LA DIRETTIVA (UE) 2022/2055 (C.D. "DIRETTIVA NIS 2") E LA SUA ATTUAZIONE IN ITALIA: IL D.LGS. 138/2024 (C.D. "DECRETO NIS 2")

1. Il quadro normativo

Il 18 ottobre 2024 è entrato in vigore il D.lgs. 138/2024, che ha recepito in Italia la Direttiva (UE) 2022/2055 del 14 dicembre 2022, c.d. "*Network and Information Security 2*" (di seguito, rispettivamente, il "**Decreto NIS 2**" e la "**Direttiva NIS 2**").

La disciplina della Direttiva NIS 2 abroga la precedente Direttiva (UE) 2016/1148 del 6 luglio 2016 c.d. (di seguito, anche solo "**NIS 1**"), già recepita in Italia con d.lgs. 65/2018 (di seguito, il "**Decreto NIS 1**"), prevedendo regole più stringenti e un più ampio ambito di applicazione al fine di, tra l'altro,

potenziare la resilienza e la cooperazione tra i Paesi membri contro le minacce alla sicurezza informatica.

2. Competenze e funzione dell'Agenzia per la Cybersicurezza Nazionale (art.1)

In primo luogo, il Decreto NIS 2 «*conferma* [...] ***l'Agenzia per la cybersicurezza nazionale*** [di seguito, l'"**Agenzia Cybersicurezza**"] ***quale***:

1) *Autorità nazionale competente NIS* [di seguito, l'"**ACN**"], *disciplinandone i poteri inerenti all'implementazione e all'attuazione del presente decreto;*

2) *Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero;*

3) *Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (**CSIRT Italia**)*» (di seguito, "**CSIRT**")» (cfr. art. 1, co. 2, lett. c).

3. Quali soggetti sono tenuti ad adempiere a quanto previsto dal Decreto NIS 2?

Benché sul punto il Decreto NIS 2 sia di difficile interpretazione a causa di numerosi riferimenti incrociati che rendono piuttosto complicato individuarne il perimetro applicativo, si può, tuttavia, affermare (cfr. art. 3) che i soggetti tenuti a rispettare le obbligazioni di cui al Decreto NIS 2 sono, in primo luogo, quelli identificati in base ai settori di attività indicati negli **Allegati I** e **II**, ossia, rispettivamente i c.d. "**settori altamente critici** (energia, trasporti, settore bancario e mercati finanziari, sanità, acqua potabile e acque reflue, infrastrutture digitali, spazio)[1]" e gli "**altri settori critici** (servizi postali, rifiuti, sostanze chimiche, alimenti, alcune tipologie di fabbricazione, servizi digitali,

[1] Più nel dettaglio, rientrano nei c.d. "**settori altamente critici**", di cui all'**Allegato I**, le imprese operanti nei seguenti ambiti: **(i)** settore dell'**energia** (ed in particolare i sottosettori dell'energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas, idrogeno); **(ii) trasporti**, ed in particolare nei sottosettori del trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua, trasporto su strada; **(iii)** settore **bancario**; **(iv)** infrastrutture dei **mercati finanziari**; **(v)** settore **sanitario**; **(vi) acqua potabile**; **(vii) acque reflue**; **(viii) infrastrutture digitali**; **(ix)** gestione dei **servizi TIC** (*business-to-business*); **(x) spazio**.

ricerca)[2]". A tutti i soggetti sinora elencati e ricompresi negli Allegati I e II si applica il Decreto NIS 2 **a condizione che superino i massimali** per le piccole imprese, ossia abbiano **più di 50 dipendenti** e un **fatturato** o totale di bilancio annuo **superiore a 10 milioni di euro**[3].

4. Eccezione al criterio dimensionale

Il limite dimensionale appena indicato non è prescritto invece per i soggetti rientranti nell'**Allegato III** (amministrazioni centrali, regionali, locali e di altro tipo) e nell'**Allegato IV** (ai soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico).

Il Decreto NIS 2 individua, inoltre, un'ulteriore serie di soggetti – solo parzialmente coincidenti con quelli operativi nei settori di cui agli allegati I e II ("altamente critici" e "critici") – che rientrano nell'ambito di applicazione **indipendentemente dalle loro dimensioni**, a prescindere pertanto dal superamento dei massimali sopra menzionati:

a) ai soggetti che sono identificati come **soggetti critici** ai sensi del D.lgs. 134/2024, che ha recepito la Direttiva (UE) 2022/2557, c.d. "Direttiva CER" (si tratta di soggetti che svolgono servizi essenziali, che, salvo alcune differenze, coincidono con i settori individuati dagli Allegati I e II)[4];

[2] Più precisamente, rientrano nei c.d. "**altri settori critici**", di cui all'**Allegato II**, le imprese operanti nei seguenti settori: **(i) servizi postali** e di corriere; **(ii)** gestione dei **rifiuti**; **(iii)** fabbricazione, produzione e distribuzione di **sostanze chimiche**; **(iv)** produzione, trasformazione e distribuzione di **alimenti**; **(v) fabbricazione**, ed in particolare i seguenti sottosettori: (a) fabbricazione di **dispositivi medici** e di **dispositivi medico-diagnostici in vitro**; (b) fabbricazione di ***computer*** e prodotti di elettronica e ottica; (c) fabbricazione di **apparecchiature elettriche**; (d) fabbricazione di macchinari e apparecchiature n.c.a.; (e) fabbricazione di altri mezzi di trasporto; **(vi)** fornitori di **servizi digitali**; **(vii) ricerca.**

[3] Ciò in forza del rimando dell'art. 3, co. 2 alle soglie indicate nell'art. 2, par. 2, dell'allegato alla Raccomandazione 2003/361/CE.

[4] I "servizi essenziali" sono individuati (non tassativamente) dal Regolamento Delegato (UE) 2023/2450.

b) ai fornitori di **reti pubbliche di comunicazione elettronica** o di servizi di comunicazione elettronica accessibili al pubblico;

c) ai prestatori di **servizi fiduciari** (*i.e.* servizi di creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati relativi a tali servizi, servizi di creazione, verifica e convalida dei certificati di autenticazione di siti *web*, servizi di conservazione di firme, sigilli o certificati elettronici relativi a tali servizi);

d) ai **gestori di registri dei nomi di dominio** di primo livello e fornitori di **servizi di sistema dei nomi di dominio**;

e) ai fornitori di **servizi di registrazione dei nomi di dominio**;

In aggiunta a tutti i soggetti riportati nell'elenco, il Decreto NIS 2 si applica ai **soggetti** che svolgano la propria attività nell'ambito di un settore di cui all'Allegato I, II, III e IV, **individuati dall'Agenzia Cybersicurezza**, in qualità di ACN (che, peraltro, ai sensi dell'art. 3, co. 13, dovrà notificare a tali soggetti la loro individuazione ai fini della registrazione di cui all'art. 7, co. 1, Decreto NIS 2)[5].

[5] In base al Decreto NIS, l'individuazione avviene nel caso in cui: **(i)** il soggetto sia stato identificato come **operatore di servizi essenziali** ai sensi del Decreto NIS 1 (art. 4, co. 2) prima della data di entrata in vigore del Decreto NIS 2. Secondo tale disposizione, un soggetto è considerato operatore di servizi essenziali se soddisfa i seguenti criteri: (a) fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; (b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; (c) un incidente (vale a dire «*un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi*») avrebbe effetti negativi rilevanti sulla fornitura di tale servizio; **(ii)** il soggetto sia **l'unico fornitore nazionale di un servizio che è essenziale** per il mantenimento di attività sociali o economiche fondamentali; **(iii)** una perturbazione del servizio fornito dal soggetto potrebbe avere un **impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica**; **(iv)** una perturbazione del servizio fornito dal soggetto potrebbe comportare un **rischio sistemico significativo**, in particolare per i settori nei quali tale perturbazione potrebbe avere un **impatto transfrontaliero**; **(v)** il soggetto sia critico in ragione della sua **particolare importanza** a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato; **(vi)** il soggetto sia considerato critico ai sensi del

Infine, va evidenziato che, ai sensi dell'art. 40, con **decreto del Presidente del Consiglio** dei ministri, su proposta dell'Agenzia Cybersicurezza, possono essere stabiliti **ulteriori criteri di identificazione** delle tipologie di soggetto di cui agli allegati I e II, nonché delle ulteriori tipologie di soggetti che ricadono nell'ambito applicativo della disciplina (cfr. art. 3)[6].

5. Qual è l'ambito di applicazione del Decreto NIS 2

Il perimetro di applicazione del Decreto NIS 2 è, come anticipato, disorganico, rendendo difficile una valutazione a priori e imponendo una valutazione caso per caso rispetto all'attività svolta dalla singola impresa e alle sue dimensioni.

A questo fine, tornano senz'altro utili, in prima approssimazione, gli strumenti messi a disposizione sul sito dall'Agenzia Cybersicurezza (disponibili *qui*) nonché dall'ISTAT (in particolare, la classificazione c.d. "ATECO" delle attività economiche, disponibile *qui*, e il procedimento automatico per la relativa individuazione, disponibile *qui*).

In caso di dubbi, resta però imprescindibile il supporto fornito da una consulenza legale *ad hoc*.

6. Identificazione e registrazione dei soggetti essenziali e importanti (art. 7)

I soggetti che rientrano nell'ambito di applicazione del Decreto NIS 2 sono tenuti, entro il 28 febbraio di ciascun

presente decreto quale elemento sistemico della **catena di approvvigionamento, anche digitale**, di uno o più soggetti considerati essenziali o importanti (cfr. infra).

[6] In tale contesto, è opportuno rilevare che il Decreto NIS 2 all'art. 6 prevede un'ulteriore distinzione tra i soggetti ricompresi nel proprio ambito di applicazione, ossia quella tra "soggetti essenziali" e "soggetti importanti". Tale distinzione rileva sotto diversi profili applicativi della disciplina di cui al Decreto NIS 2, tra cui in particolare quella in tema di sanzioni.

anno, ad effettuare la propria registrazione sulla piattaforma digitale resa disponibile dall'ACN o, se già effettuata, ad aggiornarla (cfr. art. 7, co. 1).

Entro il 31 marzo di ciascun anno, l'Agenzia Cybersicurezza, in qualità di ACN, aggiorna l'elenco dei soggetti registrati, comprensivo sia dei soggetti essenziali sia dei soggetti importanti (cfr. art. 7, co. 2).

Inoltre, i soggetti registrati comunicano e aggiornano, tramite detta piattaforma digitale, un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza (cfr. art. 30, co. 1).

7. Misure per la gestione dei rischi per la sicurezza informatica e relativa responsabilità (artt. 23 e 24)

L'art. 23 definisce gli **obblighi** e le corrispondenti **responsabilità** in capo agli organi di amministrazione e direttivi sia dei soggetti essenziali sia dei soggetti importanti, i quali sono **direttamente responsabili** per le violazioni dei suddetti obblighi.

Nello specifico, tali organi sono dunque tenuti ad:

i) **approvare le modalità di implementazione** delle **misure di gestione dei rischi** per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24 (di cui *infra*);

ii) **sovrintendere all'implementazione degli obblighi** in materia di **gestione del rischio** per la sicurezza informatica e di **notifica dell'incidente** (cfr. capo IV e art.7).

In aggiunta, l'art. 23, co. 2 prevede un **obbligo formativo** per gli organi direttivi stessi e una responsabilità nella promozione di una "cultura della sicurezza informatica" all'interno dell'organizzazione. Questo implica:

i) la partecipazione a programmi di **formazione periodica** in materia di sicurezza informatica per gli amministratori e i dirigenti (art. 23, co. 2, lett. *a)*);

ii) la promozione e l'offerta di **corsi di aggiornamento** per il personale, volti a migliorare la consapevolezza e le competenze dei dipendenti in tema di protezione dei dati e risposta agli incidenti (art. 23, co. 2, lett. *b)*).

Le **misure per la gestione dei rischi per la sicurezza informatica** sono meglio precisate all'**art. 24**, il quale impone ai soggetti essenziali e importanti l'adozione di misure **tecniche, operative e organizzative** adeguate e proporzionate (secondo le modalità e i termini di cui agli artt. 30, 31 e 32) alla **gestione dei rischi connessi alla sicurezza dei sistemi informativi** e di **rete**[7] utilizzati da tali soggetti, sia nelle loro attività operative che nella fornitura di servizi.

La *ratio* di tali disposizioni è quella di **prevenire** o **minimizzare** l'impatto di eventuali incidenti di natura informatica, sia per i destinatari dei servizi sia per altri servizi interconnessi.

Ai sensi dell'art. 24, co. 1, tali misure:

i) assicurano un livello di sicurezza dei sistemi informativi e di rete **adeguato ai rischi esistenti**, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione (art. 24, co. 1, lett. *a)*);

ii) sono **proporzionate al grado di esposizione a rischi del soggetto**, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché

[7] Con tale locuzione si intende, ai sensi del Decreto NIS 2, art. 2, lett q): «*la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi*».

alla loro gravità, compreso il loro impatto sociale ed economico (art. 24, co. 1, lett *b)*).

Queste misure sono basate su un **approccio multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono ad esempio le politiche di analisi dei rischi e di sicurezza dei sistemi informativi di rete, la gestione degli incidenti con procedure e strumenti per le notifiche obbligatorie e piani di continuità operativa[8].

Quando si applicano misure legate alla sicurezza della catena di fornitura, è importante considerare le vulnerabilità specifiche di ciascun fornitore. Ai sensi dell'art. 24, co. 3, infatti, devono essere valutati la qualità dei prodotti, le pratiche di sicurezza e le procedure di sviluppo sicuro adottate dai fornitori, nonché i risultati delle analisi coordinate sui rischi della catena di approvvigionamento condotte dal Gruppo di cooperazione NIS (che ha la finalità di garantire la cooperazione e lo scambio di informazioni tra gli Stati membri).

8. Notifica degli incidenti e dei quasi incidenti[9] (art. 25)

[8] Più precisamente, il 2° comma dell'art. 24, dispone che le misure di cui al comma 1, devono comprendere almeno i seguenti elementi: **(i)** politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete; **(ii)** gestione degli incidenti con procedure e strumenti per le notifiche obbligatorie (di cui agli artt. 25 e 26 di cui infra); **(iii)** piani di continuità operativa, incluso il backup e il recupero dati in caso di disastri e gestione della crisi; **(iv)** sicurezza della catena di approvvigionamento, con attenzione agli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; **(v)** sicurezza nello sviluppo e manutenzione dei sistemi informativi, inclusa la gestione delle vulnerabilità; **(vi)** procedure di valutazione dell'efficacia delle misure adottate; **(vii)** formazione e igiene informatica per garantire la consapevolezza e la preparazione del personale; **(viii)** uso della crittografia e tecniche di cifratura, ove necessario; **(ix)** controllo degli accessi, affidabilità del personale e gestione degli asset; **(x)** autenticazione a più fattori e sistemi protetti per le comunicazioni interne ed emergenziali.

[9] Con tale locuzione si intende, ai sensi del Decreto NIS 2, art. 2, lett q): *«cd. near-miss, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato»*.

L'art. 25 prescrive in capo ai soggetti essenziali e importanti, di ("prenotificare" e, poi, di) **notificare all'Agenzia Cybersicurezza**, quale CSIRT, «***ogni incidente che*** [...] ***ha un impatto significativo*** *sulla fornitura dei loro servizi*» (per la sua idoneità a perturbare l'operatività dei servizi resi, avere ripercussioni su altre persone fisiche o giuridiche), seguendo le seguenti fasi: prenotificare entro 24 ore l'incidente e trasmettere la successiva notifica 72 ore, e da ultimo presentare, entro un mese, una relazione finale, dettagliando l'incidente, le cause, le misure adottate e l'eventuale impatto transfrontaliero[10].

Entro 24 ore dal ricevimento della pre-notifica, **il CSIRT fornisce una risposta** al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o **consulenza sull'attuazione di possibili misure tecniche** di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico (cfr. art. 25, co. 7).

L'Agenzia Cybersicurezza, quale ACN quale CSIRT, inoltre, **può informare il pubblico** riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia nell'interesse pubblico (cfr. art. 25, co. 11).

9. Competenze e poteri dell'ACN (artt. 34 e 35)

[10] Nel dettaglio, l'art. 25 del Decreto NIS due, prevede in caso di incidente, che il soggetto essenziale o importante sia tenuto a **(i)** trasmettere, entro 24 ore, una "pre-notifica" dell'incidente, che indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero; **(ii)** trasmettere, entro 72 ore, una "notifica" vera e propria dell'incidente, che contenga, *inter alia*, una valutazione iniziale dell'incidente significativo, della gravità e del suo impatto; **(iii)** trasmettere, quando richiesti dal CSIRT, i dovuti aggiornamenti sulla situazione; e da ultimo **(iv)** trasmettere, entro un mese dalla trasmissione della notifica, una relazione finale, comprensiva di una descrizione dettagliata dell'incidente, la causa originale della stessa, le misure di attenuazione adottate o in corso nonché, ove noto, l'impatto transfrontaliero dell'incidente.

All'ACN è affidato un **compito di vigilanza** (cfr. art. 34), consistente nel **monitorare** e fornire la propria analisi e supporto ai soggetti essenziali e ai soggetti importanti, compiere attività di verifica e **ispezioni**, e, se del caso, adottare **misure di esecuzione** ai sensi dell'art. 35, e irrogare le **sanzioni** amministrative e pecuniarie (cfr. artt. 37 e 38, di cui di seguito).

Ai sensi dell'art. 35, in particolare, le misure di sicurezza che l'ACN può adottare consistono, fra l'altro, nel potere richiedere ai soggetti una **rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi** del Decreto NIS 2; richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza; di richiedere ai soggetti l'esecuzione di scansioni di sicurezza; nonché di emanare raccomandazioni e avvertimenti relativi a presunte violazioni degli obblighi.

10. Provvedimenti e sanzioni per le inadempienze (artt. 37 e 38)

Ai sensi dell'art. 37 del Decreto NIS 2, inoltre, l'Agenzia Cybersicurezza (in qualità di ACN) «*nell'esercizio dei suoi poteri di esecuzione può richiedere ai soggetti, dichiarandone la finalità, di fornire i dati che dimostrino l'attuazione di politiche di sicurezza informatica, quali i risultati di audit sulla sicurezza e i relativi elementi di prova, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali anche ai fini* […]» della valutazione delle misure di gestione dei rischi implementate (cfr. *supra*, artt. 23 e 24) e del rispetto degli obblighi di notifica (cfr. *supra*, art. 25).

Nell'esercizio dei propri poteri di controllo e sorveglianza, l'Agenzia Cybersicurezza può inoltre «*intimare l'osservanza di istruzioni vincolanti per evitare il verificarsi di un incidente o per porvi rimedio*» (cfr. art. 37, co 4), e, qualora il soggetto intimato non adempia, può diffidarlo ad adempiere (cfr. art. 37, co. 6).

Qualora il soggetto non adempia agli obblighi del Decreto NIS 2, la l'Agenzia Cybersicurezza, ai sensi dell'art. 38, può inoltre irrogare **sanzioni amministrative**, che possono arrivare sino all'importo di 10.000.000 o del 2% del totale del fatturato annuo, e, inoltre, possono inoltre colpire direttamente le persone fisiche svolgono funzioni dirigenziali all'interno del soggetto essenziale, dichiarandone l'incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto.

11. Conclusioni

In estrema sintesi, si può ritenere che il Decreto NIS 2 abbia previsto un ambito applicativo particolarmente esteso e disomogeneo, rendendo complessa l'identificazione preventiva dei soggetti obbligati a rispettare i nuovi requisiti. In questo contesto, una consulenza legale mirata diventa essenziale per orientarsi tra le sfumature normative e definire gli obblighi specifici. Il team legale di GVA è a vostra disposizione per offrire un supporto personalizzato e competente, garantendo una valutazione accurata caso per caso.

Da ultimo, è importante considerare che i soggetti obbligati saranno tenuti, fra le altre cose e sotto la propria responsabilità, a implementare sistemi di prevenzione e/o gestione dei rischi legati a incidenti o quasi-incidenti informatici, al fine di prevenirli o mitigarli.

Il Decreto NIS 2 prevede, infine, sanzioni significative per il mancato rispetto degli obblighi in esso disciplinati, rendendo ancora più urgente un adeguamento accurato e tempestivo.

Tuttavia, alla luce della portata innovativa della disciplina in esame, solo la prassi applicativa, inclusa l'attività operativa dell'Agenzia Cybersicurezza, potrà offrire nel tempo indicazioni utili per un'interpretazione più chiara e concreta di tale normativa.

Dott. Lorenzo Parma

lorenzo.parma@gvalex.it

Dott.ssa Letizia Lombardi

letizia.lombardi@gvalex.it

GRECO VITALI
ASSOCIATI

gvalex.it