LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo I artt. 1-8 - Disposizioni generali

PNRR

Dossier

Il Decreto Legislativo n. 138 del 2024 rappresenta una pietra miliare nella regolamentazione della cybersicurezza in Italia e recepisce la direttiva europea UE 2022/2555, meglio conosciuta come NIS 2. Questa direttiva è nata dall'esigenza di rafforzare il livello comune di sicurezza informatica tra gli Stati membri dell'Unione Europea per rispondere in modo uniforme e integrato alle crescenti minacce cyber. Come sottolineato nei documenti di riferimento, la direttiva NIS 2 risponde alla preoccupazione per la vulnerabilità delle infrastrutture critiche, evidenziando l'importanza di una cooperazione transfrontaliera per fronteggiare i rischi comuni. Questo quadro normativo armonizza e amplia le misure di cybersicurezza colmando le lacune delle normative dei singoli Stati membri. In Italia, il Decreto Legislativo n. 138 non solo adempie agli obblighi europei, ma si dota di una struttura normativa che riflette le sue specifiche esigenze di sicurezza nazionale. Il decreto enfatizza l'importanza di proteggere i settori essenziali per il funzionamento dell'economia e della società, creando un sistema di risposta e prevenzione che coinvolge autorità nazionali, enti pubblici e privati. L'articolo 1 del decreto stabilisce gli obiettivi generali del testo normativo, mirati a garantire un alto livello di cybersicurezza a livello nazionale e contribuire alla sicurezza dell'Unione Europea. Costituisce la base normativa, delineando una serie di misure per unificare e potenziare le difese informatiche nazionali, collegate direttamente al miglioramento della resilienza del mercato interno. Questo approccio riduce la frammentazione normativa tra i diversi Stati membri, creando un ambiente cibernetico europeo più sicuro e armonizzato. L'articolo 1 evidenzia l'importanza di una cooperazione intergovernativa e interistituzionale che consenta una risposta rapida e coordinata alle minacce cibernetiche. Il decreto stabilisce inoltre l'adozione di una Strategia Nazionale di Cybersicurezza, che include azioni mirate alla protezione di infrastrutture, istituzioni e servizi digitali essenziali. La Strategia risponde alla triplice esigenza di prevenire, rispondere e mitigare i rischi attraverso protocolli chiari che facilitano il coordinamento tra i vari attori nella gestione delle crisi cibernetiche. L'articolo 2 del decreto definisce una serie di concetti e ruoli chiave necessari per applicare e interpretare correttamente il decreto. La definizione di termini tecnici e operativi è essenziale per chiarire contorni delle responsabilità e delle misure previste. Tra i ruoli centrali definiti, l'Agenzia per la Cybersicurezza Nazionale ACN assume particolare rilevanza. Creata nel 2021, **l'ACN è incaricata di attuare e coordinare le politiche di cybersicurezza in Italia e agisce come Autorità nazionale NIS**. **In questo ruolo, monitora le minacce informatiche, fornisce assistenza tecnica e coordina la risposta alle crisi su larga scala**. La definizione dell'**ACN come Punto di contatto unico NIS** rafforza ulteriormente il suo ruolo di interlocutore principale con le autorità europee, permettendo un'interfaccia efficace e

centralizzata per la gestione degli incidenti a livello transfrontaliero. Un altro ruolo fondamentale è quello del **CSIRT - Computer Security Incident Response Team - Italia, che rappresenta il gruppo di risposta nazionale agli incidenti cibernetici**. La sua funzione consiste nel monitorare, rilevare e rispondere agli incidenti in modo rapido, garantendo una protezione efficace delle reti e dei sistemi informatici essenziali. Questa definizione di ruoli e strutture operative facilita la gestione delle emergenze, poiché definisce con chiarezza competenze e responsabilità dei vari enti, evitando sovrapposizioni e inefficienze che potrebbero compromettere la risposta agli incidenti. L'articolo 3 stabilisce l'ambito di applicazione del decreto, specificando i soggetti pubblici e privati sottoposti alle norme di cybersicurezza. Viene delineata una classificazione in **quattro allegati** che includono rispettivamente **settori altamente critici, critici, categorie di pubbliche amministrazioni e altre entità sensibili. Questa organizzazione permette di attribuire livelli di protezione differenziati, concentrando le risorse sui settori più esposti e rilevanti per la stabilità e sicurezza del paese**. I soggetti che superano le dimensioni di una piccola impresa, stabilite dai criteri della raccomandazione UE 2003/361/CE, rientrano automaticamente nell'ambito del decreto, mentre altri soggetti di pubblica utilità vengono inclusi indipendentemente dalle loro dimensioni, come i fornitori di reti pubbliche di comunicazione elettronica e i prestatori di servizi fiduciari. La categorizzazione di allegato I e II riguarda settori ad alta criticità e criticità, riflettendo l'importanza di proteggere quei settori che costituiscono l'ossatura delle infrastrutture e dei servizi essenziali. **Questa struttura di ambito applicativo consente di indirizzare le risorse disponibili e definire misure di protezione adeguate al rischio specifico di ciascun settore**. L'articolo 4 garantisce che il decreto non comprometta la sovranità nazionale in ambiti fondamentali come la sicurezza, la difesa e l'ordine pubblico. In virtù di ciò, alcune istituzioni e organismi di sicurezza, come il **Parlamento italiano, le forze di polizia e i servizi di intelligence, sono esclusi dalle disposizioni del decreto per preservare la loro autonomia e riservatezza operativa**. Come evidenziato dai dossier, questa scelta normativa è giustificata dal fatto che tali entità svolgono ruoli di alta sensibilità, dove l'esigenza di protezione e riservatezza supera quella di integrazione normativa. Questo articolo consente al governo di escludere alcuni soggetti dalle normative del decreto tramite decreti del Presidente del Consiglio, in accordo con l'ACN. Questa flessibilità normativa permette di adattare l'applicazione delle misure di sicurezza informatica in base all'evoluzione delle minacce e alle esigenze specifiche di protezione dei dati strategici, evitando che informazioni riservate possano essere esposte o compromesse. L'articolo 5 disciplina le modalità di giurisdizione e territorialità per i soggetti obbligati a conformarsi al decreto. In particolare, stabilisce che **i fornitori di servizi digitali critici, come i servizi di cloud**

computing o le reti di distribuzione dei contenuti, siano soggetti alla giurisdizione dello Stato membro in cui risiede il loro stabilimento principale, definito come il luogo in cui vengono prese le decisioni di gestione del rischio informatico. Nei casi in cui non sia possibile determinare un centro decisionale nell'Unione Europea, si considera lo stabilimento con il maggior numero di dipendenti nell'UE. **Questa disposizione è fondamentale per gestire e regolamentare i fornitori di servizi digitali che operano in più Stati membri, garantendo che le misure di cybersicurezza siano applicate in modo uniforme senza sovrapposizioni o conflitti giurisdizionali**. I dossier evidenziano che tale approccio assolve alla necessità di una governance condivisa e regolamentata dei servizi digitali transnazionali, minimizzando i rischi derivanti dalla frammentazione normativa. L'articolo 6 introduce le categorie di soggetti essenziali e importanti, definendo i primi come quelli con un impatto diretto e significativo sulla resilienza nazionale e i secondi come entità di rilevanza minore, ma comunque necessarie per la sicurezza informatica. La classificazione dei soggetti essenziali include imprese che superano i parametri dimensionali delle piccole imprese, oltre a entità specifiche che operano in settori di alta criticità. Come riportato nei documenti di supporto, questa categorizzazione permette di concentrare misure di cybersicurezza avanzate per i soggetti più rilevanti, senza appesantire le realtà minori. **L'Autorità nazionale NIS ha anche il compito di identificare altri soggetti da classificare come essenziali, permettendo di includere in modo dinamico nuove entità in base al loro impatto potenziale sulla sicurezza informatica nazionale. L'articolo 7 stabilisce le procedure di identificazione e registrazione dei soggetti essenziali e importanti, imponendo un obbligo di registrazione annuale sulla piattaforma digitale NIS**. **Ogni soggetto deve fornire informazioni aggiornate riguardanti la ragione sociale, l'indirizzo, i recapiti, nonché dettagli tecnici come gli indirizzi IP e i nomi di dominio. Questo obbligo di registrazione permette all'ACN di mantenere un registro accurato delle infrastrutture e dei servizi critici, facilitando il monitoraggio e la gestione delle minacce**. Il dossier sottolinea l'importanza di questa piattaforma, che consente un controllo centralizzato e un coordinamento rapido delle risorse in caso di emergenza. L'articolo 8 garantisce che **il trattamento dei dati personali avvenga in conformità con le normative europee, in particolare il GDPR e la direttiva e-Privacy. Questa disposizione impone un uso proporzionato e limitato dei dati personali per finalità strettamente connesse alla sicurezza informatica, garantendo al contempo che i fornitori di reti e servizi digitali proteggano adeguatamente la privacy degli utenti**. Come riportato, questa norma tutela gli interessi degli utenti, bilanciando le esigenze di sicurezza con la protezione della privacy.

Dall'analisi delle disposizioni generali del Decreto Legislativo n. 138 del 2024 si coglie un passaggio chiave verso un sistema di sicurezza informatica integrato e resiliente in Italia, in linea con gli standard europei. Il decreto non solo recepisce le direttive NIS 2, ma crea un quadro normativo che riconosce la complessità del contesto italiano, offrendo un sistema di protezione flessibile e adattabile alle esigenze di sicurezza in continua evoluzione.

Articolo 1 del Decreto Legislativo 4 settembre 2024, n. 138

L'**articolo 1** del Decreto Legislativo 4 settembre 2024, n. 138, delinea l'oggetto del provvedimento normativo e stabilisce il contesto delle misure adottate per rafforzare la sicurezza informatica in Italia, in linea con le esigenze dell'Unione europea. L'articolo si apre con un chiaro obiettivo: garantire un livello elevato di sicurezza informatica a livello nazionale per contribuire a un livello comune elevato di cibersicurezza nell'UE, elemento cruciale per assicurare il corretto funzionamento del mercato interno. Questo approccio integrato sottolinea l'interconnessione tra la sicurezza nazionale e la stabilità economica e tecnologica dell'Unione. Al **comma 1**, il decreto si prefigge di implementare misure coordinate e strategiche per accrescere la resilienza informatica italiana. Queste misure si allineano con la direttiva UE 2022/2555, conosciuta come direttiva NIS 2, che mira a rafforzare la sicurezza delle reti e dei sistemi informativi nell'intera Unione europea. **La direttiva NIS 2 nasce per superare le limitazioni della precedente direttiva UE 2016/1148, rispondendo all'evoluzione delle minacce cibernetiche e agli attacchi sempre più sofisticati e frequenti**. Il **comma 2** specifica le componenti essenziali di questa iniziativa normativa, articolate in diverse lettere, ciascuna delle quali rappresenta un elemento chiave per l'attuazione del decreto: La **lettera a)** introduce la **Strategia nazionale di cybersicurezza**, un documento programmatico che orienta le politiche e le azioni nazionali per garantire la sicurezza informatica. Questa strategia è necessaria per delineare priorità e obiettivi che coprano tutte le sfere della cibersicurezza, integrando risorse e capacità sia pubbliche che private.

La **lettera b)** richiama l'importanza di un **quadro di gestione delle crisi informatiche** che si inserisca nella struttura nazionale preesistente per la gestione delle crisi. Questo quadro deve considerare l'articolo 10 del decreto-legge 4 giugno 2021, n. 82, successivamente convertito con modifiche dalla legge 4 agosto 2021, n. 109, che ha istituito l'Agenzia per la

cybersicurezza nazionale ACN. L'integrazione tra la nuova normativa e l'esistente quadro di risposta alle crisi garantisce una coerenza e un'efficienza operativa indispensabili durante situazioni di emergenza cibernetica.

La **lettera c)** conferma l'ACN come autorità centrale per diverse funzioni: come **Autorità nazionale competente NIS**, la cui responsabilità include l'attuazione e la supervisione delle norme stabilite dal decreto; come **Punto di contatto unico NIS**, che funge da snodo per il coordinamento con le istituzioni europee e internazionali; e come **CSIRT Italia**, il team nazionale per la risposta agli incidenti informatici, la cui attività è essenziale per il monitoraggio e la risposta rapida agli eventi cibernetici.

La **lettera d)** evidenzia il ruolo dell'ACN e del **Ministero della difesa** come autorità per la gestione delle crisi informatiche su vasta scala. Questo punto ribadisce la necessità di una cooperazione interministeriale e di una chiara definizione dei ruoli per affrontare situazioni di crisi, rafforzando l'importanza della collaborazione con il **Nucleo per la cybersicurezza**, un ente istituito per la gestione coordinata delle emergenze.

La **lettera e)** stabilisce l'identificazione di **Autorità di settore NIS**, che agiscono in collaborazione con l'ACN. Questa rete di autorità garantisce che le competenze settoriali siano integrate in un sistema di sicurezza informatica che abbraccia tutto il territorio nazionale e si allinea con gli standard europei.

La **lettera f)** introduce i criteri per determinare i **soggetti cui si applica il decreto** e i relativi obblighi di gestione dei rischi e di notifica degli incidenti. Questo è un punto critico, poiché implica l'identificazione precisa dei soggetti essenziali e importanti, definizione che deriva direttamente dalle linee guida della direttiva NIS 2. L'obiettivo è assicurare che le infrastrutture critiche e i servizi essenziali siano protetti da rischi cibernetici, adottando misure preventive e reattive proporzionate al livello di rischio.

Infine, la **lettera g)** si focalizza sulla necessità di un robusto quadro di **cooperazione e condivisione delle informazioni** a livello europeo. Questo include la partecipazione al **Gruppo di cooperazione NIS**, che è composto dalle autorità competenti degli Stati membri e ha lo scopo di facilitare l'implementazione coerente della direttiva NIS 2 attraverso lo scambio di esperienze e pratiche. Si menziona anche la partecipazione alla **Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)**, un meccanismo operativo per la gestione delle crisi cibernetiche su scala europea, e alla **Rete di**

CSIRT nazionali, fondamentale per la condivisione tecnica di informazioni e per la coordinazione delle risposte a incidenti transfrontalieri.

Questo articolo del decreto rappresenta il punto di partenza per una legislazione che ambisce a rafforzare la resilienza cibernetica nazionale, integrandosi pienamente con le direttive europee e promuovendo una risposta coordinata alle minacce informatiche. **L'approccio è sia preventivo che reattivo, garantendo che l'Italia partecipi attivamente alle iniziative europee per la cibersicurezza e si doti di strumenti e strategie in grado di tutelare le sue infrastrutture critiche, il settore pubblico e privato, nonché l'intera cittadinanza**.

Articolo 2 del Decreto Legislativo n. 138 del 2024

L'articolo 2 del Decreto Legislativo n. 138 del 2024 introduce una serie di definizioni fondamentali per comprendere e applicare il decreto, specificando concetti tecnici e ruoli chiave relativi alla cybersicurezza, essenziali per garantire coerenza e chiarezza operativa nell'implementazione delle misure di sicurezza informatica. **La *Strategia nazionale di cybersicurezza* rappresenta un quadro strategico che individua obiettivi e priorità di sicurezza informatica a livello nazionale, delineando le modalità di governance per il loro raggiungimento**; questa strategia funge da riferimento centrale per il rafforzamento delle capacità di risposta a incidenti e minacce cibernetiche, contribuendo alla resilienza complessiva del paese. **L'*Agenzia per la cybersicurezza nazionale* ACN, istituita nel 2021, è l'ente nazionale responsabile della gestione della sicurezza informatica, investito del ruolo di Autorità nazionale NIS e Punto di contatto unico NIS**; **l'ACN ha il compito di coordinare le risposte agli incidenti informatici su larga scala, sia a livello nazionale che transfrontaliero, e di facilitare il dialogo e la cooperazione con le autorità europee e internazionali**. Il ***Nucleo per la cybersicurezza*, gruppo di supporto coordinato dall'ACN, è attivato in situazioni di emergenza per assistere il governo nella risposta a crisi di sicurezza informatica estese e complesse**. Per la risposta operativa agli incidenti di sicurezza informatica a livello nazionale, l'Italia dispone del ***CSIRT Italia*, un gruppo dedicato che opera all'interno dell'ACN, mentre il *Gruppo di cooperazione NIS* e la rete *EU-CyCLONe* facilitano a livello europeo la collaborazione tra Stati membri,**

rispettivamente per la cooperazione strategica e per la gestione operativa di crisi informatiche significative.

Tra le definizioni tecniche si evidenzia quella di ***sistema informativo e di rete***, che comprende infrastrutture digitali quali reti di comunicazione, dispositivi collegati e dati digitali impiegati per l'elaborazione e trasmissione delle informazioni. **La *sicurezza dei sistemi informativi e di rete*, insieme alla *sicurezza informatica*, indica la capacità di questi sistemi di resistere a eventi che potrebbero comprometterne la disponibilità, integrità e riservatezza dei dati, proteggendo sia le infrastrutture sia gli utenti**. Vengono definiti anche gli ***incidenti*** come eventi che compromettono la sicurezza dei dati o dei servizi, e i ***quasi-incidenti*** o near-miss, cioè minacce evitate o mitigate prima che si trasformino in danni effettivi. La definizione di ***incidente di sicurezza informatica su vasta scala*** identifica incidenti particolarmente gravi che superano la capacità di risposta di un singolo Stato o colpiscono più Stati membri, richiedendo così interventi coordinati e un monitoraggio a livello europeo. Il termine ***minaccia informatica*** copre qualsiasi evento con potenziale impatto negativo su sistemi e reti, con la ***minaccia significativa*** che rappresenta una versione aggravata, in grado di causare danni rilevanti o su vasta scala. **Si introduce anche l'*approccio multi-rischio*, che riconosce come le minacce informatiche siano spesso interconnesse con rischi fisici, come le interruzioni di energia o le calamità naturali, e richiede una gestione integrata per coprire tutte le tipologie di minacce ai sistemi e al contesto fisico**. In ambito tecnologico, i *prodotti e servizi TIC* - Tecnologie dell'Informazione e Comunicazione - rappresentano rispettivamente componenti hardware e software e i servizi collegati alla gestione, trasmissione, conservazione e elaborazione di informazioni digitali. **Una definizione essenziale è quella di *vulnerabilità*, ossia un punto debole nei prodotti o servizi TIC che può essere sfruttato da una minaccia per causare danni o accessi non autorizzati**. Gli *Internet Exchange Point* IXP e il *sistema dei nomi di dominio* DNS sono componenti cruciali per la connettività Internet, facilitando il traffico e garantendo l'indirizzamento e accessibilità delle risorse online. **Infrastrutture avanzate come il *servizio di cloud computing*, i *data center* e la *rete di distribuzione dei contenuti* CDN consentono la gestione su vasta scala e distribuita di dati e contenuti digitali, migliorando l'accessibilità e la continuità dei servizi per gli utenti e minimizzando le interruzioni anche in caso di problemi locali**. Altri concetti di rilievo comprendono i *servizi fiduciari*, che verificano e proteggono l'integrità delle transazioni digitali, come le firme elettroniche, e i *mercati online*, piattaforme dove utenti e professionisti possono condurre transazioni in modo sicuro. L'*audit* è un processo di verifica indipendente e

sistematica dei requisiti di sicurezza informatica, condotta da un organismo qualificato o dall'autorità NIS stessa per confermare la conformità ai requisiti del decreto. **L'articolo 2 fornisce un vocabolario standardizzato, stabilendo una base comune per la gestione della sicurezza informatica e agevolando la cooperazione tra soggetti pubblici e privati; questo linguaggio comune è indispensabile per garantire chiarezza nei ruoli, nelle responsabilità e nelle tecnologie coinvolte, migliorando la resilienza del sistema cibernetico italiano nel contesto di sicurezza europeo.**

Articolo 3 del Decreto Legislativo n. 138 del 2024

L'articolo 3 del Decreto Legislativo n. 138 del 2024 stabilisce i criteri di inclusione e le categorie di soggetti cui si applicano le misure di cybersicurezza previste dal decreto, delineando un ambito di applicazione che comprende sia soggetti pubblici sia privati la cui sicurezza informatica è fondamentale per la resilienza e il funzionamento critico del paese. Il decreto si applica ai soggetti individuati negli allegati I, II, III e IV, che includono rispettivamente settori altamente critici, settori critici, categorie di pubbliche amministrazioni e ulteriori tipologie di soggetti sensibili. **Gli allegati I e II identificano i settori ritenuti più esposti a rischi per la sicurezza informatica e, pertanto, i settori dove eventuali attacchi o interruzioni possono avere impatti gravi e diffusi sulla stabilità economica e sociale. Gli allegati III e IV individuano invece le categorie di pubbliche amministrazioni e altri soggetti essenziali, inclusi quelli operanti in settori rilevanti che forniscono servizi critici o infrastrutture strategiche.** Il decreto si applica principalmente ai soggetti privati che superano le dimensioni delle piccole imprese, secondo i criteri stabiliti dalla raccomandazione UE 2003/361/CE, rendendo il decreto applicabile in modo mirato ai soggetti con risorse adeguate e un impatto significativo sulle infrastrutture critiche. Tale criterio consente di concentrare l'applicazione delle norme NIS 2 su quelle realtà aziendali che, per volume, impatto economico e connettività, possono rappresentare un rischio maggiore. Tuttavia, alcuni criteri di esclusione contenuti nella raccomandazione non sono applicabili in questo contesto per mantenere un'indipendenza operativa tra le diverse imprese, come nel caso di sistemi informativi e servizi in outsourcing. Il decreto si applica anche, indipendentemente dalla dimensione, ai soggetti individuati come critici secondo la direttiva UE 2022/2557 e a categorie specifiche di fornitori

essenziali quali fornitori di reti pubbliche e servizi di comunicazione elettronica accessibili al pubblico, prestatori di servizi fiduciari, gestori di domini di primo livello e fornitori di servizi DNS. Questi soggetti svolgono un ruolo fondamentale nelle infrastrutture digitali, offrendo servizi che, per natura e diffusione, sono essenziali per il funzionamento di molti altri settori e per la sicurezza dei dati degli utenti finali. **Anche le pubbliche amministrazioni elencate nell'Allegato III sono incluse senza discriminazione di dimensione, con una possibile estensione dell'elenco stesso per decreto del Presidente del Consiglio in base all'evoluzione delle minacce, all'esposizione al rischio e all'impatto potenziale di incidenti**. Il decreto introduce un meccanismo di inclusione che si applica a ulteriori soggetti strategici non solo in base alla dimensione, ma anche alla loro importanza strutturale o alla potenziale rilevanza nazionale dei servizi forniti. Vengono inclusi, quindi, operatori di servizi essenziali e fornitori unici di servizi critici, soggetti per cui un'interruzione delle attività potrebbe generare rischi significativi per la sicurezza pubblica, la salute, l'economia o la stabilità regionale o transfrontaliera. Tra i criteri per questa inclusione figurano la rilevanza nazionale, il ruolo sistemico nel mercato, l'importanza strategica a livello territoriale e l'incidenza su altri settori economici o su aree di intervento digitale. Anche le imprese collegate a soggetti importanti o essenziali sono incluse nel decreto quando hanno un'influenza dominante o se gestiscono sistemi informativi e infrastrutture vitali per l'attività di soggetti critici o essenziali, o ancora, se forniscono a questi ultimi servizi TIC o di sicurezza informatica. Questo approccio considera quindi l'interconnessione operativa delle imprese per evitare che vulnerabilità presenti in soggetti collegati possano rappresentare un punto debole nella catena di sicurezza globale. Per proteggere i dati personali, l'applicazione del decreto resta conforme alle normative europee e italiane in tema di protezione dati, in particolare al GDPR e alle leggi italiane sulla privacy. **Le procedure di inclusione dei soggetti rientrano nelle competenze dell'Autorità nazionale competente NIS, la quale, su segnalazione delle Autorità di settore, può includere nuovi soggetti nelle categorie designate. I soggetti inclusi vengono notificati e sono obbligati alla registrazione presso il sistema previsto dal decreto**. Inoltre, il decreto riserva alcune limitazioni per i settori già regolamentati a livello europeo, come il settore finanziario, e per soggetti esentati da altre normative UE specifiche, con l'obiettivo di evitare sovrapposizioni normative. L'articolo 3 del Decreto Legislativo n. 138 del 2024 disegna quindi un ambito di applicazione articolato e flessibile, che garantisce la copertura di settori e soggetti di rilevanza strategica per la sicurezza informatica nazionale, mantenendo al contempo un equilibrio tra dimensioni, rischi specifici, importanza sistemica e conformità alle normative già esistenti.

Articolo 4 del Decreto Legislativo n. 138 del 2024

L'articolo 4 del Decreto Legislativo n. 138 del 2024 stabilisce che **il decreto non intacca la responsabilità dello Stato italiano nella tutela della sicurezza nazionale, lasciando invariato il potere dello Stato di proteggere l'integrità territoriale, l'ordine pubblico e altre funzioni essenziali**. **Sono esclusi dall'applicazione del decreto**, per garantire il rispetto delle prerogative costituzionali e la riservatezza di specifiche istituzioni, soggetti quali il **Parlamento italiano, l'Autorità giudiziaria, la Banca d'Italia e l'Unità di informazione finanziaria per l'Italia. A questi enti, insieme agli organi di rilevanza costituzionale, non si applicano le disposizioni del Capo V del decreto, che prevede particolari obblighi di conformità in tema di cybersicurezza. Il decreto inoltre non si applica agli enti, organi e articolazioni della pubblica amministrazione coinvolti in settori di pubblica sicurezza, difesa nazionale o attività di contrasto, che includono indagini e perseguimenti di reati, né agli organismi di informazione per la sicurezza nazionale, come stabilito dalla legge n. 124 del 2007, e nemmeno all'Agenzia per la cybersicurezza nazionale ACN**. Queste esclusioni intendono proteggere settori estremamente sensibili, dove la gestione delle informazioni e delle procedure operative richiede un livello di riservatezza e autonomia elevato per prevenire interferenze o esposizioni a rischi informatici. Ulteriori specificazioni sono fornite attraverso decreti del Presidente del Consiglio, in collaborazione con i ministri competenti per giustizia, difesa e interno e in accordo con l'ACN, per identificare soggetti che svolgono attività esclusive per enti di pubblica sicurezza, difesa e protezione civile. Tali soggetti, nell'ambito delle loro attività specifiche, non sono soggetti agli obblighi del Capo IV, che disciplina le misure di sicurezza e notifica degli incidenti, né alle disposizioni del Capo V. Questo esonero riconosce la particolare natura delle attività di questi soggetti, che potrebbero richiedere approcci differenti rispetto alle misure di cybersicurezza stabilite per il settore civile. Con un ulteriore decreto del Presidente del Consiglio, ai sensi dell'articolo 43 della legge n. 124 del 2007, vengono individuati i soggetti che operano esclusivamente per gli organismi di informazione per la sicurezza nazionale. Anche per questi soggetti, nell'ambito delle loro attività specifiche, non si applicano gli obblighi di cybersicurezza stabiliti nei Capi IV e V, con notifica all'ACN delle decisioni adottate per garantire una supervisione centrale. Gli enti che regolano o svolgono attività solo marginalmente correlate ai settori di sicurezza e difesa non possono essere esclusi dalle norme del decreto. Allo stesso modo, non possono essere esonerati i prestatori di servizi fiduciari, i quali devono continuare a garantire un livello di sicurezza

informatica conforme agli obblighi generali di cui al Capo IV. L'obiettivo è assicurare una protezione minima anche nelle aree marginalmente connesse alle funzioni essenziali, per evitare falle nella sicurezza generale e garantire la conformità alle disposizioni di sicurezza informatica su vasta scala. **Gli obblighi previsti dal decreto non richiedono la divulgazione di informazioni riservate che potrebbero compromettere gli interessi essenziali dello Stato in materia di sicurezza, pubblica sicurezza e difesa. Tale protezione si estende anche alle informazioni classificate come riservate sia dalla normativa dell'Unione Europea sia da quella italiana, per salvaguardare gli affari commerciali sensibili e altri dati protetti.** Lo scambio di tali informazioni con la Commissione europea o con autorità competenti di altri Stati membri avviene solo quando strettamente necessario per l'applicazione del decreto, assicurando che le informazioni condivise siano proporzionate allo scopo e che vengano protetti sia la riservatezza sia gli interessi commerciali dei soggetti essenziali e importanti.

Articolo 5 del Decreto Legislativo n. 138 del 2024

L'articolo 5 del Decreto Legislativo n. 138 del 2024 **disciplina la giurisdizione e territorialità dei soggetti obbligati a conformarsi alle disposizioni di cybersicurezz**a stabilite dal decreto, definendo le circostanze in cui essi ricadono sotto la giurisdizione italiana o di altri Stati membri dell'Unione Europea. **Sono generalmente sottoposti alla giurisdizione nazionale tutti i soggetti stabiliti sul territorio italiano, con alcune eccezioni specifiche: i fornitori di reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico sono invece soggetti alla giurisdizione del Paese membro in cui erogano i propri servizi**. Altre tipologie di fornitori – quali quelli di servizi di DNS, registri di nomi di dominio di primo livello, cloud computing, data center, reti di distribuzione contenuti, servizi gestiti e di sicurezza gestiti, mercati online, motori di ricerca e piattaforme di social network – sono sottoposti alla giurisdizione dello Stato membro dell'Unione **dove hanno il proprio *stabilimento principale*, inteso come il luogo in cui vengono prese le decisioni primarie riguardanti la gestione dei rischi per la sicurezza informatica**. Se lo stabilimento principale non è determinabile o non risiede nell'Unione, si considera come principale quello situato nel Paese in cui sono prevalentemente svolte le attività di sicurezza informatica o, in alternativa, quello con il maggior numero di dipendenti nell'Unione. Gli enti

della pubblica amministrazione italiana sono sottoposti alla giurisdizione dello Stato italiano, mentre quelli istituiti da altri Stati membri restano sotto la giurisdizione del rispettivo Paese di origine. Per i soggetti che forniscono servizi all'interno dell'Unione senza avere una sede fisica sul suo territorio, è obbligatoria la designazione di un rappresentante nell'Unione Europea, stabilito in uno degli Stati membri in cui i servizi vengono offerti. Tale rappresentante, oltre a fungere da punto di contatto, è soggetto alla giurisdizione del Paese di stabilimento e risponde dei requisiti e delle normative di cybersicurezza per conto del soggetto estero che rappresenta. Nel caso in cui un soggetto non adempia a questo obbligo di designazione, l'Autorità nazionale competente NIS italiana ha la facoltà di avviare azioni legali per far rispettare gli obblighi previsti dal decreto. La nomina del rappresentante europeo non limita né impedisce eventuali azioni legali già in corso, le quali possono proseguire per violazioni degli obblighi del decreto; ciò include l'imposizione degli obblighi di sicurezza informatica indicati nel Capo IV e l'esercizio dei poteri di controllo e intervento specificati nel Capo V. Questo sistema di giurisdizione stabilisce un quadro chiaro per la competenza normativa, assicurando che ogni soggetto che fornisce servizi digitali critici o di importanza strategica all'interno dell'UE sia conforme alle normative di cybersicurezza, anche quando opera a distanza o in assenza di una sede stabile sul territorio europeo.

Articolo 6 del Decreto Legislativo n. 138 del 2024

L'articolo 6 del Decreto Legislativo n. 138 del 2024 distingue tra *soggetti essenziali* e *soggetti importanti*, due categorie cruciali per l'attuazione delle misure di cybersicurezza del decreto**. I *soggetti essenziali* sono individuati come quelli la cui operatività è critica per la stabilità e la sicurezza del Paese, e pertanto devono conformarsi a standard di sicurezza informatica particolarmente rigorosi**. Rientrano in questa categoria i soggetti elencati nell'Allegato I del decreto, purché superino le soglie dimensionali delle medie imprese, definite secondo i criteri della raccomandazione UE 2003/361/CE. Questo implica che le imprese di grandi dimensioni, operanti in settori altamente critici, devono applicare misure stringenti per la protezione dei loro sistemi informativi. Indipendentemente dalla loro dimensione, vengono inoltre classificati come essenziali i soggetti già identificati come critici dal decreto legislativo che recepisce la direttiva UE 2022/2557, i fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico che rientrano nella definizione di medie imprese, nonché i prestatori di servizi fiduciari qualificati, i gestori di registri di nomi di

dominio di primo livello e i fornitori di sistemi DNS. Anche le amministrazioni centrali dello Stato indicate nell'Allegato III, come i ministeri e altri enti governativi, rientrano tra i soggetti essenziali, data la loro importanza per la continuità amministrativa e la protezione di informazioni sensibili. L'Autorità nazionale competente NIS, secondo le modalità previste dall'articolo 40 del decreto, ha la facoltà di identificare ulteriori soggetti come essenziali, anche se non rientrano automaticamente nelle categorie indicate. Questa facoltà le consente di valutare e aggiornare la lista dei soggetti essenziali in base al contesto operativo e al potenziale impatto delle loro attività sulla sicurezza nazionale, tenendo conto di specifiche caratteristiche come la dimensione, il ruolo strategico o la particolare vulnerabilità del soggetto in questione. **I *soggetti importanti* sono, invece, quelli che non rientrano nei criteri di essenzialità descritti per i soggetti essenziali, ma che, operando in settori critici e sensibili, devono comunque adottare misure di cybersicurezza conformi agli standard indicati nel decreto**. Sebbene non siano classificati come essenziali, il loro ruolo e la loro interconnessione con altri soggetti critici ne richiedono la protezione per garantire la sicurezza e l'integrità complessiva dell'infrastruttura nazionale e del sistema digitale.

Articolo 7 del Decreto Legislativo n. 138 del 2024

L'articolo 7 del Decreto Legislativo n. 138 del 2024 stabilisce le **modalità di identificazione e registrazione annuale dei *soggetti essenziali* e *soggetti importanti* ai fini della cybersicurezza, imponendo obblighi di aggiornamento e trasmissione delle informazioni tramite una piattaforma digitale predisposta dall'Autorità nazionale competente NIS, gestita dall'Agenzia per la cybersicurezza nazionale**. **Dal 1° gennaio al 28 febbraio di ogni anno, tutti i soggetti elencati nell'articolo 3 del decreto sono tenuti a registrarsi o aggiornare la propria registrazione sulla piattaforma, inserendo almeno i dettagli essenziali quali ragione sociale, indirizzo, recapiti (inclusi e-mail e numeri di telefono), un punto di contatto (con ruolo e recapiti), e informazioni specifiche sui settori e le tipologie a cui appartengono, secondo quanto stabilito negli allegati I, II, III e IV.** Successivamente, entro il 31 marzo, l'Autorità nazionale NIS compila un elenco aggiornato dei soggetti essenziali e importanti basandosi sulle registrazioni annuali e sulle decisioni derivanti dagli articoli 3, 4 e 6 del decreto. L'Autorità comunica ai soggetti interessati, attraverso la piattaforma digitale, la loro inclusione, permanenza o eventuale espunzione dall'elenco dei

soggetti essenziali e importanti. **Per garantire la sicurezza delle informazioni e l'allineamento alle normative NIS, dal 15 aprile al 31 maggio, i soggetti che hanno ricevuto notifica di inclusione o permanenza nell'elenco devono aggiornare o fornire ulteriori informazioni. Queste includono dettagli tecnici, come gli indirizzi IP pubblici e i nomi di dominio in uso, gli Stati membri in cui forniscono servizi coperti dal decreto, i nominativi e recapiti dei responsabili per la sicurezza, nonché il nome e i dettagli di un sostituto del punto di contatto designato.** Per quanto riguarda specifici operatori digitali come fornitori di servizi DNS, cloud computing, data center, mercati online, motori di ricerca e piattaforme di social network, essi devono anche fornire ulteriori dettagli, come l'indirizzo della sede principale e delle altre sedi nell'Unione Europea; se non dispongono di una sede fisica nell'UE, devono indicare l'indirizzo del rappresentante designato nell'UE, assieme ai suoi contatti aggiornati. L'Autorità NIS ha il compito di definire i termini, modalità e procedimenti per l'accesso e l'uso della piattaforma digitale, oltre a stabilire qualsiasi ulteriore informazione che i soggetti devono fornire o aggiornare. Per i rappresentanti dei soggetti esteri, l'Autorità stabilisce le procedure di designazione. Infine, i soggetti notificati come essenziali o importanti sono obbligati a informare tempestivamente l'Autorità NIS, entro quattordici giorni, di qualsiasi modifica ai dati forniti, assicurando così un aggiornamento costante delle informazioni critiche per la sicurezza informatica nazionale.

Articolo 8 del Decreto Legislativo n. 138 del 2024

L'articolo 8 del Decreto Legislativo n. 138 del 2024 stabilisce le norme per la protezione dei dati personali nel contesto delle misure di cybersicurezza. **L'Agenzia per la cybersicurezza nazionale, le Autorità di settore NIS e i soggetti individuati all'articolo 3 del decreto possono trattare i dati personali unicamente nella misura necessaria per adempiere agli obblighi di sicurezza previsti, sempre in conformità con le disposizioni del decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali e del Regolamento UE 2016/679 GDPR. Questo significa che qualsiasi operazione di raccolta, utilizzo o conservazione di dati personali deve rispettare i principi di necessità, proporzionalità e finalità, assicurando che i dati trattati siano strettamente pertinenti e limitati agli scopi specifici di cybersicurezza.** Per quanto riguarda i fornitori di reti pubbliche di

comunicazione elettronica e i servizi di comunicazione elettronica accessibili al pubblico, il trattamento dei dati personali deve conformarsi non solo alla normativa generale in materia di protezione dei dati ma anche alla legislazione europea specifica sulla tutela della vita privata nel settore delle comunicazioni elettroniche. A questo proposito, la direttiva 2002/58/CE, nota come e-Privacy Directive, impone ulteriori obblighi per garantire la riservatezza delle comunicazioni e la protezione dei dati personali degli utenti di tali servizi. **Queste disposizioni richiedono che i dati raccolti siano utilizzati in modo che sia minimizzato qualsiasi rischio per la privacy e che le operazioni di trattamento siano sempre giustificate da finalità precise legate alla cybersicurezza.**