Gianluca Amarù,
Alessandra Fava, Marco Fossi,
Eleonora Maschio

NIS2: come rafforzare la cybersicurezza

Le aziende coinvolte, le procedure operative e i controlli interni

MANAGEMENT

FrancoAngeli

TOOLS

I lettori che desiderano informarsi sui libri e le riviste da noi pubblicati
possono consultare il nostro sito Internet: *www.francoangeli.it* e iscriversi nella home page
al servizio "Informatemi" per ricevere via e.mail le segnalazioni delle novità
o scrivere, inviando il loro indirizzo, a "FrancoAngeli, viale Monza 106, 20127 Milano".

Gianluca Amarù,
Alessandra Fava, Marco Fossi,
Eleonora Maschio

NIS2: come rafforzare la cybersicurezza

Le aziende coinvolte, le procedure operative e i controlli interni

FrancoAngeli
TOOLS

Isbn: 9788835179542

Copyright © 2025 by FrancoAngeli s.r.l., Milano, Italy.

L'opera, comprese tutte le sue parti, è tutelata dalla legge sul diritto d'autore.
Sono riservati i diritti per Text and Data Mining (TDM), AI training e tutte le tecnologie simili.
L'Utente nel momento in cui effettua il download dell'opera accetta tutte le condizioni della licenza d'uso dell'opera previste e comunicate sul sito www.francoangeli.it

Indice

Prefazione, di *Luca Christian Natali* pag. 7

1. Il significato di *cybersecurity*. La nascita e gli aspetti giuridici e tecnico-informatici della cibersicurezza » 11
1.1. La definizione di *cybersicurity* » 11
1.2. Origine del concetto di *cybersecurity* » 12
1.3. Quadro giuridico della *cybersecurity*: normativa comunitaria ed italiana » 12

2. NIS2: che cosa dice la Direttiva UE e come è stata recepita in Italia col Decreto Legislativo n. 138/2024 » 15
2.1. Il contenuto della Direttiva UE e il recepimento in Italia con il Decreto Legislativo n. 138/2024 » 15
2.2. Il Decreto Legislativo n. 138/2024 e il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) » 16
2.3. L'ambito di applicazione del Decreto Legislativo n. 138/2024 » 17
2.4. Gli obblighi prescritti dal Decreto Legislativo n. 138/2024 per Aziende ed Enti soggetti alla normativa NIS2 » 18
2.5. Sanzioni e meccanismi di conformità previsti nel Decreto Legislativo n. 138/2024 » 19

3. I soggetti sottoposti alla NIS2, settori ad alta criticità ed altri settori critici » 23
3.1. I criteri per individuare le imprese sottoposte agli obblighi della Direttiva NIS2 » 23
3.2. I settori altamente critici e quelli critici secondo il Legislatore europeo » 25
3.3. I soggetti obbligati al rispetto della Direttiva NIS2 » 25
3.3.1. Premessa » 25
3.3.2. La qualificazione dei Soggetti nei settori NIS2 » 26

3.4. I soggetti essenziali ed importanti pag. 38
3.5. Informazioni necessarie al momento dell'iscrizione » 39
3.6. Imprese controllate, collegate e gruppi di imprese: criteri di individuazione » 40
3.7. Informazioni necessarie al momento dell'iscrizione delle imprese controllate, collegate e dei gruppi di imprese e l'applicazione della *clausola di salvaguardia* » 44

4. Il concetto di catena dei fornitori o *supply chain* e norme relative » 47

5. Come valutare se la tua azienda deve o no aderire alla NIS2 e le aziende escluse » 49

6. Come applicare la NIS2 e il Decreto Legislativo: indicazioni pratiche » 51
6.1. *Timeline* degli adempimenti » 51
6.2. La formazione per le figure apicali e il personale » 52
6.3. Le misure e le procedure di sicurezza » 52
6.3.1. Le misure di sicurezza previste dalla Direttiva NIS2 » 52
6.3.2. Le procedure necessarie a garantire la sicurezza informatica » 54
6.4. La notifica degli incidenti informatici significativi » 57
6.5. L'attività di auditing e monitoraggio » 59
6.6. Le sanzioni previste » 60
6.7. Il *Risk Assessment* ed il *Pen Test* » 61
6.8. Accountability » 63

7. La *check list* per la qualificazione dei soggetti sottoposti a NIS2 e come iscriversi al Registro ACN » 65
Allegato 1 – NIS2 check-list di valutazione » 66
Allegato 2 – Determinazione del Direttore generale dell'Agenzia per la cibersicurezza nazionale » 73
Allegato 3 – Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio » 82
Allegato 4 – Modello delega punto di contatto con ACN » 122
Allegato 5 – Decreto Legislativo 4 settembre 2024, n. 138 » 124
Allegato 6 – Decreto del Presidente del Consiglio dei Ministri, 9 dicembre 2024, n. 221 » 183

Bibliografia » 187

Prefazione

di *Luca Christian Natali**

Gli Autori, che conosco e stimo da tempo, mi hanno onorato dell'incarico di contribuire alla loro opera con la Prefazione alla stessa. È stata una lettura agevole e rapida, poiché il testo esaminato si contraddistingue per l'essere decisamente lineare e chiaro, pur trattando tematiche giuridiche e tecniche della sicurezza cibernetica, di per sé affatto semplici e banali, anche per esperti di sistemi e reti telematiche, nella connessa dimensione della protezione dei dati personali.

La tematica della *cybersecurity* è decisamente attuale e gioca, o comunque dovrebbe giocare, un ruolo sempre più strategico, come vero e proprio *asset* aziendale, e dovrebbe essere vissuta non solo come un ennesimo adempimento e fonte di costo né come un'ulteriore complicazione burocratica sulla via della funzionalità ed efficienza. Merita invece di essere valorizzata come una preziosa opportunità per analizzare e studiare i possibili profili di rischio per la sicurezza, ed, ancor prima, i profili di criticità organizzative e funzionali dell'azienda. Profili, a volte del tutto sconosciuti, che solo la creazione ed applicazione di una 'procedura' apposita può scovare, analizzare e 'curare', per prevenire incidenti più o meno gravi.

Ebbene – proprio in quest'ottica, consapevole quanto costruttiva! – quest'Opera fornisce ai suoi Lettori, e soprattutto agli operatori del settore, una guida decisamente chiara e concreta, sicuramente di grande ausilio su più 'fronti' di battaglia agli *hacker* – sempre più 'evoluti' ed insidiosi – o agli errori operativi, anche del tutto involontari, delle persone impiegate, a vario titolo, in azienda o nella PA.

Infatti, – dopo un opportuno inquadramento giuridico e definitorio della *cybersecurity*, considerata anzitutto nel superiore livello europeo della diret-

* Funzionario area direttiva Garante Protezione dati personali; Dottore di ricerca in Diritto Civile Scuola Sant'Anna di Pisa e Dottore di ricerca in Diritto del Lavoro Univ. Cattolica di Milano. La presente Prefazione s'intende formulata a titolo personale e non impegna in alcun modo la detta Autorità Garante.

tiva NIS2, quale cornice di principi e fondamentali istituti nonché nel derivato diritto nazionale con esplicita funzione attuativa ed operativa – gli Autori passano in rassegna gli aspetti, realmente cruciali, della materia e i connessi adempimenti, guidando, quasi per mano, i Lettori nella loro focalizzazione, ed auspicabilmente, nella loro corretta interpretazione ed applicazione. Mi riferisco, in particolare: ai soggetti sottoposti alla NIS2; ai settori ad alta criticità e agli altri settori critici, aiutando a comprendere se si rientri o meno nelle categorie obbligate dalla normativa.

Ma un valore aggiunto del Testo sono anche i passaggi – sempre chiari e pragmatici – dedicati alle procedure necessarie a garantire la sicurezza informatica; alla notifica degli incidenti informatici significativi; all'attività di *auditing* e di monitoraggio; al *Risk Assessment*; quale operazione 'strutturale' imprescindibile, per identificare, analizzare e gestire i rischi informatici che potrebbero compromettere la stabilità, la produttività e la reputazione di un'azienda, a fronte di un contesto digitale sempre più complesso, incerto e ricco di insidie, fisiologiche e patologiche, come per il caso degli attacchi informatici.

Un adeguato, ed opportuno, risalto viene riconosciuto al ruolo del principio cardine dell'accountability, o 'autoresponsabilità', potere e dovere al contempo, che rende – come per la conformità del trattamento dei dati alla stringente normativa GDPR – l'impresa e la PA il primo Garante della sicurezza informatica, spostando in alto, di un bel po', l'asticella dell'impegno di risorse umane e materiali. Ciò in un'ottica, necessariamente integrata ed olistica, non solo dei connessi adempimenti, ma della visione strategica, multilivello, dell'organizzazione aziendale, privata o pubblica che sia.

Ne consegue che gli Amministratori – e quindi anche le massime figure apicali – non possono più limitarsi a delegare la cibersicurezza alle funzioni IT né a vigilare sulle politiche di sicurezza, ma devono assumere un ruolo pro-attivo già nella fase della loro ideazione, progettazione, esecuzione e monitoraggio.

Ed è questo un precetto assistito, ai fini della sua necessaria effettività, dal rimedio coercitivo della sanzione pecuniaria – senza la quale la previsione normativa sarebbe destinata a rimanere 'lettera morta'! – rivolta non solo all'ente-impresa, ma anche agli amministratori, se non adeguatamente diligenti nella prevenzione dei rischi cibernetici. Ciò peraltro nella necessaria consapevolezza che il rischio di lesione della *cybersecurity* può associarsi a un serio rischio reputazionale. Rischio peraltro gravemente amplificato dalla cassa di risonanza del web, dove – come noto – abbondano giornali *on line*, *blog*, forum e siti d'informazione, d'indubbia rilevanza costituzionale, ma – non per tutti e non sempre – completa ed aderente alla realtà degli accadimenti.

Senza poter trascurare che ha un'eco molto maggiore la notizia relativa ad un evento negativo (qual è un incidente informatico) che quella relativa ad

una pluralità di eventi positivi, come, per il settore in esame, l'individuazione e la risoluzione dei problemi di sicurezza.

Le *bad* e le *fake news*, una volta entrate nella Rete, non possono essere più, efficacemente, riviste o tanto meno cancellate; peraltro il potente strumento del diritto "all'oblio", di cui all'art. 17 del GDPR, viene riconosciuto dal legislatore europeo solo alle persone fisiche. E sì, esiste, in astratto, lo strumento risarcitorio di eventuali danni d'immagine, ma, come noto, è agganciato a presupposti fattuali e giuridici (quali il dolo o la colpa di chi riporta e/o diffonde la notizia; il nesso causale fra la condotta dell'asserito danneggiante e il danno lamentato; la sufficiente prova di tali elementi); e, anche in questo settore, si aggiunga la complessità dei fattori tecnici e tecnologici in continua evoluzione, tali da impedire la riproduzione e la circolazione delle notizie e da rendere incerta l'individuazione dei responsabili.

Non si dimentichi che il valore Reputazione ed il valore Fiducia viaggiano sempre a braccetto in rapporto di reciproca influenza; e che, banalmente, un pregiudizio reputazionale comporta un serio rischio nella vendita di beni e servizi e, con esso, un evidente danno gius-consumeristico, oltre ad una possibile distorsione della dinamica concorrenziale del relativo mercato, soprattutto ove il produttore non goda di una condizione di monopolio.

Tutto ciò considerato, emerge la necessità anche di un'adeguata formazione – la cui funzione non a caso quest'opera chiaramente valorizza – mirata all'aggiornamento continuo, giuridico, e soprattutto tecnologico, non solo di tutti i lavoratori e di tutti quelli che prestano la loro attività in azienda, ma, anche e soprattutto, dei ruoli apicali, chiamati a confrontarsi, tempestivamente ed efficacemente, con i possibili scenari di crisi, anche perché investiti della 'responsabilità generale' ed ultima della problematica '*cybersecurity*' e dei connessi pregiudizi.

Altro aspetto importante sono, insieme, la proporzionalità e la gradualità, anche temporale, degli obblighi a carico di ogni azienda, evitando dunque di pensare che sussista un valido approccio "unico per tutti": a questo (regole diverse per realtà diverse) dovrà mirare la corretta esecuzione del ruolo della ACN, ossia l'Autorità preposta. Tuttavia, è questo medesimo approccio operativo/principio, che, a mio avviso, può trarsi da quanto – linearmente – descritto dagli Autori.

Quest'opera, in sintesi, non si perde in chiacchere dogmatiche o in dissertazioni accademiche, fornendo invece a chi vorrà – anche a quello desideroso di andare, concretamente, subito al sodo – ottime "istruzioni d'uso"!

1 Il significato di *cybersecurity*. La nascita e gli aspetti giuridici e tecnico-informatici della cibersicurezza

1.1. La definizione di *cybersecurity*

La parola *cybersecurity*, traducibile in italiano come 'sicurezza cibernetica', è in realtà un termine complesso che può essere riferito ad ambiti disciplinari molto differenti e che contiene elementi di diritto, di informatica, di analisi e di gestione dei rischi, di *governance* e di *compliance*. Volendo offrire una definizione più comprensibile potremmo sostenere che la *cybersecurity* sia un insieme di tecnologie, procedure e strumenti utilizzati per la protezione delle infrastrutture informatiche, dell'hardware, del software e delle reti da minacce esterne o interne che possono esser costituite da attacchi informatici, da attività di sabotaggio dei sistemi, dalla sottrazione di informazioni e di dati personali, dalla diffusione ed installazione di *malware* e dall'utilizzo di altri strumenti malevoli destinati a compromettere il funzionamento (*DoS Denial of Service*) o l'esistenza di uno o più sistemi informatici o di una o più reti.

Il concetto di cibersicurezza è ben rappresentato da una frase di Bruce Schneier, esperto mondiale di crittografia e sicurezza informatica: «La sicurezza non è un prodotto, ma un processo». Come ogni processo non si può definire una data esatta di inizio, né una data di ultimazione, tuttavia possiamo affermare senza timore di smentita che tale processo è in costante evoluzione e trasformazione e come avanzi parallelamente allo sviluppo della tecnologia e degli strumenti. In questo senso possiamo sicuramente concludere che l'esigenza e la domanda di sicurezza informatica non costituiscono un ostacolo allo sviluppo tecnologico ma, anzi, ha la finalità di garantire che lo stesso sia realizzato in maniera lineare, proficua, eticamente 'sostenibile' senza il rischio di generare errori, distorsioni e/o danni.

L'importanza della *cybersecurity* è cresciuta esponenzialmente negli ultimi trent'anni con la diffusione dei computer, con la creazione di internet, con il passaggio dall'analogico al digitale, con l'informatizzazione di ogni settore della vita umana dal lavoro all'economia, dalla salute al tempo libero,

l'informazione, ecc. La sensibilità per le tematiche di cibersicurezza anche da parte dei non esperti è cresciuta in maniera consistente con l'avvento dei sistemi di Intelligenza Artificiale (IA) e con l'utilizzo di strumenti che implementano queste nuove tecnologie.

Questo testo si pone come finalità quella di analizzare in modo comprensibile anche per i non addetti ai lavori gli aspetti giuridici e tecnico-informatici della *cybersecurity* fornendo definizioni, riferimenti normativi, suggerimenti ed indicando possibili strumenti di difesa, atti a garantire un ambiente digitale libero e sicuro.

1.2. Origine del concetto di *cybersecurity*

Durante gli anni della Guerra Fredda, un'Agenzia del Dipartimento della Difesa degli Stati Uniti iniziò a sviluppare una rete – denominata ArpaNet – in grado di assicurare lo scambio di informazioni anche in caso di eventi catastrofici quali attacchi militari o disastri naturali. Verso la fine degli anni '80 il progetto terminò, ma la tecnologia e le conoscenze acquisite diedero vita, grazie anche al supporto di imprese private, al World Wide Web, la rete internet.

Il primo attacco *hacker* ed il primo virus informatico risalgono al 1988 quanto uno studente americano, Robert Tappan Morris creò – più o meno involontariamente – un *malware* capace di replicarsi ed infettare altri sistemi operativi senza la necessità di un intervento umano. La creazione di Morris, chiamata *Morris worm*, infettò circa 6.000 computer utilizzati da università ed enti governativi statunitensi causandone il blocco totale per alcuni giorni.

Possiamo sostenere come il concetto di *cybersecurity* nasca e si amplifichi parallelamente allo sviluppo delle tecnologie informatiche e delle telecomunicazioni. Negli anni '90, l'espansione di internet e l'aumento delle minacce informatiche hanno attribuito al termine *cybersecurity* un significato ben preciso ed un'importanza sempre maggiore nella nostra società, al punto che attualmente possiamo parlare di un vero e proprio diritto della *cybersecurity*.

1.3. Quadro giuridico della *cybersecurity*: normativa comunitaria ed italiana

Il diritto della *cybersecurity* è sorto e si è sviluppato con l'andar del tempo trasformandosi da un insieme più o meno articolato di *best practices* in materia di sicurezza informatica ad un impianto organizzato su diversi livelli che comprende elementi di diritto, di informatica, di analisi e di gestione dei rischi. In questo capitolo andremo ad analizzare l'aspetto normativo della *cybersecurity* costituito, per l'Europa, da regolamenti immediatamente vincolanti e da direttive recepite dagli Stati membri dell'Unione.

Volendo censire le fonti del diritto della cibersicurezza occorre far riferimento sia ad organi legislativi comunitari che ad Autorità nazionali.

Come è noto, i Regolamenti europei emanati dagli Organi legislativi dell'Unione sono immediatamente vincolanti per tutti i Paesi membri, mentre le Direttive sono vincolanti solo allorquando siano state recepite dal singolo Paese attraverso l'emanazione di un atto normativo nazionale vincolante.

Se al momento attuale volessimo elencare le norme che dettano regole capaci di imporre obblighi in materia di sicurezza informatica dovremmo fare riferimento a più documenti:

- il **Regolamento Europeo 679/2016** del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (detto anche *General Data Protection Regulation* – GDPR) che disciplina la protezione dei dati personali nell'Unione Europea, stabilendo obblighi per il trattamento e la sicurezza delle informazioni personali. In particolare l'art. 32 prescrive che: «*il titolare e il responsabile del trattamento mettono in atto* ***misure tecniche e organizzative adeguate*** *per garantire un livello di sicurezza adeguato al rischio*»;
- la **Direttiva n. 2022/2555 NIS2** (*Network and Information Security*) del 14 dicembre 2022 del Parlamento Europeo e del Consiglio recepita dall'Italia con il **Decreto Legislativo n. 138/2024** che ha imposto obblighi di sicurezza più stringenti rispetto alla precedente Direttiva NIS1 per i soggetti definiti *essenziali* ed *importanti,* che operano in settori critici. La NIS2 e il Decreto n. 138 estendono l'ambito di applicazione a più settori chiave per l'economia del Paese e introducono sanzioni severe per il mancato rispetto degli standard minimi di sicurezza;
- la **Direttiva n. 2022/2557 CER** (*Critical Entities Resilience*) del 14 dicembre 2022 del Parlamento Europeo e del Consiglio relativa alla resilienza dei soggetti critici, recepita dall'Italia con il **Decreto Legislativo n. 134/2024** che si concentra sulla resilienza delle entità critiche. Mentre la NIS2 si focalizza sulla sicurezza delle reti e dei sistemi informativi, la Direttiva CER mira a garantire che i servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche, relative alla salute, alla sicurezza pubblica o dell'ambiente, siano forniti senza interruzioni, rafforzando la resilienza delle infrastrutture dei soggetti definiti *critici*;
- il **Regolamento CRA n. 2024/2847** del Parlamento Europeo e del Consiglio del 23 ottobre 2024 (*Cyber Resiliance Act- CRA*) prescrive requisiti di cibersicurezza per i prodotti hardware che software immessi sul mercato dell'UE garantendo che gli stessi siano progettati, sviluppati e realizzati con un adeguato livello di sicurezza informatica, affrontando le vulnerabilità durante l'intero ciclo di vita del prodotto;
- il **Regolamento DORA n. 2022/2554** del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il

settore finanziario (o anche *Digital Operational Resilience Act – DORA*) stabilisce requisiti per la resilienza operativa digitale degli enti finanziari, garantendo che gli stessi siano in grado di resistere e rispondere a attacchi informatici, che possano riprendere l'operatività entro breve tempo. Il Regolamento dispone controlli e verifiche periodioche sulla robustezza dei sistemi ICT.

In aggiunta alla produzione normativa sopra esposta non possiamo non menzionare alcune iniziative assunte dall'Italia che hanno determinato la definizione di un Piano Nazionale per la Cybersecurity e l'individuazione di un Framework Nazionale per la *cybersecurity* e la data protection.

Il **Piano nazionale per la *cybersecurity*** definito dall'Agenzia Cybersicurezza Nazionale (ACN) fa parte della cosiddetta *Strategia Nazionale di cibersicurezza 2022-2026,* che ha come obiettivo quello di garantire una transizione digitale sicura per il settore privato e per quello pubblico. La strategia prevede l'attuazione di 82 misure entro il 2026, assegnando la priorità al rafforzamento della resilienza cibernetica delle infrastrutture critiche, alla promozione di una cultura della sicurezza informatica ed allo sviluppo di capacità nazionali di prevenzione e risposta agli incidenti cibernetici.

Il Framework Nazionale per la *cybersecurity* e la data protection realizzato sul modello del *Cybersecurity Framework* del National Institute of Standards and Technology statunitense, è stato sviluppato per supportare le organizzazioni italiane nell'implementazione di strategie efficaci di gestione del rischio cibernetico e di protezione dei dati personali in 5 fasi.

- **Identificazione**: comprendere il contesto organizzativo per gestire il rischio cibernetico.
- **Protezione**: attuare misure di salvaguardia per garantire la continuità dei servizi.
- **Rilevazione**: implementare l'attività per individuare tempestivamente gli eventi di sicurezza informatica.
- **Risposta**: definire azioni per affrontare gli incidenti di sicurezza informatica.
- **Ripristino**: pianificare l'attività per ripristinare le capacità e i servizi compromessi a seguito di un incidente.

I due strumenti sopra citati hanno entrambi grande rilevanza in ambito cibersicurezza: mentre il Piano nazionale per la *cybersecurity* fornisce una visione strategica a livello nazionale per affrontare le sfide della sicurezza informatica, il Framework Nazionale offre alle organizzazioni strumenti pratici per implementare misure di sicurezza efficaci e conformi alle normative sulla protezione dei dati.

Questi riferimenti offrono una base solida per approfondire il tema della *cybersecurity* da una prospettiva sia tecnico informatica che giuridica.

2 NIS2: che cosa dice la Direttiva UE e come è stata recepita in Italia col Decreto Legislativo n. 138/2024

2.1. Il contenuto della Direttiva UE e il recepimento in Italia con il Decreto Legislativo n. 138/2024

Negli ultimi anni, la crescente digitalizzazione dei servizi essenziali e l'aumento delle minacce informatiche hanno reso indispensabile l'adozione di normative specifiche per garantire la sicurezza delle reti e delle informazioni all'interno dell'Unione Europea.

La Direttiva NIS (Direttiva 2016/1148, *Network and Information Security*), introdotta nel 2016, ha rappresentato il primo passo verso una regolamentazione unitaria in materia di *cybersecurity* tra Stati membri. Essa ha imposto requisiti di protezione a settori strategici come energia, trasporti e sanità. Tuttavia, la rapida trasformazione digitale e l'aumento degli attacchi informatici hanno evidenziato la necessità di aggiornare e rafforzare tale normativa.

Per rispondere a queste esigenze, è stata emanata la **Direttiva n. 2022/2555**, nota come NIS2, dal Parlamento Europeo e dal Consiglio. Il suo obiettivo è superare le criticità riscontrate nell'applicazione della normativa precedente e garantire un'efficacia uniforme delle misure di sicurezza a livello europeo.

La Direttiva NIS2 è stata recepita in Italia dal **Decreto Legislativo n. 138/2024**, entrato in vigore il 16 ottobre 2024. Il provvedimento aggiorna il quadro esistente in materia di cibersicurezza e garantisce un aumento del livello di sicurezza informatica comune. Il fine perseguito mira a soddisfare l'esigenza, ormai improrogabile, di garantire la sicurezza delle infrastrutture informatiche e la tutela dei dati sensibili, elementi fondamentali tanto per le Aziende private quanto per la Pubblica Amministrazione.

Il Decreto Legislativo n. 138/2024 introduce un quadro normativo più ampio e rigoroso rispetto alla precedente Direttiva NIS1, abrogando le misure contenute nel Decreto Legislativo n. 65/2018.

Le nuove disposizioni coinvolgono un numero maggiore di settori e soggetti, impongono standard di sicurezza più stringenti e introducono l'obbligo di implementare le misure di sicurezza, attribuiscono maggiori responsabilità ai dirigenti e prevedono controlli e sanzioni più severi in caso di mancata conformità.

2.2. Il Decreto Legislativo n. 138/2024 e il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN)

Per garantire l'attuazione efficace delle nuove misure in materia di cibersicurezza, il Decreto Legislativo n. 138/2024 affida un ruolo centrale all'**Agenzia per la Cybersicurezza Nazionale (ACN)**, ente responsabile della sicurezza informatica in Italia.

ACN ha il compito di applicare la normativa NIS2, supervisionare il rispetto delle regole e supportare Aziende ed Enti pubblici nel rafforzare la loro sicurezza contro le minacce informatiche.

A tal fine, l'Agenzia definisce delle Linee guida, fornisce raccomandazioni e chiarimenti e promuove buone pratiche per agevolare la conformità alla normativa.

ACN gestisce l'elenco delle Aziende e degli Enti soggetti agli obblighi previsti dalla NIS2, assicurandosi che siano adeguatamente preparati ad affrontare i rischi informatici.

ACN collabora strettamente con le Istituzioni europee, partecipa a gruppi di lavoro e interagisce con gli altri Stati membri per migliorare la sicurezza informatica nel nostro Paese. Opera in sinergia con le **Autorità di settore** (come il Ministero dell'Economia e delle Finanze e il Ministero delle Imprese e del Made in Italy), che hanno il compito di supervisionare l'attuazione degli obblighi in materia di *cybersecurity* nei rispettivi ambiti.

Il supporto operativo di ACN è garantito dal **CSIRT Italia** (*Computer Security Incident Response Team*), che gestisce gli incidenti informatici e coordina la comunicazione tra le istituzioni coinvolte. Le sue funzioni principali comprendono il monitoraggio degli incidenti informatici a livello nazionale, l'emissione di allarmi e avvisi sui rischi emergenti, l'analisi e gestione degli attacchi informatici e la sensibilizzazione delle istituzioni e dei cittadini sui pericoli informatici.

Oltre a stabilire le misure di sicurezza che le organizzazioni devono adottare, **ACN** ha anche il compito di monitorare e vigilare sulla loro applicazione, intervenendo se necessario per garantire che le norme vengano rispettate. Inoltre, rappresenta il punto di riferimento per la cooperazione con le altre autorità europee, mantenendo i contatti con la Commissione Europea e con **ENISA**, l'Agenzia dell'Unione Europea per la cibersicurezza.

2.3. L'ambito di applicazione del Decreto Legislativo n. 138/2024

Per comprendere se un soggetto è sottoposto agli obblighi della NIS2 occorre considerare le caratteristiche dimensionali e l'ambito di operatività settoriale in cui operano le Aziende e gli Enti pubblici.

A tal fine, il Decreto Legislativo n. 138/2024 stabilisce all'art.3 il **perimetro di applicazione** della normativa e individua le categorie di soggetti, pubblici e privati interessati.

L'elenco dettagliato di queste categorie è contenuto in quattro Allegati.

1. Il primo raccoglie i settori considerati «**altamente critici**» (energia, trasporti, acque, bancario, sanitario ecc.).
2. Il secondo include gli altri ambiti **«critici»** (servizi postali e di corriere, gestione rifiuti, fornitori di servizi digitali ecc..).
3. Il terzo specifica le **«Pubbliche Amministrazioni»** coinvolte (Pubbliche Amministrazioni centrali, le Regioni e Province autonome, le Città metropolitane, i Comuni con popolazione superiore ai 100.000 abitanti, i Comuni capoluoghi di Regione, le ASL e le organizzazioni pubbliche se presentano determinate caratteristiche dimensionali o qualitative in base ai settori di attività).
4. Il quarto identifica ulteriori soggetti privati che, pur non rientranti nei settori critici, sono soggetti alla normativa a seguito di un **processo di valutazione governativa**, in quanto svolgono attività importanti per la cibersicurezza nazionale.

L'art. 3, comma 2, stabilisce che il Decreto si applica ai soggetti indicati negli allegati I e II che superano i massimali previsti per le piccole imprese (ossia sono almeno medie imprese), ai sensi dell'art. 2, paragrafo 2, della Raccomandazione 2003/361/CE della Commissione. Tale norma definisce una piccola impresa come un'azienda con meno di 50 dipendenti e un fatturato annuo o un bilancio annuo che non superi i 10 milioni di euro.

Inoltre, la normativa contenuta nel Decreto si applica, **indipendentemente dalla dimensione dell'impresa, ad una serie di soggetti**, identificati come *critici* ai sensi della Direttiva n. 2022/2557, nonché ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, ai prestatori di servizi fiduciari, ai gestori dei registri di dominio di primo livello e ai fornitori di servizi di sistema dei nomi di dominio, ai fornitori di servizi di registrazione dei nomi di dominio e alle imprese associate o collegate ad un soggetto essenziale o importante, se soddisfano una serie di criteri.

Infine, ACN, su proposta delle Autorità di settore, può identificare **ulteriori soggetti** a cui applicare le misure previste dalla NIS2, sulla base di una

valutazione del rischio e in base alla tipologia di attività svolta. Tali soggetti, conclusa la procedura di identificazione descritta all'art. 3 comma 13 del Decreto, riceveranno una specifica notifica da parte di ACN e saranno tenuti a registrarsi sulla specifica piattaforma (art. 7 comma 1).

2.4. Gli obblighi prescritti dal Decreto Legislativo n. 138/2024 per Aziende ed Enti soggetti alla normativa NIS2

Le Aziende e gli Enti che rientrano nella normativa NIS2 devono rispettare una serie di obblighi per garantire la sicurezza informatica e la gestione efficace dei rischi. Gli obblighi riguardano diversi aspetti, come la registrazione e l'aggiornamento delle informazioni, l'adozione di misure di sicurezza, la gestione degli incidenti e la protezione dei dati.

L'obiettivo di queste misure è garantire che le Aziende e gli Enti coinvolti siano adeguatamente preparati ad affrontare le minacce informatiche. Inoltre, esse mirano a proteggere i loro sistemi e servizi, assicurando un livello elevato di sicurezza e resilienza.

I principali obblighi previsti dalla NIS2, recepiti nel Decreto Legislativo n. 139/2024 riguardano:

- **la registrazione e l'aggiornamento dei dati (art. 7)**: le Aziende devono iscriversi a una piattaforma dell'ACN e fornire informazioni preliminari, come la loro ragione sociale, l'indirizzo e i dati di contatti aggiornati. Devono inoltre designare un referente e specificare il settore in cui operano. Questi dati confluiscono in un elenco ufficiale e servono per elaborare statistiche destinate alla Commissione UE;
- **la maggiore responsabilità degli organi amministrativi (art. 23)**: i dirigenti sono tenuti a supervisionare e approvare le misure di sicurezza necessarie, assumendosi la responsabilità di eventuali violazioni;
- **le misure di sicurezza informatica (art. 24)**: le Aziende e gli Enti pubblici devono adottare strategie e strumenti adeguati per proteggere i loro sistemi informatici e prevenire incidenti. Questo obbligo include la necessità di svolgere una serie di attività come l'analisi dei rischi, la gestione degli incidenti, la protezione della catena di approvvigionamento, la formazione del personale e l'uso di tecnologie avanzate come la crittografia e l'autenticazione sicura;
- **l'obbligo di notifica degli incidenti (art. 25)**: in caso di attacchi informatici o altre criticità che possano compromettere i servizi, le Aziende e gli Enti devono informare tempestivamente il CSIRT Italia. La normativa prevede una comunicazione preliminare entro 24 ore, seguita da una no-

tifica più dettagliata entro 72 ore (24 ore per i fornitori di servizi fiduciari). Infine c'è l'obbligo di redigere una relazione finale entro un mese;

- **la gestione dei dati di registrazione dei nomi di dominio (art. 29)**: i Gestori dei registri di nomi di dominio e i fornitori di servizi di registrazione devono raccogliere e mantenere dati accurati sugli utenti, rispettando le normative europee sulla protezione dei dati personali;
- **la classificazione delle attività e dei servizi (art. 30)**: ogni Organizzazione deve identificare chiaramente la propria categoria e il tipo di servizi offerti, in conformità con la normativa.

Il Decreto n. 138/2024 prevede un'applicazione graduale delle nuove regole sulla sicurezza informatica: gli obblighi relativi alla sicurezza e alla gestione degli incidenti (articoli 23, 24 e 25) saranno definiti tramite provvedimenti del Direttore generale dell'Agenzia per la Cybersicurezza Nazionale. Questi provvedimenti stabiliranno i requisiti minimi di sicurezza che le Organizzazioni dovranno adottare entro ottobre 2026.

Per ciascuno dei 10 ambiti previsti dall'articolo 24 del Decreto NIS2, verranno specificati i requisiti di sicurezza essenziali da rispettare.

Per quanto riguarda, invece, la notifica degli incidenti informatici, negli allegati tecnici sono elencati i tipi di eventi considerati *incidenti significativi*, ovvero quelli che le organizzazioni saranno obbligate a segnalare secondo quanto previsto dall'articolo 25.

2.5. Sanzioni e meccanismi di conformità previsti nel Decreto Legislativo n. 138/2024

Aziende ed Enti pubblici devono rispettare la normativa NIS2 e il relativo Decreto di recepimento, poiché in caso di violazione sono previste sanzioni significative (art. 38).

ACN ha il compito di vigilare sul rispetto delle regole, intervenendo in caso di inadempienze. Tuttavia, l'obiettivo del sistema sanzionatorio non è solo punitivo, ma anche preventivo: le sanzioni mirano a incentivare un approccio proattivo alla sicurezza informatica.

Per raggiungere questo obiettivo, il sistema si basa su tre principi fondamentali. Innanzitutto, il **principio di effettività** assicura che le sanzioni abbiano un impatto reale, impedendo ai trasgressori di trarre vantaggio economico dal mancato rispetto delle norme. Il secondo principio, la **proporzionalità**, garantisce che l'entità della sanzione sia commisurata alla gravità della violazione, tenendo conto del danno causato e della condotta del soggetto.

Infine, il **principio di dissuasività** mira a scoraggiare non solo il trasgressore, ma anche altri soggetti dal commettere infrazioni analoghe, rafforzando la percezione del rischio e incentivando un comportamento più responsabile.

Le violazioni che possono comportare sanzioni sono diverse e riguardano principalmente:

- la mancata registrazione nella piattaforma, l'aggiornamento e la trasmissione delle informazioni;
- l'inosservanza delle modalità e degli standard di sicurezza imposti dalla NIS2;
- la violazione di obblighi settoriali di sicurezza imposti dagli artt. 27 e seguenti (come l'adozione di schemi di certificazione e la registrazione dei nomi di dominio);
- il mancato rispetto degli obblighi di collaborazione con le Autorità competenti (comportamento che ostacola la capacità di risposta agli incidenti di sicurezza e compromette la protezione dell'intero sistema);
- la mancata collaborazione con il CSIRT Italia.

Per evitare sanzioni troppo severe, il Decreto introduce meccanismi che favoriscono la **conformità volontaria**: l'ACN, prima di applicare una multa, può invitare il soggetto a regolarizzare la propria posizione entro un termine stabilito, offrendo così la possibilità di sanare l'infrazione senza incorrere in conseguenze più gravi.

Inoltre, è prevista la possibilità di estinguere anticipatamente la sanzione attraverso il pagamento ridotto, che consente di chiudere la contestazione con una somma pari a un terzo della sanzione massima applicabile. In alcuni casi, qualora la pubblicazione della sanzione risultasse sproporzionata, il soggetto può essere esonerato dall'obbligo di divulgazione, evitando ripercussioni reputazionali e incentivando il rispetto spontaneo delle norme.

Un aspetto rilevante del sistema sanzionatorio riguarda le **misure aggravate per le violazioni ripetute**, finalizzate a scoraggiare atteggiamenti di persistente inosservanza della norma. Se un soggetto commette la stessa infrazione più volte, l'importo della sanzione può essere raddoppiato, mentre nel caso di violazioni diverse, ma riconducibili a un comportamento sistematicamente non conforme, la multa può essere triplicata.

L'ammontare delle sanzioni amministrative pecuniarie varia in base alla tipologia del soggetto coinvolto (art. 38 comma 8).

Le Aziende classificate come *soggetti essenziali*, ovvero quelle che operano in settori critici, possono essere multate fino a 10 milioni di euro o al 2% del fatturato annuo globale, a seconda di quale importo sia superiore.

Per i *soggetti importanti*, ossia operatori di rilievo ma non strategici, la sanzione può arrivare a 7 milioni di euro o all'1,4% del fatturato annuo globale.

Le Pubbliche Amministrazioni, invece, sono soggette a multe più contenute, che variano tra i 25.000 e i 125.000 euro, con riduzioni per quelle di minore rilevanza. Pur essendo tenute a rispettare le regole di cibersicurezza, le

Pubbliche Amministrazioni beneficiano di alcune deroghe, finalizzate a garantire la continuità operativa dei servizi essenziali. Per questo motivo, non possono essere colpite da sanzioni che compromettano il loro funzionamento, come la sospensione delle attività. Tuttavia, devono comunque predisporre piani di adeguamento e sicurezza, che vengono costantemente monitorati dall'Agenzia per verificare il rispetto degli standard richiesti.

Il sistema sanzionatorio previsto dal Decreto sulla cibersicurezza non si limita a punire le infrazioni, ma è strutturato in modo da incentivare la conformità e la prevenzione. Chi si adegua alle norme in modo tempestivo può evitare sanzioni pesanti e ridurre al minimo le conseguenze di eventuali inadempienze, mentre chi ignora le direttive rischia multe elevate e provvedimenti progressivamente più severi in caso di recidiva.

3 I soggetti sottoposti alla NIS2, settori ad alta criticità ed altri settori critici

3.1. I criteri per individuare le imprese sottoposte agli obblighi della Direttiva NIS2

Per valutare se si è sottoposti o meno alla NIS2 è necessario considerare due diversi elementi:

- la dimensione dell'impresa (numero dei dipendenti e fatturato o bilancio);
- la sua appartenenza ad un settore ad alta criticità o comunque critico secondo quanto previsto dagli allegati n. I e II della Direttiva NIS2 e del Decreto legislativo di recepimento n. 138/2024.

Solo incrociando adeguatamente questi due parametri (dimensione dell'impresa e settore in cui si opera) è possibile ottenere una risposta.

In relazione alla dimensione dell'impresa (micro, piccola, media o grande) occorre far riferimento all'articolo 2, dell'allegato della Raccomandazione 2003/361/CE che recita:

1. *La categoria delle microimprese, delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.*
2. *Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.*
3. *Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.*

È opportuno specificare che per una corretta qualificazione inizialmente si considerava che l'azienda dovesse avere sia il requisito relativo al nume-

ro dei dipendenti (detti effettivi), che il requisito relativo al fatturato o al bilancio. Almeno questa è l'interpretazione che sino ad oggi era stata adottata dagli operatori, tuttavia l'ACN pare avere un orientamento diverso, maggiormente *estensivo,* che è descritto nella Faq n. 2.3 (Sezione "Ambito di applicazione") pubblicata sul sito dell'Agenzia https://www.acn.gov.it/portale/faq/nis che di seguito si trascrive:

Per la definizione di media impresa occorre far riferimento ai requisiti dimensionali indicati nell'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE: nonché, in modo più specifico alla Guida all'utente alla definizione di PMI (pubblicata dalal Commissine europea nel 2020).
Confrontando i propri dati con le soglie stabilite dalla citata disciplina, un'impresa può determinare se è una microimpresa, una piccola o una media impresa.
Le microimprese sono definite come imprese con meno di 10 occupati e che realizzano un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro.
Le piccole imprese sono definite come imprese con meno di 50 occupati e che realizzano un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.
Le medie imprese sono definite come imprese con meno di 250 occupati e che realizzano un fatturato annuo non superiore a 50 milioni di euro oppure un totale di bilancio annuo non superiore a 43 milioni di euro.
Si evidenzia che per essere riconducibile a una delle categorie di PMI (micro, piccola o media impresa) devono essere sempre soddisfatti, sia il criterio del numero di effettivi, sia almeno uno dei due parametri contabili (fatturato o bilancio) tra loro alternativi, essendo sufficiente che almeno uno dei due rientri nei parametri dimensionali. Se i valori dei parametri contabili sono superati entrambi, oppure se si supera anche solo il criterio del numero di effettivi, si ricade nella categoria più elevata di PMI (micro, piccola o media impresa), ovvero nella categoria delle grandi imprese. [...] La presente F, elaborata sulla base "Guida dell'utente alla definizione di PMI" pubblicata dalla UE nel 2020, mira a favorire l'attività di autovalutazione dell'impresa. Si segnala che analoga impostazione è stata seguita dall'Autorità nazionale competente NIS belga e che interpretazioni veicolate da fonti non ufficiali non saranno prese in considerazione.

In buona sostanza per l'Agenzia è sufficiente i) superare anche solo il numero dei dipendenti (gli effettivi) a prescindere dalla presenza dei requisiti dimensionali, ovvero ii) superare entrambi i parametri contabili, anche se il numero degli effettivi è inferiore, per rientrare nella categoria di impresa superiore. Secondo gli autori, tale interpretazione parrebbe poco convincente, tanto più in quanto contenuta in una Faq nella quale – poche righe prima – viene affermato l'esatto contrario. Sarà utile tener d'occhio ulteriori futuri chiarimenti.

3.2. I settori altamente critici e quelli critici secondo il Legislatore europeo

Rispetto al settore di operatività delle imprese che sono sottoposte alla Direttiva NIS2, è opportuno ricostruire il ragionamento del Legislatore Europeo che è partito dal concetto della necessità di difesa di '*soggetti critici*' con la Direttiva n. 2022/2557 CER (*Critical Entities Resilience*) del 14 dicembre 2022, che ha abrogato una precedente Direttiva CE del 2008 (n. 114).

Nelle considerazioni introduttive della Direttiva n. 2557 leggiamo che:

In quanto fornitori di servizi essenziali, i soggetti critici svolgono un ruolo indispensabile per il mantenimento delle funzioni vitali della società o di attività economiche nel mercato interno di un'economia dell'Unione sempre più interdipendente. È pertanto essenziale definire un quadro a livello dell'Unione volto sia a rafforzare la resilienza dei soggetti critici nel mercato interno, stabilendo misure minime armonizzate, sia ad assistere tali soggetti mediante misure di sostegno e vigilanza coerenti e dedicate.

Ai settori dei **trasporti** e dell'**energia** – già precedentemente individuati come **critici** dalla precedente Direttiva 2008/114/CE sulle «*infrastrutture critiche europee dei settori dell'energia e dei trasporti*» – la Direttiva n. 2022/2557 ha aggiunto altre organizzazioni che costituiscono «*soggetti critici nel settore alimentare, logistica e distribuzione all'ingrosso*». Quindi, sin dall'inizio, il Legislatore Europeo ha fissato alcuni punti fondamentali della strategia sulla cibersicurezza: chiarire gli obiettivi strategici, realizzare una *governance* per l'applicazione della strategia, individuare le misure e sopratutto fornire «una descrizione del processo di individuazione dei soggetti critici», (art. 4 Direttiva 2022/2557).

3.3. I soggetti obbligati al rispetto della Direttiva NIS2

3.3.1. Premessa

Come abbiamo avuto modo di osservare all'inizio del capitolo, al fine di accertare se un soggetto sia sottoposto o meno agli obblighi NIS2 occorre considerare le caratteristiche dimensionali e l'ambito di operatività settoriale.

L'attività di analisi finalizzata alla qualificazione di un'impresa come sottoposta alla Direttiva NIS2 incontra notevoli difficoltà sul piano interpretativo. Le definizioni delle attività e dei settori NIS2 devono essere adeguatamente compresi e calati nella realtà aziendale italiana. Questa attività ermeneutica è complicata dall'assenza di definizioni certe e dalla presenza di una

terminologia che è il risultato della traduzione in italiano del testo originale (inglese) della Direttiva.

Per facilitare l'interpretazione, ACN ha pubblicato sul proprio sito alcune Faq che sembrano offrire una risposta almeno a qualche interrogativo. L'Agenzia ha chiarito che al fine di ritenere ricompreso un soggetto all'interno delle definizioni della Direttiva **non risulta determinante né il codice ATECO dell'attività** (corrispondente al codice NACE europeo *Nomenclature statistique des activités économiques*), **né la prevalenza o meno di quell'attività particolare sul *core business* aziendale**. L'interprete dovrà tenere in considerazione le sole definizioni offerte dalla normativa europea.

Alla luce di ciò, la raccomandazione che gli autori si sentono di dare – qualora vi siano dubbi o incertezze sulla qualificazione dell'attività dell'impresa o sulla sua eventuale appartenenza ad uno specifico settore – è quella di procedere all'iscrizione sulla piattaforma ACN a scopo precauzionale al fine di non incorrere nell'applicazione delle sanzioni pecuniarie previste dalla normativa, come indicato al capitolo 6, paragrafo 6.

3.3.2. La qualificazione dei Soggetti nei settori NIS2

Sono sottoposti a NIS2 secondo l'art. 3 del Decreto legislativo n. 138/2024 di recepimento della Direttiva e successivi chiarimenti dell'Agenzia, pubblicati a marzo nelle Faq:

I) I **soggetti pubblici e privati che superino i limiti della piccola impresa** (quindi che siano media o grande impresa) **e che operino nel settore ad alta criticità di cui all'allegato I)** della Direttiva NIS2 e del Decreto di recepimento n. 138/2024 **o che operino nel settore comunque critico di cui all'allegato II)** della Direttiva NIS2 e del Decreto di recepimento n. 138/2024.

Secondo **l'allegato I)** sono **settori e sottosettori ad alta criticità:**

a) Energie

- **Sottosettore energia elettrica**, quindi l'impresa elettrica che rientra nelle ipotesi previste dall'art. 2 del Regolamento (UE) 2019/944, numeri 12 e 28 (produttori), 8, 29 e 35 (gestori) 25 (chi fornisce servizi di aggregazione, gestione della domanda o stoccaggio di energia), nonché gestori di un punto di ricarica che fornisce un servizio di ricarica ad utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità. La descrizione dei settori ha sollevato non poche perplessità al punto che ACN è dovuta intervenire emanando specifiche Faq di chiarimento. Le perplessità maggiori hanno riguardato:

- la figura del *produttore* all'interno della cui definizione sarebbe potuto entrare anche il soggetto che avesse prodotto elettricità per 'autoconsumo', avendo installato qualche pannello fotovoltaico e la figura del gestore delle colonnine di autoricarica dei veicoli elettrici.

Sul primo aspetto è intervenuta la Faq n. A1.1.a.3 che ha risposto al quesito:

Tutte le medie e grandi imprese che hanno impianti di produzione da fonti rinnovabili (es. fotovoltaico) rientrano nell'ambito di applicazione della nuova disciplina NIS? L'allegato I, settore 1) sotto-settore a) Energia elettrica nel definire, tra le altre, la seguente tipologia di soggetto 'produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944' non richiama anche l'articolo 2, comma 8, che identifica i cc.dd. prosumer, definiti quali clienti attivi.

Pertanto, le organizzazioni che non svolgono altre attività riconducibili agli allegati I e II e i soggetti che rispondono ai requisiti della definizione di ***prosumer*** (cliente attivo che ha installato un impianto di produzione elettrica per autoconsumo) non rientrano nell'ambito di applicazione del Decreto NIS2. Il termine *prosumer* o *prosumatore* è frutto di una crasi utilizzata per definire un soggetto che al tempo stesso è consumatore e produttore di un bene o un servizio.

Sul secondo aspetto è intervenuta la Faq n. A1.1.a.2 che ha risposto al quesito:

I punti vendita che offrono alla loro clientela punti di ricarica elettrica rientrano nell'ambito di applicazione della nuova disciplina NIS?
I punti vendita che offrono alla loro clientela punti di ricarica elettrica **non** rientrano nella definizione della tipologia di soggetto di "gestore di un punto di ricarica … Rientrano in tale definizione **solo i soggetti obbligati a registrarsi sulla Piattaforma nazionale unica dei punti di ricarica per i veicoli a energia elettrica – PUN** ai sensi dell'articolo 5 del Decreto ministeriale MASE n. 106 del 16 marzo 2023.

- **Sottosettore teleriscaldamento o teleraffrescamento**: gestori di impianti definiti all'articolo 2, punto 19), della Direttiva (UE) 2018/2001.
- **Sottosettore gas**: gestori dei sistemi di produzione, distribuzione e trasporto o stoccaggio di gas che rientrano nelle ipotesi di cui alla Direttiva 2009/73/CE.
- **Sottosettore petrolio**: gestori di oleodotti, impianti di raffinazione, trattamento, produzione trasporto o stoccaggio di petrolio.
- **Sottosettore idrogeno**: gestori di impianti di trattamento, produzione trasporto o stoccaggio di idrogeno.

b) Trasporti

- **Sottosettore aereo**: vettori aerei, gestori aeroportuali, imprese di controllo.
- **Sottosettore ferroviario**: gestori infrastrutture, imprese ferroviarie, gestori di servizi di controllo.
- **Sottosettore trasporto per acqua**: compagnie di navigazione, porti, gestori di servizi di assistenza ai traffici marittimi.
- **Sottosettore trasporto su strada**: autorità stradali, sistemi di controllo intelligenti.

c) Acque

- **Sottosettore acque potabili**: un fornitore di acque destinate al consumo umano o un distributore la cui attività essenziale (prevalente) è la distribuzione di acque destinate al consumo umano soggetto alla direttiva 2020/2184 recepita dal Decreto Legislativo 2023/18.
- **Sottosettore acque reflue**: un'impresa la cui attività essenziale (prevalente) è la raccolta di acque reflue urbane o domestiche o lo smaltimento di acque reflue urbane o domestiche o il trattamento di acque reflue urbane o domestiche o la raccolta di acque reflue industriali o lo smaltimento di acque reflue industriali (o il trattamento di acque reflue industriali soggetta alla direttiva 1991/271/CEE concernente il trattamento delle acque reflue urbane, recepita dal Decreto Legislativo 1999/152).

d) Settore bancario: enti creditizi la cui attività consiste nel raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto.

e) Infrastrutture finanziarie: gestori sedi di negoziazione e controparti centrali che si interpongono tra le controparti di contratti negoziati su uno o più mercati finanziari, diventando l'acquirente per ogni venditore e il venditore per ogni acquirente.

f) Settore sanitario: organizzazioni per le quali è vera almeno una delle seguenti affermazioni.

1. All'organizzazione si applica la Direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria recepita dal Decreto Legislativo 2014/2008; la stessa organizzazione è riconducibile a un prestatore di assistenza sanitaria ("qualsiasi persona fisica o giuridica o qualsiasi altra entità che fornisce legalmente assistenza sanitaria sul territorio di uno Stato membro" ex. articolo 3, lettera g), della medesima direttiva).

2. L'organizzazione è stata designata quale laboratorio di riferimento dell'UE ai sensi dell'articolo 15 del Regolamento 2022/2371/UE relativo alle gravi minacce per la salute a carattere transfrontaliero («la Commissione

può, mediante atti di esecuzione, designare laboratori di riferimento dell'UE per fornire supporto ai laboratori di riferimento nazionali al fine di promuovere le buone pratiche e l'allineamento da parte degli Stati membri su base volontaria in materia di diagnosi, metodi di analisi, utilizzo di determinati test per la sorveglianza uniforme, la notifica e la segnalazione delle malattie da parte degli Stati membri», ex. art. 15 del Regolamento medesimo).

3. All'organizzazione si applica la Direttiva 2001/83/CE recante un codice comunitario relativo ai medicinali per uso umano recepita dal Decreto Legislativo 2006/219; la stessa organizzazione è riconducibile a un soggetto che svolge attività di ricerca e sviluppo relative a medicinali («qualsiasi sostanza o combinazione di sostanze presentata allo scopo di curare o prevenire le malattie negli esseri umani; è considerato medicinale anche qualsiasi sostanza o associazione di sostanze che può essere somministrata all'uomo allo scopo di stabilire una diagnosi medica o di ripristinare, correggere o modificare funzioni fisiologiche dell'uomo», ex art. 1, punto 2), della medesima Direttiva).

4. L'organizzazione è riconducibile ai soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21 della NACE rev. 2.

5. All'organizzazione si applica il Regolamento 2022/123/UE sul rafforzamento del ruolo dell'Agenzia europea per i medicinali nella preparazione e nella gestione delle crisi relative ai medicinali e ai dispositivi medici; la stessa organizzazione è riconducibile ai soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica di cui all'«elenco dei dispositivi critici per l'emergenza di sanità pubblica», ex. articolo 22 del medesimo Regolamento.

In questo settore è stato particolarmente dibattuto il tema relativo alla qualificazione delle RSA. All'uopo ACN ha emanato la Faq A1.5.2:

Con riferimento alle RSA, tali organizzazioni, qualora superino i massimali per le piccole imprese definiti dalla Raccomandazione 2003/361, rientrano nell'ambito di applicazione del Decreto NIS in quanto, anche in forma residuale, prestano assistenza sanitaria.

g) Infrastrutture digitali, organizzazioni che sono riconducibili a:

- **fornitore di punti di interscambio internet** (cd. *Internet exchange point,* IXP);
- **fornitore di servizi fiduciari non qualificato** («una persona fisica o giuridica che fornisce uno o più servizi fiduciari in qualità di prestatore di servizi fiduciari non qualificato»);

- **fornitore di servizi fiduciari qualificato** («un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato»);
- **fornitore di reti pubbliche di comunicazione** («rete pubblica di comunicazione elettronica, una rete di comunicazione elettronica, utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di rete»);
- **fornitore di servizi di comunicazione elettronica accessibili al pubblico** («servizio di comunicazione elettronica, i servizi forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti, i tipi di servizi seguenti: a) servizio di accesso a internet», ovvero un servizio di comunicazione elettronica accessibile al pubblico che fornisce accesso a Internet e, di conseguenza, connettività a praticamente tutti i punti finali di Internet, indipendentemente dalla tecnologia di rete e dalle apparecchiature terminali utilizzate; b) servizio di comunicazione interpersonale; c) servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva»);
- **fornitore di servizi di sistema dei nomi di dominio** (un soggetto che fornisce alternativamente: i) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet; ii) servizi di risoluzione dei nomi di dominio autoritativi per uso da parte di terzi, fatta eccezione per i server dei nomi radice (cosiddetto root nameserver); sistema dei nomi di dominio, cosiddetto *Domain name system* (DNS), un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di instradamento e connettività di internet al fine di accedere a tali servizi e risorse»);
- **gestore di registro dei nomi di dominio di primo livello** («cosiddetto registro dei nomi TLD – *Top level domain*) o *registry*, soggetto cui è stato delegato uno specifico dominio di primo livello e che è responsabile dell'amministrazione di tale dominio di primo livello, compresa la registrazione dei nomi di dominio sotto tale dominio di primo livello, e del funzionamento tecnico di tale dominio di primo livello, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona del dominio di primo livello tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situa-