilità, agendo da intermediario di fiducia tra la persona fisica o giuridica che segnala la vulnerabilità e il fornitore del prodotto potenzialmente vulnerabile. La divulgazione delle vulnerabilità è identificata dalla direttiva come fondamentale per assicurare un alto livello di cybersicurezza. Il CSIRT individua i soggetti interessati, assiste le entità che segnalano una vulnerabilità, e gestisce i tempi e le modalità di divulgazione della stessa. A questo fine, adotta una politica nazionale di divulgazione coordinata delle vulnerabilità.

2.6. Coordinamento con il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Si inseriscono qui le previsioni dell'art. 33 in materia di coordinamento con la disciplina del PSNC. Si tratta, in questo caso, di assicurare chiarezza nella definizione dell'ambito di applicazione tra NIS 2, dedicata alle misure di sicurezza informatica delle aziende nei settori economici principali, e il Perimetro, pensato per la protezione degli asset strategici da cui dipende un servizio essenziale.

Il decreto prevede in particolare che gli obblighi stabiliti dalla legge 133/2019, che istituisce il PSNC, siano considerati almeno equivalenti a quelli legati al recepimento della direttiva NIS 2, e che i sistemi informativi già coperti dal Perimetro non siano interessati dalle disposizioni di recepimento.

Osservazioni

Il Quadro presentato dal decreto istituisce un valido sistema di preparazione, monitoraggio e risposta agli incidenti di sicurezza informatica.

Tuttavia, sarebbe importante riconoscere un ruolo attivo più importante ai portatori di interesse esterni alle Autorità di settore, soprattutto nell'ambito del Tavolo di lavoro per l'attuazione della disciplina NIS2. Il settore ICT, rappresentato da Anitec-Assinform, ha una doppia funzione fondamentale alla buona riuscita della direttiva: da una parte è fornitore dei prodotti di sicurezza, dall'altra è sotto intenso scrutinio da parte del decreto in quanto settore naturalmente esposto ad attacchi informatici.

Perciò, oltre che una partecipazione significativa nei tavoli settoriali, si potrebbe prevedere il ruolo di osservatore permanente per i settori più interessati dal decreto. Tale disposizione sarebbe congruente con la proposta della direttiva che il Gruppo di cooperazione NIS organizzi incontri congiunti e regolari con gli stakeholder privati per discutere le attività e i problemi incontrati dal settore privato nell'adozione e implementazione del provvedimento.

A questo proposito, la conoscenza delle associazioni di categoria potrebbe essere un importante strumento per le Autorità di settore che cominceranno a sviluppare competenze in materia di sicurezza informatica.

Tra le esperienze positive di applicazione delle norme di cybersicurezza, si segnala in particolare il PSNC, con il quale sarà importante evitare duplicazioni degli obblighi e sovrapposizioni dell'ambito di applicazione. Particolarmente positivo è il quadro di compliance del Perimetro, che risulta sufficientemente chiaro senza per questo essere eccessivamente prescrittivo.

Infine, per quanto riguarda la divulgazione coordinata delle vulnerabilità, sarebbe opportuno che il CSIRT potesse selezionare le segnalazioni con un approccio basato sul rischio, per evitare un numero eccessivo di richieste da evadere e dunque ridotte capacità di intervento negli ambiti prioritari.

3. Capo III – Cooperazione con Autorità degli Stati membri e l'UE

La direttiva NIS 2 risponde ad un crescente numero di attacchi informatici a imprese nell'Unione. L'aggiornamento della vecchia disciplina NIS prevede anche un rafforzamento delle capacità di coordinamento europeo delle disposizioni nazionali.

Il Gruppo di cooperazione NIS è pensato per assicurare un coordinamento regolare dell'applicazione della direttiva in tutta l'UE. Vi dovrebbero partecipare sia ACN che le Autorità di settore. Tra i compiti del Gruppo si sottolineano non solo quelli di assistenza reciproca e collaborazione in caso di vulnerabilità e incidenti transfrontalieri, ma anche l'uniformazione delle misure applicate nei diversi Stati membri e l'applicazione corretta delle disposizioni stabilite dalla Commissione per i settori sui quali ha competenza, come visto nel caso dell'atto di esecuzione sui servizi internet.

La rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) è l'organo di risposta europea alle crisi alla sicurezza informatica. Ne farà parte ACN in quanto Autorità nazionale di gestione delle crisi informatiche. Tra i compiti di ACN in questo ambito si segnala in particolare l'aumento del livello di preparazione generale per le risposte a crisi informatiche su vasta scala.

Osservazioni

La cooperazione tra ACN, altre Autorità nazionali degli Stati membri, ENISA e Commissione europea è cruciale per la corretta implementazione della direttiva.

Si auspica che il Gruppo di cooperazione NIS sappia guidare con forza l'applicazione dei provvedimenti, soprattutto per evitare che le disposizioni della Commissione sui settori di sua competenza – soprattutto i servizi delle società dell'informazione – risultino eterogenee e di difficile comprensione per gli operatori. ACN in questo senso si è dimostrata proattiva non solo nella collaborazione con il Gruppo, ma anche con i portatori di interesse rilevanti nel settore privato.

Infine, l'evoluzione delle politiche europee in materia di cybersecurity impone attenzione particolare per evitare duplicazioni applicative delle misure NIS2 con ulteriori provvedimenti. Si pensi ad esempio al *Digital Operational Resilience Act* (DORA), che prevede delle norme

specifiche per il settore bancario e dei pagamenti. Analogamente pare che siano in lavorazione Regolamenti simili da parte delle istituzioni dell'Unione, riguardanti norme settoriali di sicurezza informatica. E' auspicabile che ACN mantenga un dialogo costante con la Commissione europea per evitare che le determinazioni proprie e delle Autorità di settore risultino diverse da provvedimenti settoriali che potrebbero essere approvati a breve a livello europeo.

4. CAPO IV – OBBLIGHI IN MATERIA DI GESTIONE DEL RISCHIO E DI NOTIFICA DI INCIDENTE

Si tratta del Capo centrale del decreto, che identifica gli obblighi riguardanti le misure di gestione del rischio di sicurezza informatica, sia le notifiche di incidente.

Anche in questo caso il legislatore ha previsto spazi di discrezionalità per ACN, al fine di ridurre gli oneri sia per le imprese soggette alla direttiva che per l'Autorità.

4.1. Misure di gestione del rischio

I soggetti NIS sono tenuti a adottare misure di:

- analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- gestione degli incidenti, comprese le procedure per notificarli secondo le disposizioni di questo decreto;
- continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, e gestione delle crisi;
- sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, incluse la gestione e la divulgazione delle vulnerabilità;
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica; pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni;

L'applicazione di queste misure deve assicurare un livello di sicurezza informatica d'impresa adeguata ai rischi esistenti, e tenuto conto delle conoscenze e tecnologie più aggiornate. Le misure devono essere inoltre proporzionate al grado di esposizione ai rischi del soggetto, alle

sue dimensioni e al potenziale impatto di incidenti sul contesto sociale ed economico.

4.2. Obbligo di segnalazione degli incidenti

I soggetti NIS segnalano al CSIRT ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi, senza ingiustificato ritardo.

Un incidente deve essere considerato significativo se:

- Può causare una grave perturbazione dei servizi o perdite finanziarie per il soggetto interessato;
- Può avere ripercussioni su altre persone fisiche o giuridiche, causando perdite materiali o immateriali considerevoli.

L'obbligo di notifica dell'incidente si declina nelle seguenti tempistiche:

- entro 24 ore da quando il soggetto è venuto a conoscenza dell'incidente, una pre-notifica che indichi se l'incidente possa essere stato causato da atti illegittimi o malevoli, e se possa avere un impatto transfrontaliero.
- entro 72 ore, una notifica che aggiorni la pre-notifica e dia una valutazione iniziale sulla gravità e l'impatto dell'incidente, e se possibile indicando gli indicatori di compromissione.
- in seguito, il CSIRT può richiedere una relazione intermedia sulla situazione;
- infine, entro un mese dalla notifica che fornisce una valutazione iniziale, una relazione finale al CSIRT che includa una descrizione dettagliata dell'incidente, la minaccia e la root cause che ha probabilmente innescato l'incidente, le misure di attenuazione adottate e in corso, e se noto, l'impatto transfrontaliero.

Qualora dopo un mese dalla notifica l'incidente sia ancora in corso, è richiesta una relazione mensile sui progressi fatti, e una relazione finale un mese dopo la conclusione dell'incidente.

La notifica non espone il soggetto che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

Il CSIRT, entro 24 ore dalla pre-notifica, fornisce una risposta al soggetto notificante, dando un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta, inoltre, il CSIRT fornisce ulteriore supporto tecnico.

Se possibile e ritenuto opportuno, i soggetti colpiti dall'incidente sono tenuti, previa consultazione con il CSIRT, a notificare ai destinatari dei propri servizi delle potenziali ripercussioni sulla fornitura di tali servizi. Se i destinatari possono essere colpiti a loro volta, i soggetti possono essere tenuti a comunicare possibili misure di contenimento o correttive della minaccia. In caso di necessità, l'ACN può decidere di informare il pubblico riguardo all'incidente, qualora la divulgazione sia nell'interesse pubblico.

4.3. Responsabilità degli organi di amministrazione e direttivi dei soggetti NIS

Gli organi di amministrazione e direttivi dei soggetti NIS avranno la responsabilità di adottare le modalità di implementazione delle misure di gestione del rischio e sovraintendere alla loro esecuzione. Saranno dunque responsabili personalmente delle violazioni del decreto.

Ne consegue che tali organi saranno tenuti a seguire corsi di formazione in sicurezza informatica, e promuovere una offerta periodica di formazione in materia ai propri dipendenti. Gli organi di amministrazione e direttivi saranno inoltre informati periodicamente, o se opportuno tempestivamente, degli incidenti e delle notifiche riguardanti il soggetto NIS che dirigono.

4.4. Modalità di elencazione e categorizzazione dei servizi e proporzionalità

L'ACN stabilisce, tramite determinazione, una categorizzazione di rilevanza delle attività e dei servizi, ai fini della definizione delle misure di gestione del rischio necessarie per categoria.

A partire dalla notifica di inserimento nell'elenco dei soggetti NIS2 essenziali o importanti (art. 7, co. 3, come visto nella sezione 1.3 "1.3. Definizione di soggetti essenziali e importanti"), dal 1° maggio al 30 giugno di ogni anno i soggetti comunicano sulla stessa piattaforma un elenco delle proprie attività e servizi, in modo da poterli assegnare ad una categoria di rilevanza. Entro novanta giorni dalla comunicazione, l'ACN verifica che le informazioni inserite siano corrette.

L'ACN dovrà inoltre determinare i criteri di proporzionalità degli obblighi in materia di gestione del rischio, sulla base del grado di esposizione del soggetto, la sua dimensione e l'impatto potenziale di un incidente sul contesto sociale ed economico. Gli obblighi sono dunque proporzionati sulla base della categoria di rilevanza precedentemente identificata, sul settore di appartenenza – tenendo conto della maturità tecnologica di partenza del soggetto, e sulla definizione di soggetto essenziale o importante.

Per attuare queste disposizioni l'ACN può emanare linee guida vincolanti per l'applicazione degli obblighi di gestione del rischio e di notifica degli incidenti, raccomandazioni per fornire supporto ai soggetti nell'implementazione degli obblighi, e determinare le fattispecie che determinano la sospensione dei termini di gradualità di implementazione degli obblighi.

4.5. Servizi di registrazione dei nomi di dominio

I servizi di registrazione dei nomi di dominio, seppur interessati dalla direttiva indipendentemente dalle proprie dimensioni, non sono soggetti agli obblighi di gestione del rischio e di notifica degli incidenti, ma garantiscono misure coerenti con le disposizioni in materia.

Il dlgs prevede invece delle misure specifiche per questa categoria di imprese, così come per i gestori di registri dei nomi di dominio di primo livello. Questi operatori sono tenuti a mantenere una banca dati di registrazione dei nomi di dominio, che contenga le informazioni necessarie a identificare e contattare i titolari dei nomi di dominio, e devono rendere disponibili i dati ivi contenuti sotto richiesta motivata dei soggetti legittimati.

4.6. Certificazioni e specifiche tecniche

Per garantire l'adozione di misure di gestione del rischio in linea con le previsioni del decreto, l'ACN può imporre ai soggetti NIS di utilizzare categorie di prodotti, processi e servizi TIC, sviluppati internamento dal soggetto o acquistati da terzi, che siano certificato nell'ambito dei sistemi europei di certificazione della cybersicurezza. In mancanza di tali sistemi, l'ACN può imporre le categorie di prodotti, processi e servizi di cui sopra, che siano riconosciuti da schemi di certificazione a livello europeo.

Inoltre, senza per questo favorire o discriminare un particolare tipo di tecnologia, l'Autorità può promuovere l'adozione di specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informativi e di rete. A questo fine, l'ACN si basa sulle linee guida pubblicate da ENISA, e redige un elenco delle categorie di tecnologie più idonee ad assicurare la corretta applicazione da parte dei soggetti NIS delle misure di gestione del rischio. L'elenco non è esaustivo né vincolante.

Osservazioni

Le disposizioni del presente Capo introducono obblighi precisi per le imprese soggette al decreto, che richiederanno significative risorse organizzative, umane e finanziarie per essere soddisfatti. La sicurezza informatica, tuttavia, è un obiettivo fondamentale per la tenuta del tessuto economico italiano.

Per questo motivo, sarà importante che l'Autorità sappia fornire sostegno adeguato ai soggetti nella definizione delle proprie mancanze e nella risposta agli incidenti, soprattutto nei casi in cui sia l'entità interessata dall'incidente a farne richiesta.

In quest'ottica, la determinazione di ACN di certificazioni e specifiche tecniche adatte all'adempimento degli obblighi previsti dal decreto può essere una misura semplice da adottare ma di grande impatto. Le imprese associate di Anitec-Assinform mettono a disposizione le proprie competenze per facilitare l'Autorità in questo compito.

Tuttavia, sembra opportuno specificare che ad oggi, purtroppo, le procedure per certificare prodotti secondo i sistemi di certificazione di cui all'articolo 49 del regolamento (UE) 2019/881 richiedono tempi

lunghi e costi gravosi alle aziende produttrici. Per evitare che l'Autorità non abbia a disposizione un'ampia selezione di prodotti, servizi e processi TIC da imporre ai soggetti NIS2, sarebbe utile prevedere un lasso di tempo adeguato prima di arrivare alla determinazione degli stessi, per consentire alle imprese di ottenere le certificazioni necessarie.

Analogamente, il decreto potrebbe creare attriti con quanto disposto dal ddl cybersicurezza, generando una duplicazione di obblighi sostanzialmente sovrapponibili. Appare evidente, infatti, come i soggetti di cui al periodo precedente si trovino costretti ad una doppia notifica al medesimo soggetto.

Si rileva infine come la previsione di misure di gestione del rischio legate ai propri fornitori sia, come già evidenziato nel capitolo dedicato al campo di applicazione, un potente strumento di allargamento degli obblighi del presente decreto e dei costi di compliance dei soggetti. Sarà opportuno valutare il tempo messo a disposizione dei soggetti ai fini della compliance a detto obbligo: gli operatori dimensionalmente più importanti potrebbero riscontrare serie difficoltà nel censimento dei loro fornitori.

5. CAPO V - POTERI DI VIGILANZA E ESECUZIONE

Rispetto al testo della direttiva europea, il decreto di recepimento prevede una disciplina maggiormente improntata alla flessibilità e alla proporzionalità.

Anche in questo caso, dunque, ACN dovrà intervenire con atti secondari per definire meglio come intende applicare le disposizioni del presente Capo.

5.1. Monitoraggio

L'ACN, ai fini di monitorare l'applicazione delle disposizioni del decreto, può richiedere ai soggetti:

- una rendicontazione dello stato di attuazione delle previsioni del dlgs e le informazioni necessarie a svolgere le proprie prerogative;
- di effettuare degli audit di sicurezza svolti da organismi indipendenti;
- di eseguire scansioni di sicurezza;
- di emanare raccomandazioni e avvertimenti relativi a presunte violazioni degli obblighi nel presente decreto.

L'attività di monitoraggio si accompagna ad interventi di supporto dei soggetti, qualora ciò non costituisca un onere sproporzionato ed eccessivo.

5.2. Verifiche e ispezioni

Sono previste poi attività di verifica dell'applicazione degli obblighi, in particolare con:

- verifiche della documentazione e delle informazioni trasmesse dai soggetti;
- ispezioni in loco e a distanza, inclusi controlli casuali;
- richiesta di accesso a dati e documenti necessari allo svolgimento delle verifiche.

Per i soggetti importanti, le attività di verifica e ispezione si applicano solo nel caso in cui l'ACN acquisisca elementi di prova a riguardo di violazioni delle disposizioni del presente decreto.

5.3. Misure di esecuzione

L'ACN potrà richiedere ai soggetti di fornire i dati che dimostrino l'attuazione di politiche di sicurezza informatica, come ad esempio i risultati di audit effettuati in materia, per verificare il rispetto degli obblighi del presente decreto.

Il decreto elenca poi le misure di esecuzione che saranno disponibili all'Autorità, la quale potrà obbligare i soggetti a:

- eseguire audit sulla sicurezza, in particolare a seguito di un incidente significativo o di una violazione del decreto. Questo obbligo si applicherà solo ai soggetti essenziali;
- effettuare scansioni di sicurezza;
- porre termine ad un comportamento che violi il decreto e porre rimedio a carenze individuate nell'applicazione delle disposizioni del decreto;
- comunicare ai destinatari dei propri servizi gli incidenti che possono avere una ripercussione sulla fornitura dei servizi, così come le misure che essi possono adottare per rispondere all'incidente subito dal soggetto, qualora ne siano potenzialmente interessati;
- se necessario, informare il pubblico dell'incidente occorso. Quest'obbligo, come riportato sopra nella sezione riguardante le notifiche di incidenti, può essere imposto se l'ACN ritiene che la divulgazione sia di interesse pubblico. L'Autorità potrà anche imporre di rendere pubbliche le violazioni del presente decreto.

Il dlgs stabilisce inoltre i passi che l'ACN può intraprendere per imporre gli obblighi ai soggetti interessati dalla direttiva. Si prevede prima di tutto la possibilità per l'Autorità di trasmettere istruzioni vincolanti per evitare il verificarsi di un incidente o per porvi rimedio.

ACN avrà la facoltà, inoltre, di designare un funzionario con lo scopo di supportare il soggetto interessato a rispettare gli obblighi del decreto. Il

rapporto tra funzionario e soggetto sarà circostanziato nel tempo e nell'ambito dei compiti assegnati.

Se il soggetto non dovesse adempiere alle misure di esecuzione elencate finora, alle istruzioni vincolanti o alle indicazioni del funzionario designato, l'Autorità sarà autorizzata a diffidarlo all'adempimento.

L'ACN, nell'applicazione delle previsioni riguardanti le misure di esecuzione, dovrà indicare al soggetto tempi e modalità proporzionate di adempimento. Le misure di esecuzione e la diffida saranno precedute da una notifica ai soggetti interessati delle conclusioni preliminari dell'Autorità, lasciando loro almeno quindici giorni per presentare informazioni in merito.

5.4. Sanzioni

Nel caso in cui un soggetto essenziale non dovesse adempiere, nei tempi e modalità indicati, alla diffida dell'Autorità, l'ACN potrà richiedere agli organi competenti di sospendere temporaneamente un certificato o un'autorizzazione relativi alle attività del soggetto inadempiente. Non sarà possibile comminare questa sanzione alle pubbliche amministrazioni, né alle imprese sottoposte a controllo pubblico.

Inoltre, agli organi di amministrazione e direttivi dei soggetti che non adempiano alla diffida sarà possibile dichiarare l'incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Anche in questo caso alla pubblica amministrazione si applica una disciplina diversa: i direttivi della PA saranno infatti sottoposti alle norme in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

Le sanzioni di cui sopra saranno applicabili fino all'adempimento degli obblighi da parte del soggetto.

Il decreto prevede infine sanzioni pecuniarie, seguendo l'impostazione della direttiva:

Violazione	Soggetto	Sanzione

- Mancata osservazione degli obblighi di gestione del rischio e di notifica degli incidenti; - inottemperanza alle misure di esecuzione e alle istruzioni vincolanti dell'Autorità.	Essenziale	Fino a €10 milioni o 2% del fatturato annuo mondiale (se superiore).
	Importante	Fino a €7 milioni o l'1,4% del fatturato annuo mondiale (se superiore)
	Essenziale - PA e imprese sottoposte a controllo pubblico	Da €25.000 a €125.000
	Importante - PA e imprese sottoposte a controllo pubblico	Un terzo delle sanzioni per le PA e le imprese controllate essenziali
- Mancata comunicazione delle informazioni sulla propria attività ad ACN; - mancata applicazione degli obblighi su schemi di certificazione o sulle banche dati di registrazione dei nomi di dominio; - mancata collaborazione con l'Autorità per le misure di vigilanza ed esecuzione, o con il CSIRT	Essenziale	Fino allo 0,1% del fatturato annuo mondiale
	Importante	Fino allo 0,07% del fatturato annuo mondiale
	Essenziale - PA e imprese sottoposte a controllo pubblico	Da €10.000 a €50.000. Solo nel caso di reiterazione specifica nell'arco di cinque anni.
	Importante - PA e imprese sottoposte a controllo pubblico	Un terzo delle sanzioni per le PA e le imprese controllate essenziali Solo nel caso di reiterazione specifica nell'arco di cinque anni.

La sanzione potrà essere raddoppiata in caso di reiterazione della violazione.

Sono previste poi misure deflattive del contenzioso, in particolare l'invio da parte di ACN di un invito a conformarsi al soggetto inadempiente, indicando un termine perentorio di adeguamento; e la possibilità di estinguere il procedimento con un pagamento di parte della sanzione.

Queste misure deflattive dovranno essere definite da un Decreto del Presidente del Consiglio dei ministri.

5.5. Criteri di proporzionalità delle misure di vigilanza e esecuzione

Il decreto prevede che l'Autorità adotti un approccio basato sul rischio per definire le proprie priorità di utilizzo dei poteri di vigilanza e esecuzione. ACN dovrà inoltre tenere conto della gravità della violazione, la sua durata, eventuali ripetizioni, i danni causati, e l'eventuale condotta intenzionale o negligente del soggetto. Saranno tenute anche in considerazione le misure adottate dal soggetto per attenuare i danni causati, così come tutte le certificazioni conseguite e il livello di collaborazione dimostrato.

I criteri e le modalità di applicazione dei poteri di vigilanza ed esecuzione di ACN saranno definiti con un DPCM.

Osservazioni

I poteri di vigilanza ed esecuzione sono le disposizioni che più necessitano di flessibilità e capacità di adattamento. Si ritiene dunque che l'approccio del legislatore, rispetto a quanto previsto dalla direttiva, sia positivo.

Sarebbe opportuno considerare, nella determinazione dell'approccio basato sul rischio, di non limitare eccessivamente le misure di vigilanza e supporto ex ante: in questo modo si correrebbe il rischio di non supportare e supervisionare efficacemente tutti i soggetti, soprattutto le imprese di dimensioni più piccole che potrebbero avere meno risorse per conoscere e adeguarsi alle previsioni del decreto. La conseguenza di questa situazione potrebbe essere un ricorso più ampio a misure di esecuzione per i soggetti importanti, che non hanno avuto lo stesso livello di supervisione ex ante dei soggetti essenziali.

Si segnala infine che, per evitare di oberare l'autorità nel sostegno alle imprese, si potrebbe prevedere la possibilità per operatori privati qualificati e riconosciuti di supplire ai funzionari designati di cui all'art. 37, comma 5.

6. CAPO VI – DISPOSIZIONI FINALI E TRANSITORIE

Le disposizioni finali e transitorie del decreto sono state inserite, ai fini di questa nota, nei paragrafi pertinenti a cui si riferivano. Si riportano in questo capitolo le previsioni relative all'entrata in vigore della disciplina NIS.

6.1. Fase di prima applicazione ed entrata in vigore

La direttiva NIS 2 indica che gli Stati membri hanno fino al 17 ottobre per recepire il provvedimento nei propri ordinamenti.

In seguito, si aprirà la fase di prima applicazione, di transizione per concedere alle imprese il tempo di adeguarsi agli obblighi previsti.

In particolare, in questa fase:

- Servizi della società di informazione ("*i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network*") che rientrano nell'ambito di applicazione del decreto dovranno registrarsi alla piattaforma fornita da ACN per il caricamento dei propri dati entro 17 gennaio 2025, in modo che l'Autorità possa procedere a identificarli come soggetti essenziali o importanti;
- fino al 31 dicembre 2025, le imprese dovranno adempiere agli obblighi in materia di segnalazione degli incidenti a partire da nove mesi dalla ricezione della comunicazione di inserimento nella lista dei soggetti importanti o essenziali; per quanto riguarda gli obblighi di gestione del rischio, il termine per l'adempimento è diciotto mesi dalla comunicazione.
- a partire dal 1° gennaio 2026 si applicherà l'obbligo di comunicazione, tramite la piattaforma disposta da ACN, dell'elenco delle proprie attività e servizi, in modo che si possa determinare la categoria di rilevanza del soggetto e dunque le modalità di adempimento agli obblighi del decreto. In questo

senso, il 1° gennaio 2026 si può dire la data di fine della fase di prima applicazione, in quanto a questo punto sarà possibile per l'Autorità, sulla base della categoria di rilevanza e in collaborazione con i tavoli settoriali, determinare precisamente l'entità degli obblighi per ogni soggetto.

Si segnala inoltre che il decreto prevede che ACN, entro il 17 aprile 2025, comunichi alla Commissione europea il numero di soggetti essenziali e importanti dei settori degli allegati I, II e III.

Osservazioni

La portata del decreto impone un forte impegno da parte di tutti i portatori di interesse nel far conoscere alle imprese le misure adottate, e supportarle nell'implementazione.

Alcune date previste in questo Capo, soprattutto la data di caricamento dei propri dati per le imprese dei servizi della società dell'informazione, potrebbero richiedere uno sforzo ancora maggiore, visto il poco tempo a disposizione.

Si rileva inoltre che, se entro il 17 aprile l'Autorità dovrà comunicare una stima dei soggetti essenziali e importanti alla Commissione europea, sarà importante per allora avere già una definizione chiara di tutte le categorie di soggetti sottoposte al presente decreto.