Simona Lanna
Vincenzo Colarocco

Il nuovo *framework* europeo per la tutela dei dati e la prevenzione sistemica degli attacchi informatici: la direttiva NIS2*

PARTE 2

Il 18 ottobre 2024 diventerà applicativa la Direttiva (Ue) 2022/2555 ("NIS2") sulla sicurezza delle reti e dei sistemi informativi dell'Unione europea. Cerchiamo di capire quali sono i soggetti interessati dalla normativa ed a quali obblighi sono tenuti.

* Articolo collegato al contributo di S. LANNA e V. COLAROCCO "Il nuovo framework europeo per la tutela dei dati e la prevenzione sistemica degli attacchi informatici: dalla Direttiva NIS 1 alla Direttiva NIS 2" in Rivista Qualità n.1/2023 pag.6

1. I soggetti interessati dagli obblighi imposti dalla disciplina della NIS2

La Direttiva NIS2 ha come obiettivo di eliminare le ampie divergenze che l'attuazione della Direttiva NIS1 ha creato tra gli Stati membri al fine di garantire una gestione integrata dei rischi cyber ed una applicazione uniforme degli obblighi all'interno di tutto il territorio europeo. A tal fine, la NIS2 ha definito dei criteri oggettivi per la corretta individuazione dei soggetti obbligati dalla nuova disciplina, i quali vengono classificati in due categorie - **"soggetti essenziali"** e **"soggetti importanti"** – in funzione della loro rilevanza strategica dovuta al settore nel quale operano, ai servizi che erogano nonché alle loro dimensioni (c.d. ***"Size-cap"***).

Più nel dettaglio, ai sensi dell'art. 2 della Direttiva, sono interessati dall'applicazione della nuova disciplina:

- i soggetti pubblici e privati, considerati **almeno** medie imprese[1] , che prestano i propri servizi o svolgono le loro attività nell'Unione europea nell'ambito dei settori strategici indicati negli Allegati I e II della stessa Direttiva;
- quei soggetti, pubblici o privati, rientranti nelle categorie di cui agli Allegati I e II della Direttiva che, indipendentemente dalle loro dimensioni, abbiano una rilevanza strategica per cui la loro compromissione comporterebbe un elevato rischio di sicurezza per tutti i Paesi dell'Unione.

I soggetti destinatari della nuova disciplina sono poi classificati, ai sensi dell'art. 3 della Direttiva, in "Soggetti essenziali" e "Soggetti importanti" in relazione al tipo di attività svolta e al settore nel quale operano. **(vedi box 1 sotto).**

BOX 1
Soggetti ESSENZIALI e Soggetti IMPORTANTI a norma della Direttiva NIS2 (cfr. articolo 3 Direttiva)

SOGGETTI ESSENZIALI	a) i soggetti di cui all'allegato I della Direttiva che superano i massimali per le medie imprese di cui all'art. 2, par. 1, dell'allegato della raccomandazione 2003/361/CE; b) i prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni; c) i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'art. 2, dell'allegato alla raccomandazione 2003/361/CE; d) i soggetti della pubblica amministrazione di cui all'art. 2, par. 2, lett. f), punto i); e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'art. 2, par. 2, lett. da b) a e); f) i soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557, di cui all'art. 2, par. 3 della presente direttiva; g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale.
SOGGETTI IMPORTANTI	In via residuale: a) i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del par. 1 dell'art. 3. b) i soggetti pubblici o privati identificati dagli Stati membri come soggetti importanti che, indipendentemente dalle loro dimensioni, abbiano una rilevanza strategica per cui la loro compromissione comporterebbe un elevato rischio di sicurezza per tutti i Paesi dell'Unione, ai sensi dell'art. 2, par. 2, lett. da b) a e).

BOX 2 Settori a rischio altamente critico/critico ai sensi della Direttiva NIS 2 (cfr. Allegati I e II alla Direttiva)	
Settori ritenuti a rischio altamente critico	**Settori ritenuti a rischio critico**
Energia	Servizi postali e di corriere
Trasporti	Gestione dei rifiuti
Settore Bancario	Fabbricazione, produzione e distribuzione di sostanze chimiche
Infrastrutture dei mercati finanziari	Fabbricazione di dispositivi medici e medico-diagnostici in vitro
Settore Sanitario	Fabbricazione di prodotti elettronici quali computer e prodotti di elettronica e ottica, apparecchiature elettriche e mezzi di trasporto
Acqua potabile e delle acque reflue	
Infrastrutture digitali	
Gestione dei rischi TIC (Business to Business)	
Pubblica Amministrazione	
Settore Aerospaziale	

Gli Allegati I e II alla Direttiva individuano invece, nel dettaglio, i settori ritenuti a rischio critico o altamente critico a livello europeo **(a tal fine si veda il box 2 sopra).**

Ogni Stato membro potrà, in sede di applicazione della Direttiva, integrare tale elenco inserendo ulteriori settori ritenuti a rischio elevato (dunque critico o altamente critico) e decidere di rendere applicabile la Direttiva anche agli enti della pubblica amministrazione locale ed agli istituti di istruzione, in particolare ove si svolgano attività di ricerca.

Al fine di definire in modo chiaro i soggetti sottoposti all'applicazione della Direttiva, ciascun Paese dovrà pertanto elaborare, **entro il 17 aprile 2025,** un elenco dei soggetti ritenuti essenziali ed importanti nella normativa di attuazione interna. Gli Stati dovranno altresì istituire dei meccanismi nazionali che consentano agli operatori di registrarsi all'elenco che sarà soggetto a revisione periodica, almeno biennale.

1. E ciò secondo quanto previsto dalla Raccomandazione 2003/361/CE della Commissione europea relativa alla definizione delle microimprese, piccole e medie imprese. In particolare, ai sensi dell'art. 2, par. 1, della Direttiva "La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione".

1.1. Soggetti esclusi

Esclusi dalla Direttiva sono i soggetti della pubblica amministrazione che operano **principalmente** nei settori della sicurezza nazionale, della sicurezza pubblica, della difesa o che svolgono attività di contrasto, prevenzione, indagine, accertamento e perseguimento dei reati[2] al contrario dagli enti della PA le cui attività rientrano anche solo **marginalmente** nei settori sopra menzionati, ivi inclusi i soggetti aventi competenze normative.

2.La strategia nazionale per la cybersicurezza

In linea con le previsioni programmatiche della Direttiva ogni Stato membro dovrà definire il proprio nuovo piano strategico nazionale per la cybersicurezza e sarà chiamato a designare:

- una o più autorità competenti responsabili della cybersicurezza e delle attività di vigilanza e controllo sull'attuazione della direttiva a livello nazionale;
- un c.d. punto di contatto unico avente funzione di collegamento con le altre autorità europee, la Commissione e l'ENISA *("European Union Agency for Cybersecurity" - Agenzia dell'Unione europea per la Cyber Sicurezza)*, al fine di garantire la cooperazione transfrontaliera;
- una o più autorità competenti a gestire gli incidenti ed i rischi di cybersicurezza su larga scala (le c.d. **autorità di gestione delle crisi informatiche**) – sulla base di quanto definito nel *piano nazionale di risposta agli incidenti e alle crisi di cybersicurezza su vasta scala,* contenente gli obiettivi e le modalità operative di prevenzione e reazione ai rischi di sicurezza informatica su vasta scala che dovrà essere adottato da ciascun Paese – presso le quali verranno istituiti;
- i **team di gestione e risposta agli incidenti di sicurezza informatica,** (i c.d. *Computer Security Incident Response Team,* di seguito, **"CSIRT"**) – è già presente, in Italia, presso l'Agenzia per la Cybersicurezza Nazionale (**"ACN"**).

RUOLO DEI CSIRT COMPUTER SECURITY INCIDENT RESPONSE TEAM (cfr. Articolo 11 della Direttiva)

I CSIRT:

- svolgono attività di monitoraggio ed analisi delle minacce informatiche, delle vulnerabilità e degli incidenti di sicurezza a livello nazionale e, su richiesta, forniscono assistenza ai soggetti essenziali ed importanti per quanto riguarda il monitoraggio dei loro sistemi informatici e di rete, ovvero scansioni proattive dei loro sistemi informatici e di rete per rilevare le vulnerabilità con impatto potenzialmente significativo;
- emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti interessati, nonché alle autorità competenti ed agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti[3].

2. Si veda, in tal senso, il Considerando (8) della Direttiva 2022/2555
3. Cfr. Art. 11, par. 3, della Direttiva 2022/2555.

3. Gli obblighi in capo ai soggetti interessati: la predisposizione ed implementazione di adeguate misure tecniche ed organizzative adeguate e gli obblighi di segnalazione

I soggetti interessati sono chiamati a compiere una serie di attività, tra cui l'adozione di modelli di *governance* basati su un approccio *risk-based,* l'implementazione di misure adeguate di gestione dei rischi di cybersicurezza, l'obbligo di effettuare valutazioni del rischio sulla sicurezza delle catene di approvvigionamento critiche ed obblighi di segnalazione alle autorità.

- **Dal punto di vista della *governance* aziendale,** la Direttiva impone ai soggetti interessati di implementare misure tecniche, operative ed organizzative adeguate per la gestione dei rischi e finalizzate a prevenire o ridurre al minimo l'impatto di eventuali incidenti. Tra queste, a titolo esemplificativo:
  - l'adozione di politiche di analisi e gestione dei rischi di sicurezza dei sistemi informatici e di gestione degli incidenti,
  - l'implementazione di procedure di *incident response* e di *Business Continuity* per la gestione delle crisi,
  - lo svolgimento di sessioni formative per il personale in materia di *cybersecurity* o la predisposizione di test periodici volti a verificare la sicurezza dell'infrastruttura IT e l'efficacia delle misure implementate.

Le misure di sicurezza devono essere approvate dagli organi di gestione dei soggetti interessati, i quali sovrintendono l'attuazione delle prescrizioni imposte dalla disciplina e sono responsabili in caso di violazione di tali obblighi[4].

- **Gli obblighi di segnalazione di cui all'art. 23 della Direttiva** impongono ai soggetti interessati di notificare al CSIRT (o ad altra autorità competente) gli incidenti significativi[5] subìti, senza indebito ritardo, specificando qualsiasi informazione utile che consenta all'autorità di determinare l'eventuale impatto transfrontaliero dell'incidente.

Qualora tali incidenti rischino di compromettere la fornitura dei propri servizi in favore dei *partner* destinatari, i soggetti interessati saranno tenuti ad informare anche questi dell'eventuale incidente ed a fornire indicazioni circa le misure e/o le azioni correttive da adottare in risposta a tale minaccia.
Vi è sul punto da segnalare che il processo di segnalazione della NIS2 è più circoscritto, completo e tempestivo rispetto a quello previsto dalla NIS1, con l'introduzione di termini specifici per l'adempimento degli obblighi di comunicazione degli incidenti alle autorità **(v. figura 1).**

4. I poteri di vigilanza ed esecuzione

La Direttiva riconosce alle autorità competenti il potere di svolgere attività ispettive nei confronti dei soggetti interessati dalla normativa secondo un regime di controlli differenziato tra i soggetti essenziali ed importanti. A norma dell'art. 23, infatti, i soggetti essenziali possono essere assoggettati ad attività di vigilanza sia di tipo preventivo che successivamente alla segnalazione di un incidente (controlli ex ante ed ex post), mentre i soggetti importanti possono essere sottoposti solo a controlli ex post - cioè successivi al ricevimento di segnalazioni da parte dell'autorità competente ovvero in conseguenza del reperimento di informazioni che suggeriscano una possibile violazione della Direttiva.

4. Cfr. Artt. 20 e 21 della Direttiva 2022/2555.
5. Cfr. Art. 23, par. 3, della Direttiva 2022/2555, a norma del quale un incidente è significativo se:
"a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli".

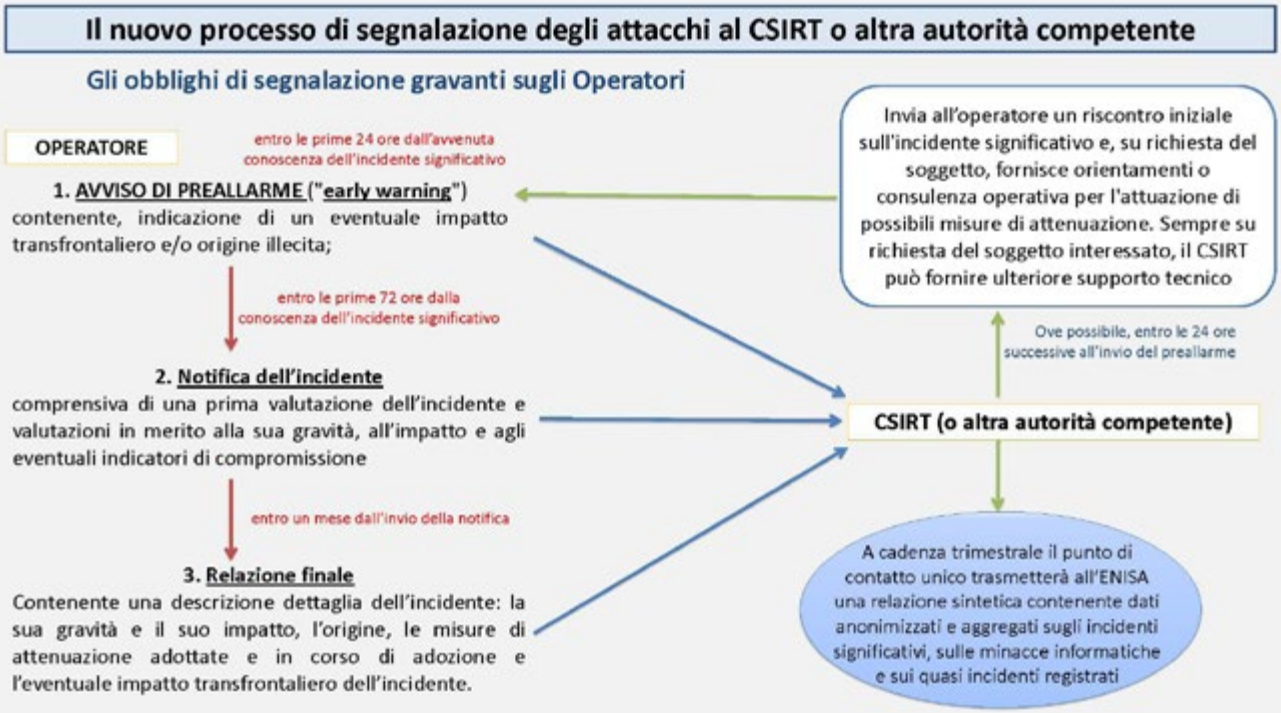

Figura 1 - Fonte: Questo flusso è stato elaborato direttamente da noi di Studio Previti

ESEMPIO ATTIVITÀ ISPETTIVE DA PARTE DELL'AUTORITÀ

L'autorità competente a svolgere le attività di vigilanza ed esecutive può, a titolo esemplificativo: effettuare *audit* periodici o mirati sulla sicurezza; svolgere ispezioni presso la sede degli operatori interessati; effettuare scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti; sottoporre gli interessati a richieste di accesso a dati e informazioni, ivi comprese le evidenze delle politiche di *cybersecurity* adottate.

6. Si veda il Considerando (133) alla Direttiva 2022/2555.

4.1. Rischi sanzionatori

A seguito dello svolgimento delle attività ispettive, le autorità competenti hanno il potere di comminare sanzioni di tipo amministrativo-pecuniarie a carico dei soggetti interessati nel rispetto dei requisiti di effettività, proporzionalità e dissuasività.

Inoltre, per rafforzare ulteriormente l'efficacia ed il carattere dissuasivo delle misure di esecuzione applicabili nel caso sia accertata la violazione degli obblighi imposti ai soggetti interessati, è riconosciuta altresì alle autorità competenti la facoltà di "*sospendere temporaneamente o di richiedere la sospensione temporanea di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi pertinenti forniti o dalle attività effettuate da un soggetto essenziale* e ***di richiedere l'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di qualsiasi persona fisica che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale***[6]" .

Quest'ultima ipotesi sanzionatoria costituisce comunque una *extrema ratio* esperibile esclusivamente una volta esaurite tutte le altre misure di esecuzione previste dalla Direttiva e solo fintantoché il soggetto interessato non adotti le misure necessarie imposte dalle prescrizioni dell'autorità competente.

5. Entrata in vigore della Direttiva e considerazioni conclusive

I Legislatori nazionali dell'Unione hanno tempo fino al **17 ottobre 2024** per recepire la Direttiva NIS2 ed anche le imprese interessate avranno a disposizione lo stesso tempo per adeguarsi e dotarsi delle misure di *governance* e di *cyber* sicurezza richieste dalla nuova disciplina europea: si resta dunque in fremente attesa dell'intervento normativo del Legislatore italiano.

SCHEMA DELLE MISURE SANZIONATORIE

Sanzioni di tipo amministrativo pecuniarie	Sanzioni ulteriori (extrema ratio)
Nei confronti dei soggetti essenziali: **fino a 10 milioni di euro** - o ad un massimo di **almeno il 2% del totale del fatturato** mondiale annuo dell'impresa.	Sospensione temporanea di una certificazione o di un'autorizzazione relativa ad una parte o alla totalità dei servizi pertinenti forniti o dalle attività effettuate da un soggetto essenziale.
Nei confronti dei soggetti importanti: **fino 7 milioni di euro** – o ad un massimo di **almeno l'1,4% del totale del fatturato** mondiale annuo dell'impresa.	Imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di qualsiasi persona fisica che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale.